RANK ATTACK DETECTION TECHNIQUES FOR THE INTERNET OF THINGS

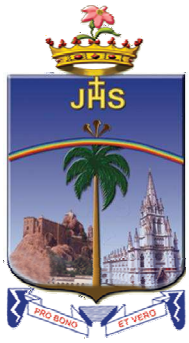
Thesis submitted to the Bharathidasan University
in partial fulfillment of the requirements for
the award of the degree of
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

By

A. STEPHEN, M.Sc., M.Phil.,
(Ref. No. 01263/Ph.D.K10/Computer Science/F-T/April 2019)

Under the Guidance and Supervision of

Dr. L. AROCKIAM, M.C.A., M.Tech., M.B.A., CSM., BLIS., M.Phil., Ph.D.,
Associate Professor



PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE
St. JOSEPH'S COLLEGE (Autonomous)
Special Heritage Status Awarded by UGC, Nationally Accredited at 'A++' Grade (4th Cycle) by NAAC
College with Potential for Excellence by UGC, DBT-STAR & DST-FIST Sponsored College
TIRUCHIRAPPALLI - 620 002, INDIA.

JUNE 2022

Dr. L. Arockiam
Associate Professor
Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli - 620 002, India.

CERTIFICATE

This is to certify that the thesis entitled **"RANK ATTACK DETECTION TECHNIQUES FOR THE INTERNET OF THINGS"** submitted by **Mr. A. Stephen,** a research scholar in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli - 620 002, for the award of the degree of **Doctor of Philosophy in Computer Science**, is a record of original work carried out by him under my supervision and guidance. The thesis has fulfilled all requirements as per the regulations of the University and in my opinion the thesis has reached the standards needed for submission. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Date: **(L. Arockiam)**

Place: Tiruchirappalli *Research Supervisor*

A. Stephen
Research Scholar
Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli - 620 002, India.

DECLARATION

I hereby declare that the work embodied in this thesis entitled **"RANK ATTACK DETECTION TECHNIQUES FOR THE INTERNET OF THINGS"**, is a research work done by me under the supervision and guidance of **Dr. L. Arockiam,** Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli - 620 002, India. The thesis or any part there of has not formed the basis for the award of any Degree, Diploma, Fellowship or any other similar titles.

Date: **(A. Stephen)**

Place: Tiruchirappalli *Research Scholar*

DEPARTMENT OF COMPUTER SCIENCE

St. JOSEPH'S COLLEGE (Autonomous)

TIRUCHIRAPPALLI – 620 002

TAMILNADU, INDIA

CERTIFICATE OF PLAGIARISM CHECK

1	Name of the Research Scholar	**A. Stephen**
2	Course of Study	Ph.D., Computer Science
3	Title of the Thesis / Dissertation	**RANK ATTACK DETECTION TECHNIQUES FOR THE INTERNET OF THINGS**
4	Name of the Research Supervisor	**Dr. L. Arockiam**
5	Department / Institution / Research Centre	Associate Professor in Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli - 620 002
6	Acceptable Maximum Limit	10%
7	Percentage of Similarity of Content Identified	5%
8	Software Used	OURIGINAL
9	Date of Verification	01.06.2022

Report on plagiarism check, item with 5% of similarity is attached.

Signature of the Research Supervisor **Signature of the Candidate**

Curiginal

Document Information

Analyzed document	Stephen (1).pdf (D138816705)
Submitted	2022-06-01T13:19:00.0000000
Submitted by	Dorairajan
Submitter email	manavaidorai@gmail.com
Similarity	5%
Analysis address	manavaidorai.stjct@analysis.ouriginal.com

Sources included in the report

W	URL: https://www.annalsofrscb.ro/index.php/journal/article/download/3724/3035 Fetched: 2021-11-13T00:27:07.5100000	19
W	URL: https://arxiv.org/pdf/2011.12996 Fetched: 2021-04-12T12:56:37.9630000	3
W	URL: https://turcomat.org/index.php/turkbilmat/article/download/3707/3174 Fetched: 2021-08-03T14:59:12.1470000	22
W	URL: https://www.researchgate.net/publication/352738207_Attacks_against_RPL_in_IoT_A_Survey Fetched: 2021-10-09T17:09:19.6070000	4
W	URL: https://www.mdpi.com/1424-8220/20/21/5997/pdf Fetched: 2020-11-28T17:06:43.4170000	1
W	URL: https://www.turcomat.org/index.php/turkbilmat/article/download/3020/2596/5703 Fetched: 2021-07-09T20:17:41.3670000	4
W	URL: https://link.springer.com/article/10.1007/s12083-021-01275-3 Fetched: 2022-06-01T13:20:58.7800000	1
W	URL: https://iopscience.iop.org/article/10.1088/1742-6596/1142/1/012009/pdf Fetched: 2019-12-13T10:31:20.1430000	3
W	URL: https://ijict.itrc.ac.ir/article-1-481-en.pdf Fetched: 2022-06-01T13:20:59.1000000	1

ACKNOWLEDGEMENT

With joyful heart and gratitude, I thank **God Almighty** for his accompaniment and showers of blessings throughout the course of this work.

Foremost, I owe my sincere gratitude from the depth of my heart to the respectful Research Supervisor **Dr. L. Arockiam**, Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli. His inspiring nature, scholarly guidance and motivation spurred me to do my research with great zeal.

Beside my research supervisor, I am greatly indebted to my Doctoral Committee members, **Dr. E. George Dharma Prakash Raj**, Assistant Professor, Department of Computer Science and Engineering, Khajamalai Campus, Bharathidasan University, Tiruchirappalli and **Dr. S. Chellammal**, Assistant Professor & Head, Department of Computer Science, Government Arts and Science College, Srirangam, Tiruchirappalli. Their stimulating motivation and valuable ideas helped me to enrich this research work.

I owe a special thanks to **Rev. Fr. Fernando Leonard Nevis SJ**, Rector, **Rev. Dr. K. Amal SJ,** Secretary, **Rev. Dr. Arockiasamy Xavier SJ**, Principal, **Rev. Dr. S. Santiago SJ**, Vice Principal and the Management of St. Joseph's College (Autonomous), Tiruchirappalli for providing me with great research opportunity to pursue the doctoral programme in this esteemed institution with par excellence.

I express my sincere thanks to **Mr. A. Charles**, Head and all the faculty members Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli for providing an ambient research environment in the department.

I sincerely thank **Dr. P.D. Sheba Kezia Malarchelvi**, Professor and Head, Department of Computer Science & Engineering, JJ College of Engineering and Technology, Tiruchirappalli and **Dr. P. Calduwel Newton**, Assistant Professor, Department of Computer Science, Government Arts College, Thiruverumbur, Tiruchirappalli for their support and valuable suggestions.

I would also like to thank all research group members of **Dr. L. Arockiam** and other fellow researchers, my research team **Sr. A. Arul Anitha, Ms. D. Janet Ramya, Ms. S. Sathyapriya, Mr. V. A. Jane** and **Mr. K. Subash** for their valuable suggestions, encouragement and help during the course of my research. It is indeed wonderful experience journeying with them these years.

I also wish to express heartfelt thanks **Rev. Sr. Sahaya Lilly** and **Rev. Sr. Angel**, St. Anne's, Trichy for their prayers and supports.

I thank **Dr. Nisman** Assistant Professor, Christ University, Bangalore and **Dr. Ram Kumar** Assistant Professor, Vishwakarma University, Pune for their research guidance.

My sincere thanks to my father **R. Anthony Cruz**, my mother **A. Amalorpavamary** and my brothers **Arun Kumar**, **Prakash** and **Br. Anthony Raj MSFS** who stood by me and supported me in difficult years.

And also, my special thanks to **INLOVERS** team, Loyola College, Vettavalam and my dear **Friends** for their support.

A. Stephen

ABSTRACT

The Internet of Things (IoT) brings a revolutionary change in the modern computer era. It enables physical objects to connect and communicate with each other. It also connects things to humans, machine to machine and human to machine. They are connected and they communicate directly or indirectly through the Internet. IoT makes human lives much easier. The growth of IoT technology is unimaginable in recent times. IoT technology empowers humans with sensors and other IoT-enabled smart devices. IoT devices are resource constrained and more affordable. IoT devices do all the work efficiently through sensors and actuators. It changes the workstyle of humans by incorporating other technologies such as Artificial Intelligence, Data Mining, Neural Networks and Machine Learning. The performance of IoT systems is much faster than the performance of humans' conventional working methods. The tremendous performance of the IoT in the contemporary world makes it difficult for the user to gauge which technology will rule for another decade. IoT products are becoming more popular, attractive and sophisticated for mankind. Many innovative products are manufactured based on IoT technology. Many corporate companies envision the needs of IoT technology for users in all the fields for the next ten years.

Though the IoT has made significant advances in computer science, it has a number of issues, including data collection, quality of service, security, and privacy. Security plays a vital role in the IoT. There are different types of security in the IoT, like device security, data security and network security. Among these security issues, network security has been thriving recently in research. Rank attacks, hello flood

attacks, wormhole attacks, blackhole attacks, version number attacks, sybil attacks, selective forward attacks and sinkhole attacks are all types of attacks against routing protocols in a network. Out of all these attacks, the rank attack is the most vulnerable attack. In this research, three techniques, such as RSSI based rank attack detection technique (RACE), Level based rank attack detection technique (LEACE) and Location based rank attack detection technique (LACE) are proposed to detect rank attacks in RPL based IoT networks. All three of these techniques are implemented using the Cooja simulator over the Contiki operating system.

The RSSI based rank attack detection technique (RACE) is used to detect the rank attack based on the received signal strength indicator (RSSI) value of a node in the network. The RACE consists of three phases, such as the DODAG construction phase, the TRRX computation phase and attack detection phase. In the first phase, the DODAG is constructed by hop count (objective function). The second phase is used to compute the RSSI value of the nodes in the network. The RSSI value of each node in the network is calculated and stored in the root node. And also, the total RSSI value of a node towards the root node is computed using the intermediator nodes of that node and stored in the root node. In the third phase, the rank attack is detected using the RSSI value of the nodes in the network. The RACE technique is compared with the existing technique called RDAID. The RACE technique works better than the existing technique in terms of packet delivery ratio, throughput and attack detection accuracy. The limitation of the RACE technique is the detection of rank attack in an obstacle environment. Because some problems arise as the RSSI value is not received properly in an obstacle environment.

The Level based rank attack detection technique (LEACE) is proposed to detect rank attacks using a node's level in the network, even in an obstacle environment. In the LEACE technique, the nodes are divided into levels. The level and rank of each node correspond to each other in the RPL based IoT network. The rank and level of the nodes in the network are synchronized with each other to detect rank attacks. The level of a node is verified when a node broadcasts its rank. So, the rank attack is detected when there is an inconsistent change in the rank and level, which are synchronized with each other. The LEACE technique is compared with the RACE technique. The LEACE technique outperforms the RACE technique in terms of packet delivery ratio, throughput and attack detection accuracy. The detection accuracy of rank attacks in RPL based IoT networks has to be improved more. So, the Location based rank attack detection technique (LACE) is proposed to improve attack detection accuracy.

The LACE technique utilizes the location of each node to detect the rank attack. In RPL network, the rank of a child node should be higher than the rank of its parent node. Because the RPL network increases the rank of a node from top to bottom and decreases it from bottom to top. To identify the rank attack, the location of each node has to be calculated. The location of each node in the network is identified by calculating the distance of the nodes towards the root node using Manhattan distance and stored in the root node. The distance of a node is checked when a node publishes its rank. The rank attack is identified when there is an inconsistent change in the rank and distance between a child and its parent. The LACE technique is compared with the LEACE technique in terms of packet delivery ratio, throughput and attack detection accuracy. It performs better than the LEACE technique.

These three techniques are used to detect rank attacks in RPL-based IoT networks. The STARO Framework is proposed to use these rank attack detection techniques efficiently. The STARO framework utilizes all three techniques according to the nature of their behaviour. And the LACE technique is deployed in the smart hostel environment. Thus, deploying the STARO framework provides a rank attack free IoT environment.

LIST OF PUBLICATIONS

International / National Journals

1. **A. Stephen** and Dr. L. Arockiam, "**Attacks against RPL in IoT: A Survey**", Annals of the Romanian Society for Cell Biology, ISSN 1583-6258, Volume 25, Issue 4, pp. 9767-86, 2021, (**Scopus Indexed**).
2. **A. Stephen** and Dr. L. Arockiam, "**RSSI based Rank Attack Detection Technique for RPL**", Webology, ISSN 1735-188X, Volume 18, Issue 6, pp. 5189-5197, 2021, (**Scopus Indexed**).
3. **A. Stephen** and Dr. L. Arockiam, "**Level based Rank Attack Detection Technique (LEACE)**", Turkish Journal of Computer and Mathematics Education, ISSN 1309-4653, Volume 12, Issue 9, pp. 268-272, 2021, (**Scopus Indexed**).
4. **A. Stephen** and Dr. L. Arockiam, "**Location Based Rank Attack Detection Technique (LRADT)**", Webology, ISSN 1735-188X, Volume 18, Issue 5, 2021, (**Scopus Indexed**).
5. A. Arul Anitha, **A. Stephen** and Dr. L. Arockiam, "**A Hybrid Method on Smart Irrigation System**", International Journal of Recent Technology and Engineering (IJRTE), ISSN 2277-3878, Volume 8, Issue 3, pp. 2995-2998, 2019, (**Scopus Indexed**).

CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
6LoWPAN	Internet Protocol version6 over Low power and Wireless Personal Area Networks
ADA	Attack Detection Accuracy
AN	All Nodes in the network
AODV	Ad-hoc On-demand Distance Vector
AODVv2	Ad Hoc On-demand Distance Vector Version2
BAP	Broadcast Authentication using cryptographic Puzzles
Ch	Children
CLAIDS	Cellular Learning Automata based Approach for Anomaly Nodes Detection in Clustered Mobile Ad Hoc Networks
CoPA	Constrained Application Protocol
CRT	Chinese Reminder Theorem
CU	Current node
DAG	Directed Acyclic Graph
DAO	DODAG Advertisement Object
DAO_Ack	DODAG Advertisement Object Acknowledgement
dB	decibel
DCP	DODAG Construction Phase
DEMO	An IDS Framework for Internet of Things Empowered by 6LoWPAN
DIO	DODAG Information Object
DIS	DODAG Information Solicitation

DODAG	Destination-Oriented Directed Acyclic Graphs
DoS	Denial of Service
DSFLACQ	Detection of SFA based on adaptive LA and Communication Quality
E2V	Energy based Validation and Verification
ETX	Expected Transmission Count
FS	File Size
GPSR	Greedy Perimeter Stateless Routing
HC	Hop Count
IBOOS	Identity Based Offline – Online Scheme
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IMn	Inter Mediator node
INTI	Intrusion detection of siNhole attack on 6LoWPAN for interneT of thIngs
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LA	Learning Automata
LACE	Location based Rank Attack detection technique
LAN	Local Area Network
LEACE	Level based Rank Attack detection technique
LLNs	Low power and Lossy Networks

LOADng	Lightweight On-Demand Ad hoc Distance Vector Routing Protocol
LoRa	Long Rang
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrow Ban IoT
NBnodes	Neighbor nodes
NFC	Near Field Communication
NHC	Number of hop count
NPMT	Neighbour Passive Monitoring Technique
NR	Neighbour nodes
NS2	Network Simulator version2
OF	Objective Function
OLSR	Optimized Link State Routing Protocol
OLSRv2	Optimized Link State Routing Protocol version2
PAN	Personnel Are Network
PDR	Packet Delivery Ratio
PKE	Public Key Encryption
Pnode	Parent node
RA	Rank Attack
RACE	RSSI based Rank Attack Detection Technique
RADP	Rank Attack Detection Phase
RDAID	Rank Decreased Attack Identification
RFC	Request for Comment
RFID	Radio-Frequency Identification
RIA	Rank Increased Attack

RIDES	Robust Intrusion Detection System
RK	Rank of a node
RNode	Root Node
ROA	Rider Optimization Algorithm
RPL	Routing Protocol for Low Power and Lossy networks
RSA	Rivest Shamir Adelemen
RSSI	Received Signal Strength Indicator
RT	Root node
SA	Sybil Attack
SAD-EIoT	Intrusion detection system to detect sinkhole attack in Edge based Internet of Things
SBIDS	Sink Based Intrusion Detection System
SVM	Support Vector Machine
SEER	Simple Energy Efficient Routing
SFA	Selective Forwarding Attack
SOC-M2M	Self-Organized Clustering - Machine-to-Machine
SRPL	Secure RPL
T-IDS	Trust based Intrusion Detection System
TN	True Negative
TORA	Temporally Ordered Routing Algorithm
TP	True Positive
TPR	Total number of Packets Received by the receiver
TPS	Total number of Packets Sent by the sender
TRAIL	Trust Anchor Interconnection Loop

TRCP	TRRX Computation Phase
TRRP	Total RSSI value from Root node to parent Node
TRRX	Total RSSI value from Root node to current Node
TT	Transmission Time
VeRA	Version number and Rank Authentication
W3C	World Wide Web Consortium
Wi-Fi	Wireless Fidelity
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Network
Xnode	Current Node
ZRP	Zone Routing Protocol

Chapter – 1

Introduction

CHAPTER - 1

INTRODUCTION

1.1 Overview

Internet of Things (IoT) is a magic word which creates the magic world through the automation system. In the IoT system, anything can be connected through the Internet. The typical things become Internet of Things when they are connected and communicated through the Internet. Millions of objects can be connected through the IoT technology [Gup, 20]. Several communication technologies are used to connect the objects in IoT. And different types of communication models are used in IoT based on the needs of the users. IoT attracts everyone by its unique characteristic of twenty four hours services at anywhere.

IoT technology is emerging in all the fields throughout the world [Jia, 21]. Though, it emerges in all the fields, it does not have any standard architecture. The architecture may vary based on the requirements of the users concerned with the applications. IoT is used in many applications throughout the world and IoT makes the hard work into smart work through the automation processes [Asi, 21]. IoT applications reduces the human works by connecting things into one system. Since, things are connected and communicated through the Internet, there are many issues and challenges while using the IoT. Among the issues, security is the major issue in IoT [Fad, 17]. Among the security issues, network security is the most notable one. Attacks in Routing Protocol for Low power and Lossy Networks (RPL) is a salient issue in IoT network.

In this Chapter, the basic concepts of IoT such as definition of IoT, characteristics of IoT and communication technologies in IoT are detailed clearly. IoT architectures,

IoT applications, issues and challenges in IoT, routing protocols in IoT and attacks in RPL protocol are discussed. This chapter provides the fundamental knowledge to understand the purpose of this research work.

1.2 Basic Concepts of IoT

1.2.1 Definition

The term IoT was coined by the Kevin Ashoton in 1999 [Kev, 09]. The IoT was used in the supply chain management with Radio Frequency Identification (RFID) tags at the first time [Neh, 19]. Internet of Things is a technology which connects physical and virtual things by the Internet. The connected things in the IoT have their specific identities in the network. Things are communicated with each other using their unique ID. The things connected in the IoT environment can collect data using various sensors. The IoT technology is used worldwide because of its unique characteristics.

1.2.2 Characteristics of IoT

The unique characteristics of IoT make the technology the best among other technologies. The characteristics of IoT attracts the users to use IoT technology in all the fields in the world. The Figure 1.1 shows characteristics of IoT.

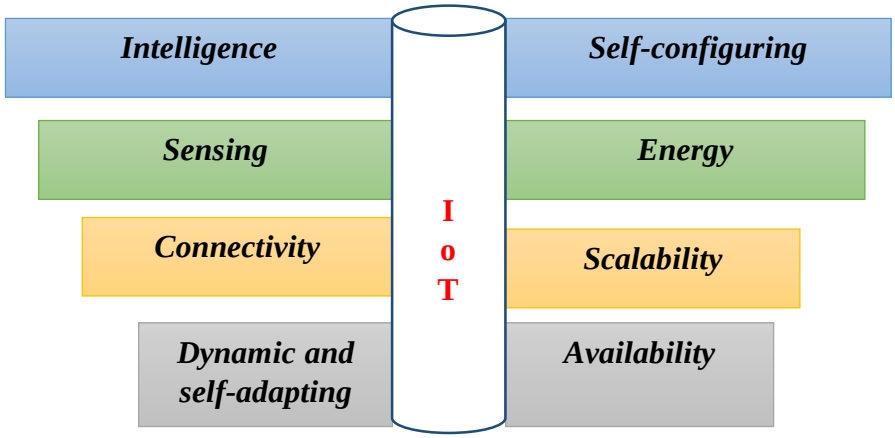


Figure 1.1 Characteristics of IoT

Intelligence: IoT has the intelligence system which makes the hardest work into smartest work. The intelligence system in IoT extracts the knowledge from the collected data using the sensors [Dee, 19]. Based on the needs of the conditions given in the IoT system, the intelligence provides the services.

Sensing: The sensing characteristics plays the major role in the IoT technology. The sensing process is done in the physical layer. Different types of sensors are used based on the requirements of the applications [Sil, 20]. Sensors sense the data based on the condition given in the IoT system. The sensing characteristics is used for gathering the data and generating the output based on the gathered data [San, 21].

Connectivity: The connectivity characteristic makes sure the connections between all things in the IoT system. IoT connects millions of physical and virtual things using their distinct identification [Jie, 20]. The connection of all the things makes the human more comfortable. All the things are communicated through the connections in the IoT environment.

Dynamic and Self-adapting: IoT is a dynamic system which adapts the environment based on the needs of the services for the users. The dynamic and self-adapting characteristics are the major key factors for making decision in an IoT environment [Mah, 17b].

Self-configuring: IoT enables self-configuring process in the connected network. The self-configuring characteristic allows all devices such as sensors, network devices and other devices to work together to complete the tasks given for the system. It automatically configures the latest upgradation for the IoT system [Key, 16].

Energy: IoT uses less energy to complete the tasks. IoT devices consume less energy to perform their given jobs. This special character makes the users to go with IoT technology to save power and reduce the cost for the power supply [Bha, 21]. Many corporate companies utilize the energy characteristic and make several energy efficient IoT products.

Scalability: IoT has the ability to scale up in all the dimensions such as hardware, software and performance of the system. It gives special attention among other technologies in terms of increasing and decreasing the sources based on the requirements of the users [Dam, 20].

Availability: IoT provides services at any time at anywhere [Yus, 19]. Since the system is connected through Internet, all the services can be given at any time based on the requirements of the users [Abh, 19].

1.2.3 Communication Technologies in IoT

Various communication technologies are used in IoT network to communicate efficiently with IoT devices connected in the network [Nas, 20].

Near Field Communication (NFC): NFC is the near field communication technology. NFC uses radio frequency for communication process. NFC's function is categorized into three ways firstly touch and go, secondly touch and confirm and thirdly touch and connect. It is a short range communication technology. The NFC enabled devices can communicate within few centimeters. In the beginning of this communication technology, NFC was used in mobile devices only [Swa, 20]. But after the growth of the IoT technology, NFC is used in many applications such as banking, logistics, ticketing, transport cards and health care.

Radio Frequency Identification (RFID): Radio frequency identification communication technology uses RFID labeled tags for communications. In an early stage, it was used to track the objects. But nowadays, RFID is used with IoT technology for various purposes such as payment, logistics, library system, colleges and schools Enterprise Resource Planning (ERP) system and asset management system [Pao, 21]. RFID communication technology can work only within 10 cm to 200 m.

Bluetooth: Bluetooth is the wireless communication technology used to share data through electronic devices. The technology uses master and slave method for sharing the communication. The Bluetooth enabled devices can communicate with each other once they are paired with one another [Jue, 19]. It is mostly used in Personnel Area Network (PAN). The communication range for the Bluetooth technology is ten to hundred meters. Bluetooth with IoT enabled devices are used in many applications like smart health, smart home, smart class room and public transportations.

Wireless Fidelity (Wi-Fi): Wi-Fi communication technology is used in Local Area Network (LAN). Compared with Bluetooth, it has maximum communication range. The communication range of Wi-Fi is up to hundred meters. Internet can be easily accessed through Wi-Fi communication technology. It provides flexibility to use the Internet within its communication range. The most IoT enabled devices uses Wi-Fi for the communication. Because, Wi-Fi is the best communication technology for mobile devices [Ann, 18].

ZigBee: It is used in creating Personal Area Network (PAN). It is mostly used in industrial side as well as in the medical line because it provides very long battery life. It supports good number of nodes to be connected under single communication

network [Sus, 19]. It covers up to thirty meters. It is used in many IoT applications which required long life battery feature.

Z-Wave: It is low power radio frequency communication technology. It is mostly used in home automation [Tar, 17]. There are lots of Z-wave enabled devices invented especially for the smart home. Communication range of Z-Wave is up to hundred meters.

Long Rang (LoRa): It is long range and low power communication model. It is used in wide area network [Qih, 19]. Among other low power communication technology only LoRa has maximum communication coverage. Many LoRa is utilized in many IoT applications for communicating IoT network even in the long range. The communication range of LoRa is up to ten kilometers.

Narrow Ban IoT (NB-IoT): NB-IoT is broadly used and fast growing low power communication technology. It is used in several IoT applications especially for the commercial products. It has long life battery capacity. It works excellently in indoor environment. Massive number of connections can be established though NB-IoT [Abd, 21].

SigFox: It is one of the low power communication technologies which is used to scale up the connectivity in the IoT applications. This communication technology is very reliable in the communication process. It is cost efficient technology. Many researchers are using SigFox in IoT based indoor and outdoor localization applications [Kai, 18]. The communication range of SigFox is forty kilometers.

1.3 IoT Architecture

There is no standard architecture for IoT [Mar, 21]. Based on the needs of researchers the IoT architecture varies. IoT provides diverse applications in all the

fields. At the early days of IoT lifestyle, only three layer architecture was used which was proposed by Internet Engineering Task Force (IETF). The usage of IoT technology is increased day by day in the modern world. The IoT architecture is also got transformation from three layer architecture into four layer architecture and five layer architecture based on the requirements of the users. In future, the architecture may get newer version according to the necessity of the modern lifestyle. Figure 1.2 illustrates the three types of IoT architectures [Muh, 18].

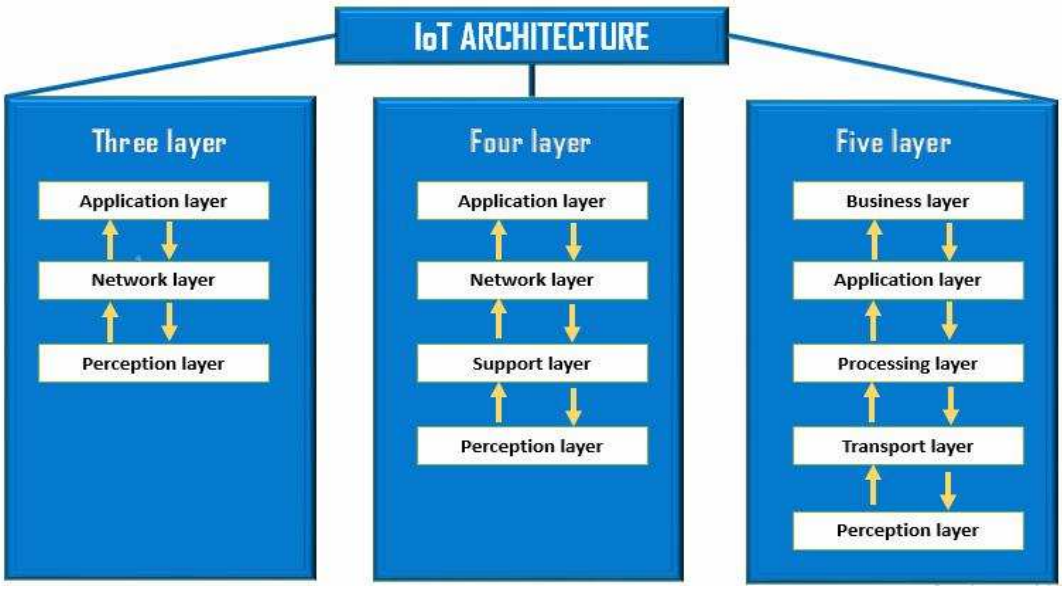


Figure 1.2 IoT Architectures

1.3.1 Three Layer Architecture

Three layer architecture is the first layer architecture which was proposed by the IETF. This is the base architecture for other architectures in IoT. The layers in the three layer architecture are perception layer, network layer and application layer. The three layers in the architecture do their unique jobs to form IoT networks.

Perception Layer: It has the responsibilities to monitor the physical objects in the IoT network. All the physical objects such as sensors, actuators and other connecting

objects lie in the perception layer. Data collection and objects monitoring works are done through the perception layer using the sensors.

Network Layer: It helps to connect the things in the physical layer through various network device and servers. The connected things are communicated via different communication technologies. It is used to transmit and process the collected data in the IoT network.

Application Layer: This layer acts as the interface between the user and the objects in the IoT network. It is used to provide application specific services to the users. Many IoT application are created in two different ways like mobile applications and web applications. The raw data collected from the perception layer is processed though network layer and is delivered through application layer as service.

1.3.2 Four Layer Architecture

In four layer architecture, only one layer is added additionally. The layer which is there in the four layer architecture and not there in the three layer architecture is the support layer. Works of the other layers such as perception layer, network layer and application layer are same with the three layer architecture. In this section, only the support layer is discussed.

Support Layer: The support layer provides the confirmation that the information is sent by the legitimate (authentic) users or not. It also confirms that the sent data is protected from threats. It has major responsibility like authentication of the data in the four layer architecture.

1.3.3 Five Layer Architecture

In five layer architecture, the two layers such as perception layer and the application layer are same, compared with three layer and four layer architectures. Three layers namely transport layer, processing layer and business layer are different from other two architectures. This section details only the transport layer, processing layer and business layer.

Transport Layer: It takes the responsibility of transferring the sensor data to the next layer through communication technologies such as RFID, NFC, Wi-Fi and other technologies. Once the data is collected in the perception layer using sensors, the transport layer starts the transmission of the collected data to the concerned layer.

Processing Layer: This layer plays a vital role in five layer architecture. It is used to process the stored data using various processing techniques. After processing the data, the data is analyzed using the analytical and statistical methods. Cloud computing provides for storing and processing data in five layer architecture. Machine learning and big data techniques are also used for processing and analyzing the data efficiently.

Business Layer: The business layer makes the IoT services into business through different applications that are needed in the contemporary world. It is responsible for making the profit models in the IoT system and also it manages the users' policy while making the profit models.

The work of the IoT architecture is same in all three types of layered architecture. But the layers are divided and given some specific jobs to process within the layer. Even though, there are many types of layer architecture available for IoT technology, the three layer architecture is the base of all architecture.

1.4 Applications of IoT

IoT emerges very fast and no other technologies pace with IoT growth and its vast applications in the recent years. IoT utilizes all the technologies and provides the best IoT enabled applications to the users [Goy, 21]. The applications of IoT are much needed in the present times. Automation process in the IoT applications draws all the people's attention towards IoT technology. There are many IoT applications available, but in this section only the most used applications are discussed. Figure 1.3 presents the most used IoT applications.

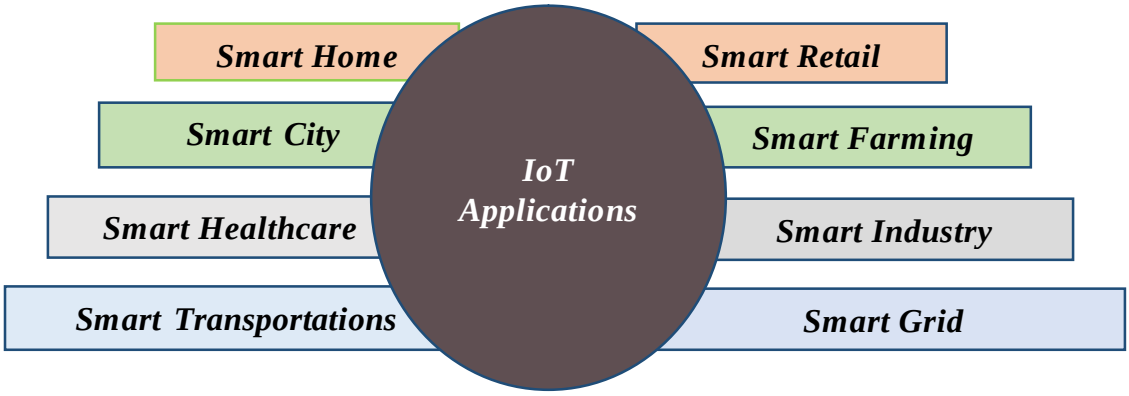


Figure 1.3 Applications of IoT

Smart Home: The most used IoT application over the world is smart home. All the physical objects in a home are connected and communicated with each other. Smart light is turned on automatically when people enter into the house or room. It saves the energy and reduces the electricity cost. Smart appliances like refrigerator, television, washing machine coffee makers can communicate with each other in the smart home [Cri, 21]. It provides security for the home by monitoring the home using cameras and security alarming system.

Smart City: In the smart city, the city is controlled by the IoT enabled system. It provides smart street light which saves the energy, smart garbage system, monitoring

the city which provides security to the city, tracking all the city's moveable and immoveable assets and connecting the city offices to provide better service to the city's people [Abb, 21].

Smart Healthcare: It provides enormous services to the patients. Health conditions of all the patients are monitored by different sensors and wearable IoT enabled devices. The health conditions of the patients are sent periodically to the Doctors automatically. The Doctors can give instant medication to the patients with help of IoT system in the healthcare. In smart health care, doctors no need to carry any manual records to check patient's conditions. Because, everything is digitalized [Tra, 21]. It reduces the risky situation and death cases in healthcare.

Smart Transportations: It provides many smart services through IoT system. The smart transportations give hassle-free journey to the passengers, because everything is monitored and controlled perfectly. The services given under the smart transportations are accident free journey, automatic ticket collection, smart parking, location tracking, emergency notification system, and traffic free journey [Abb, 21].

Smart Retail: In retail industries, the IoT technology is used for both large scale as well as small scale retail. It improves the overall performance of the retail [Kun, 21]. It is used for supply chain logistic management system in retail by tracking and monitoring things [Sha, 21]. It analyses the customer satisfaction level on each products. It also prevents the product breakage. It is used in food safety monitoring system by maintaining the temperature of the storage cabins.

Smart Farming: IoT does many wonders for the farmers through smart farming. The smart farming reduces the manual works of the farmers. The smart farming system

increases productivity compared with the traditional farming [Abh, 20]. The smart farm is maintained and monitored by sensors and cameras. So, it efficiently uses the farming sources such as water, electricity and fertilizer according to the needs of the crop. It includes automated pesticide, smart irrigation, disease identification and field monitoring such as humidity, temperature and soil moisture [Sob, 20].

Smart Industry: All the industries are started to use IoT based smart industrial process. It reduces the human resources and saves the money. It connects all the technologies such as Artificial Intelligence, Cloud Computing and Data Analytics under one system and dynamically works together to complete the tasks [Moh, 20]. It helps the workers to work safely with the help of security monitoring system. It optimizes the production process and reduces the workload of workers in the industry. It saves energy and reduces the electricity cost and maintenance cost.

Smart Grid: The smart grid system works better than the conventional grid system [Bha, 20]. The smart grid system is controlled and monitored through sensors and IoT enabled devices. It reduces energy wastage and increases energy supply chain [Hos, 19]. It prevents from the power leakage problem and provides secure and safe environment to work in the grid system [Son, 21]. Smart grid is formed in many fields like retail stores, educational institutions, hospitals and corporate companies.

1.5 Issues and Challenges

The outcomes of the IoT technology is incredible. But, in one hand, the IoT technology is growing more and more in all the fields and in the other hand, the issues in IoT also increasing a lot [Tin, 20], [Vip, 17]. The issues and challenges are the headache of the IoT technology. The major issues and challenges are as follows.

Internet Outage: All the things in IoT system are connected through the Internet. If there is Internet outage in the IoT environment, the system cannot work. The IoT connection should be there in both sides like the request point and the response point. If the IoT system gets internet connection either by the request point or the response point, the task cannot be completed. It has to wait till both the ends get the Internet connections. The Internet outage issue puts the users in a big trouble.

Lightweight: IoT is a light weight technology. IoT devices have only limited power and limited storage capacity. IoT devices have to get energy periodically to be connected in the network. Since, IoT has limited storage, high amount of data cannot be stored in IoT devices. Even it cannot use the heavyweight algorithms for processing or security purpose. It supports only lightweight resources.

Connectivity: IoT technology is being used worldwide. The IoT devices are increasing day-by-day throughout the world. It is capable of connecting millions of devices under one system but reliability of the connections are not ensured for the users. Connecting all the devices through the world is quite difficult due to limited bandwidth and other problems in the networks.

Big Data: Millions of devices are connected to IoT network. All the devices are generating data every second, hence the data becomes big data. The IoT system struggles to handle such amount of data. So, handling the big data in IoT network with light weight technologies is not so easy [Rah, 20]. Cloud technologies are utilized to handle the big data.

Privacy: It is one of the major issues in IoT. Though, IoT technology admires all the people in the world by its fabulous services to the people, everyone worries how to

get rid from the privacy issues. In the connected world everything can be tracked, even the human beings too. And all the sensitive data are stored in the cloud which is third party [Nar, 20]. The sensitive and the confidential data can be hacked. So, the effective privacy policy cannot be expected while using IoT technology.

Security: Security is major concern in IoT network. In IoT system, all the security issues are notable such as data security [Miz, 17], device security and network security [Iev, 19]. Data can easily be tampered by the hackers. Because, all the data are being stored, communicated and processed via the Internet. The IoT devices face lots of security consequences such as virtual device cloning, and illegitimate controls over the IoT devices. Among all these issues, network security is the most prominent one. The IoT network has to be secured from the attacks by intruders. If the IoT network security is broken, the intruders can get access to the entire IoT system. To prevent from these issues, the network routing protocols must be secured. Because the routing protocols play major role in IoT technology.

1.6 Routing Protocols

Routing protocol is used for constructing optimal path to communicate and transfer data in the IoT networks. IoT routing protocols are responsible for finding and providing the suitable path to the nodes in the network based on the needs of the nodes. The efficient routing system does not worry about the accumulation of data in IoT environment. Efficient routing process gives effective outcomes in the network. There are three types of routing protocols used in IoT network such as reactive protocol, proactive protocol and hybrid protocol [Amo, 16].

Reactive Protocol: It is also called as on demand routing protocol. It makes path based on the requirements of the nodes in the network. It creates routes when source needs to send the data to the destination [Amo, 16].

Proactive Protocol: It maintains the routing table for the network. The routing information is periodically updated in the routing table. The paths are created based on the routing table for each node in the network [Amo, 16].

Hybrid Protocol: It is the combination of both reactive and proactive protocols [Amo, 16].

Table 4.1 lists the routing protocols used in IoT network.

Table 1.1 Routing Protocols in IoT

S. No.	Reactive Protocol	Proactive Protocol	Hybrid Protocol
1	AODV, AODVv2	OLSR and OLSRv2	ZRP
2	LOADng	Routing Protocol for Low Power and Lossy Networks (RPL)	SOC-M2M
3	TORA	GPSR	-
4	SEER	-	-

The protocols listed in table 1.1 are most used routing protocols in IoT network. Among all the protocols, proactive protocol works better in difficult IoT environment. Because, it maintains routing information and it is easy to solve any issues in the network by getting information from the routing table. In proactive protocols, issues in the RPL protocol research is done by many researchers.

1.7 Routing Protocol for Low Power and Lossy Networks (RPL)

RPL is designed for Low-power and Lossy Networks (LLN). It is distance vector routing protocol. It is a resource constraint protocol which uses low power, low

memory and low battery lifetime. It supports point to point, point to multipoint and multipoint point to point network traffic methods. It has two mode such as storing mode and non-storing mode. In storing mode each node stores the routing information. Storing mode may cause shortage of memory in routing table [Bar, 18]. Because, it accumulates the routing information in the table. The non-storing mode stores the routing information in root node itself. Non-storing mode creates more traffic in a network. Because, every request is directed towards the root node only. RPL uses Directed Acyclic Graph (DAG) topological method. RPL is the destination oriented protocol. So, it makes Destination Oriented Directed Acyclic Graph (DODAG) to create a network.

Objective Function (OF) is used for constructing the DODAG in IoT [Han, 19]. OF is also used to select and optimize routes in network. The most used objective functions are expected transmission count (ETX), hop count (HC) and energy. RPL uses four types of control messages to manage RPL network. Figure 1.4 illustrates the format of the RPL control message [RFC 6550].

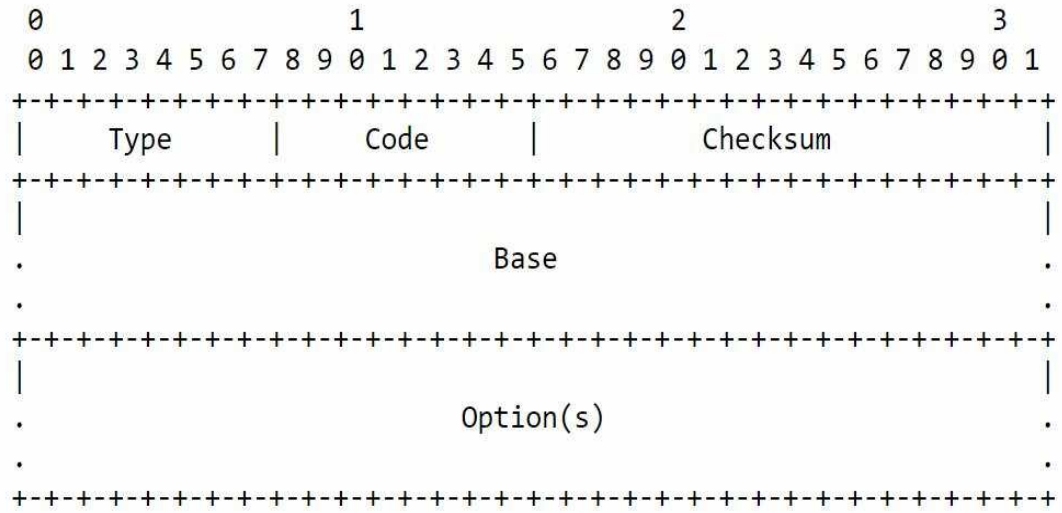


Figure 1.4 RPL Control Message Format

In figure 1.4, the "Type" is used to refer which type of message such as DODAG Information Object (DIO), DODAG Information Solicitation (DIS), DODAG Advertisement Object (DAO) and DODAG Advertisement Object Acknowledgement (DAO_Ack). All types of control messages have their specific code. It is mentioned in "Code" section in the control message. The "Checksum" is used to provide security mechanisms. The "Base" holds the fundamental information about the functions of the carried object. The "option(s)" is body of the message. Figure 1.5 shows the RPL construction process.

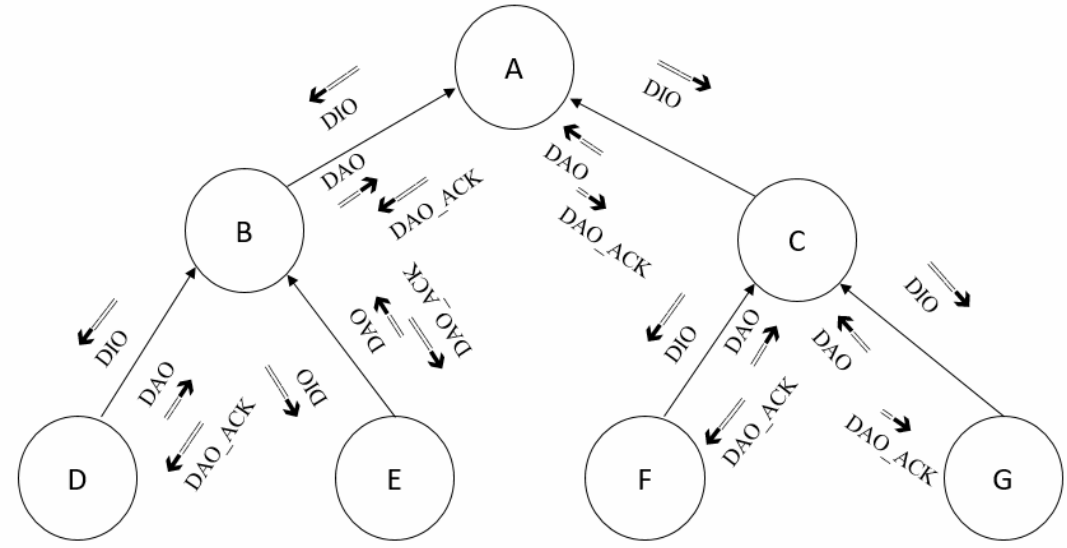


Figure 1.5 Construction of RPL Network

DODAG Information Object: In RPL network, the DIO control message is used to broadcast the fundamental information such as RPL instance ID, DODAG version number, rank and DODAG ID of a node in a network. Each node in a network periodically multicasts the DIO message in the IoT environment. The nodes which are near to the concerned node which multicasts the DIO message, receive the DIO message and utilize the DIO message.

DODAG Advertisement Object (DAO): The DAO message is unicasted to a node in the RPL network to advertise about itself that the node is closer to it to connect as a child. The DAO is sent only by the node which receives DIO message in the network.

DODAG Advertisement Object Acknowledgement (DAO_Ack): It gives acknowledgement to a node which sends the DAO message to the node. Once the node receives the DAO message, the concerned node sends the DAO_Ack control message to the child node.

DODAG Information Solicitation (DIS): DIS message is used to solicit the information about which node is near to connect to the RPL network. The objective function of the soliciting node should be the same with node which is near to the network. If the objective function is same for the two nodes then the node is connected with RPL network. Otherwise the node is floated.

In the RPL network, many issues are occurring like less quality of service, attacks against RPL network and managing the RPL control messages. Among all these issues, attack against the RPL is the predominant issue. Many researches are done to provide solution for the attacks in RPL network.

1.8 Attacks against RPL Protocol

Various attacks such as blackhole attack, hello flood attack, rank attack, selective forward attack, sinkhole attack, sybil attack, version number attack and wormhole attack occur in RPL [Mar, 19]. Each attack affects the RPL network in different ways.

Blackhole Attack: In a blackhole attack, the attacker node attracts the neighbour nodes by advertising that it has shortest path to the destination. It does not forward the received packets to the destination [Sho, 18]. The main aim of the blackhole attack is to drop packets and make traffic in the network [Bha, 19].

Hello Flood Attack: The node affected by the hello flood attack is broadcasting the hello message unnecessarily in the network. The unwanted hello messages create the traffic in the IoT network. The hello message increases periodically and makes the flood using the message [Adi, 20]. And finally the network struggles to respond to the requests. It also reduces the nodes energy by keep on sending the hello messages.

Selective Forward Attack: It is an attack where the malicious node selectively drops the packets and send the message [Fat, 17]. It is a deterioration condition in the network for getting the entire packets received by the adversary node [Sur, 19]. It reduces the efficiency of the performance of the network.

Sinkhole Attack: The sinkhole attack broadcasts the bogus information to all the neighbour nodes including nodes which are very closer to the root node to attract the nodes in the network. It claims that it has shortest path to reach the destination node. The attacker node compromises all the other nodes by its fake information and makes the other nodes to send messages towards itself. It creates traffic in the RPL IoT network. It can easily modify or drop the packets in the network [Sum, 20].

Sybil Attack: In sybil attack, the attacker node generates fake identities to pretend like other nodes in the network at the same time. It breaches the security of the IoT network. It reduces the performance of the whole network system [Mia, 18]. It affects the network directly as well as indirectly by compromising the nodes in the network.

Version Number Attack: In version number attack, the malicious node illegitimately changes the DODAG version number. It increases the DODAG version of a node illegitimately in the network. It cannot be solved locally in the network. Because, it is global repair related attack [Ahm, 20]. It generates traffic in the network by compromising

nodes by increasing the DODAG version number. The attack leads to control message overhead and reduces the lifetime of the node in the network.

Wormhole Attack: This type of attack is very difficult to identify in an IoT network. It creates a tunnel for getting the information of nodes illegitimately. It gets the confidential information through the tunnel called wormhole. The confidential data is captured and sent through the tunnel by the compromised nodes [Nan, 20].

Rank Attack: The rank of a node increases from top to bottom and decreases from bottom to top in RPL network. The rank of a parent node must be lower than the rank of its child nodes in the network. If there is an inconsistent change in the rank then it is called as rank attack. In the rank attack, the attacker node changes its rank and broadcasts in the network [Abd, 20]. The rank attack is classified into two types such as rank increased attack and rank decreased attack. In rank increased attack, the malicious node increases its rank and broadcasts. In the rank decreased attack, the malicious node decreases its rank and broadcasts. The rank attack reduces the packet delivery ratio, creates network traffic and reduces the performance of the network. Among these attacks rank attack is the most severe attack. It makes many issues in the RPL network in an IoT environment.

1.9 Motivation

IoT is one of the leading technologies worldwide. The growth of IoT is noted one around the world in a short time. It provides more sophisticated environment to the user. Every one desires to use the IoT technology for its comfort zone feature. It makes the hard work into smart work by the automation process. The automation process is done with the help of various sensors and the network devices. In the IoT

environment, network does the prominent work for connecting the things as one system. Since, IoT network is connected in the Internet, there are lots of possibility for the vulnerability in the network. Especially, there is more vulnerability in the routing protocol. From all these issues, attacks in the RPL network is most wanted research in the field of IoT. It motivates to choose any one of the attacks against RPL network for this research.

1.10 Problem Definition

One of the most wanted and emerging technologies in worldwide is Internet of Things. Millions of devices are connected using the Internet and communicated with each other. IoT does not have any standard architecture. Based on the application and the requirements of the users the architecture varies. But the three layer architecture is widely accepted architecture by most of the IoT researchers. Many issues are raised in the each layer. But, attacks in network layer is the most severe issue in the IoT network. From these issues, the attacks against RPL protocol in IoT is the recent needed research. Among several attacks such as blackhole attack, hello flood attack, sinkhole attack, sybil attack, version number attack, wormhole attack and rank attack in IoT, rank attack is chosen for the research. Because, rank attack causes high traffic, high packet loss and other unauthorized access. Many researches have been done to provide solution for the rank attack. But, there is a need to provide better technique to detect rank attack to increase the attack detection accuracy in the IoT network.

1.11 Aim and Objectives

The aim of this research is to propose rank attack detection techniques and increase the detection accuracy of the rank attack in RPL based Internet of Things. The following are the objectives to accomplish the aim of the proposed research.

- To propose Received Signal Strength Indicator (RSSI) based rank attack detection technique (RACE) to eliminate malicious nodes and increase detection accuracy.
- To propose Level based rank attack detection technique (LEACE) to eliminate malicious nodes and increase detection accuracy.
- To propose Location based rank attack detection technique (LACE) to eliminate malicious nodes and increase detection accuracy.
- To propose STARO Framework for smart hostel with rank attack free environment.

1.12 Scope of the Research

Three layer architecture is the base architecture for all other IoT architectures. So, three layer architecture is taken for the research. In the three layer architecture, the attacks in network layer is selected. RPL network in IoT has gained more attention in recent time in the IoT research. Though, several attacks affect the RPL network, the rank attack affects more than other attacks. The rank attack reduces the packet delivery ratio, consumes high energy, and creates high traffic and congestion in the RPL network. Techniques to detect rank attack in RPL network are required. So, scope of the research work is narrowed down to propose techniques to detect rank attack in RPL based IoT networks.

1.13 Organization of the Thesis

The thesis is organized with seven chapters. The organization of the thesis is as follows:

Chapter 1 explains the fundamental concepts of Internet of Things such as definition of IoT, applications of IoT, Characteristics of IoT, issues in IoT, importance of routing, types of routing protocol and attacks against RPL protocol. It provides enough knowledge to understand the background of this research work.

Chapter 2 describes the related works concerned with this research work. It exposes various researches done by the researchers connected with attacks against routing protocol RPL. This chapter categorizes the existing research works according to attacks. It provides the research road map and how the research work is narrowed down with the specific issue.

Chapter 3 proposes Received Signal Strength Indicator based rank attack detection technique (RACE) in RPL network. The proposed work utilizes the RSSI value of each node in the network to detect rank attack. The technique is simulated in Cooja Simulator over Contiki operating system. The proposed work is compared with the existing RDAID technique. The proposed technique work better than the RDAID technique in terms of attack detection accuracy, packet delivery ratio and throughput.

Chapter 4 introduces level based rank attack detection technique (LEACE) for RPL based IoT network. In this work, the level and the rank of each node in the network is given the correspondence connection with each other. A node which has same rank and level value is stored separately. For detecting the rank attack, the correspondence of the level and rank of a node is verified. This work is compared with the RACE technique. It outperforms RACE technique.

Chapter 5 recommends location based rank attack detection technique (LACE) for RPL networks in IoT environment. In this technique, each and every node's location is identified by calculating the distance of a node towards the root node. The Manhattan distance is used for calculating the distance in the network to identify the node's location. The LACE technique is compared with earlier work LEACE. The LACE technique works better than the LEACE technique.

Chapter 6 proposes STARO Framework to provide rank attack free RPL network in IoT environment. The framework utilizes the three techniques such as RACE, LEACE and LACE to make rank attack IoT environment. It selects the appropriate technique based on the obstacle and obstacle free zone. The STARO Framework is deployed in smart hostel with five nodes. It gives rank attack free smart hostel atmosphere.

Chapter 7 concludes the research work by epitomizing essence of the entire research work. It expounds all the three proposed techniques and framework with their pros and cons. It explains the key concepts and the usage of the each techniques.

1.14 Chapter Summary

Internet of Things is the most needed technology throughout the world which provides comfort zone for the users. The automation system in IoT makes the comfort zone. It inclines researchers to do research on IoT. This chapter explodes the fundamental concepts of IoT such as definition of IoT, characteristics of IoT, communication technologies in IoT, IoT architecture, applications of IoT, issues in IoT, routing protocols and attacks in routing protocols. The scope, aim and objectives of this research is described in this chapter. The next chapter explains the related works and highlights the issues and challenges connected with IoT especially routing protocols.

Chapter – 2

Review of Literature

CHAPTER - 2

REVIEW OF LITERATURE

2.1 Introduction

Internet of Things (IoT) is the platform where things/devices connected together to communicate with each other through Internet at anywhere and anytime. These things are embedded with hardware and software [Olu, 21]. IoT provides ambient intelligence system for sensing, actuating and interacting with connected devices [Far, 20]. For sharing the sensitive data securely, the communication network must be secured in IoT. So, secured routing plays an essential role in IoT network. IoT uses many protocols for routing. Routing Protocol for Low power lossy networks (RPL) is one of the routing protocols in IoT [Zah, 20a]. Intruders subject over the RPL based communication to devastate the network. Different types of attacks are eventuated in RPL based network which cause peculiar behavior in IoT environment. There is no adequate proficient techniques available to overcome the RPL based attacks.

Security plays predominant role in IoT. Each layer in IoT is prone to be vulnerable in certain circumstances. So, IoT security gate-crasher can easily attack the IoT system. The attacks could be active or passive and they could be induced by internal source or external source. Active attacks modify the legitimate messages whereas passive attacks only loot the data [Mir, 17].

This chapter describes IoT security issues and various techniques, methods and algorithms to detect and mitigate various attacks against RPL protocol. It covers different aspects of RPL based secure routing mechanisms. The major purpose of this chapter is to examine and analyze the research issues and challenges over RPL based Internet of Things. It provides knowledge on types of attacks against RPL.

2.2 Related Work

2.2.1 Overview on Internet of Things and RPL

IoT

Linus Wallgren et al. [Lin, 13] described the overview of IoT technologies and routing attacks. The network protocols such as IPv6 over Low-Power Wireless Personal Area (6LoWPAN), Constrained Application Protocol (CoPA/COAPS) and RPL were clearly discussed. The concept behind Intrusion Detection System (IDS) in IoT was explained. The attacks against RPL namely selective forwarding attack, sink hole attack, hello flood attack, wormhole attack, clone ID and sybil attack were described, checked and implemented using Contiki and Cooja simulator.

Eleonora Borgia et al. [Ele, 14] elucidated the key features, driving technologies, research challenges and open issues of Internet of Things (IoT). The different phases of IoT such as collection phase, transmission phase, process, management, and utilization phase were clearly explained with a proper diagram. The technologies used in IoT and their capabilities, data rate and the maximum distance for communication were discussed. IoT applications in industrial domain, logistics and product life time management, agricultural and breeding, smart city and smart home, smart grid, public safety and environment monitoring, health and well-being domain, smart medical and independent living were described. The technologies used in IoT were stated out with their unique functionalities.

Hafizur Rahman et al. [Haf, 16] described the components of Internet of Things. The challenges and the research opportunities were clearly explained. Heterogeneity in IoT was explained in terms of operating condition, functionalities, hardware platform, service pattern, implementation, interaction mode and the interoperability. Different

types of interoperability were depicted namely technical interoperability, syntactic interoperability, sematic interoperability, pragmatic interoperability and organizational interoperability. Scalability in IoT, cloud and servers intervention in IoT, network and communication used in IoT were neatly pictured. The security and privacy issues were discussed. Quality of services in accordance with resource constraint devices, traffic load, data redundancy, scalability, fault tolerance, heterogeneity, multiple receivers and real time requirements were explained.

Gordana et al. [Gor, 16] addressed the Internet of Things architectural frameworks that is given by the various standard organization like IEEE, ISO, W3C, ITU and 3GPP. The design issues with regard to Internet of Things hardware (TeloseB, MICAz, OpenMote, Waspmote, Raspberry pi, Arduino Uno, Intel Galileo) and software (TineyOS, Contiki, FreeRTOS, RIOT OS, and Open WSN) were chewed over in detail. OpenMote platform was tested with industrial Internet of Things (IIoT). The existing IoT applications like smart city, medical and health care, agriculture and Nano-scale applications were explained. Internet of Nano Things was explained concerning with biomedical, defense and security. The MQTT protocol was explained with regard to application protocol.

Vipindev Adat et al. [Vip, 17] scrutinized the background and the history of IoT. The security issues of IoT were analyzed based on its architecture. The design of IoT architecture was described in detail with its layers. The four layers of IoT namely perception layer, network layer, support layer, application layer were described. The different issues in the layers were discussed with clear-cut manner as well as the requirements for security issues were elucidated. The attacks in the 6LoWPAN and RPL like rank attack, resource depletion, tampering, link repair, disrupting traffic,

eavesdropping and flooding were listed out. Threats in the wireless sensor networks; physical layer - jamming and tampering, data link layer - collision and resource exhaustion, network layer - sybil attack, selective forwarding, sinkhole, hello flood, ack spoofing, transport layer - flooding and de-synchronization were explained. The other security issues in IoT environment such as object safety, network security, data confidentiality and encryption, information privacy, interoperability and standardization and naming and the identity management were expounded. The taxonomy of existing defense mechanisms SVELTE, RIDES, Specification based IDS, DoS detection in IoT and DEMO were discussed.

RPL

Anthea et al. [Ant, 16] introduced a taxonomy to classify the attacks against RPL protocol in Internet of Things. The attacks are primarily classified into three types such as resource based RPL attack, topology based RPL attack and traffic based RPL attack. The key concept of RPL protocol like building and maintaining DODAG, loop detection, local repair mechanism and global repair mechanism were clearly explained in detail. The dynamic risk management system of RPL was investigated based on the existing techniques.

Linus Wallgren et al. [Lin, 13] reviewed the IoT protocols and examined their strength and weakness. The attacks against RPL were explored and listed out. The listed attacks were analyzed and tested using Cooja simulator. The security issues were delved into different layers in IoT. The IDS for solving RPL against attacks were presented.

2.2.2 Sinkhole Attack

In sinkhole attack, the malicious node attracts the other nodes in the network by broadcasting false information in order to do illegitimate process in the network [Mey, 21].

Geroge W Kibirige et al. [Ger, 15] explored the existing solution for detecting and identifying sinkhole attack in wireless sensor networks. The authors analyzed the various techniques and mechanisms used for identifying and mitigating the sinkhole attack in WSNs. Challenges such as communication pattern in WSNs, unpredictable situation, physical attack and resource constraints to detect sinkhole attack in WSNs were discussed clearly. Different approaches used for mitigating sinkhole attack such as rule based detection, statistical method, hybrid based intrusion detection and key management were explained. The existing approaches were neatly described with their advantages, limitations and the solution.

Atena Shiranzaei et al. [Ate, 18] proposed an Intrusion Detection System (IDS) to protect the IoT network against sinkhole attack. In the proposed system, all sensors were deployed and initiated in the network. The attack occurred after deploying the sensors nodes. The 6BR requested to the available nodes in the networks to send their information at the regular time interval. The proposed system analyzed whether the attack was occurred or not in IoT network. Cooja and Contiki were used for the implementation.

Sumit Pundir et al. [Sum, 20] recommended proficient Intrusion Detection System (IDS) to detect sinkhole attack in Edge based Internet of Things (SAD-EIoT). The SAD-EIoT was competent in terms of computation cost and communication. It was tested mathematically with various parameter such as packet delivery ratio, end

to end delay and throughput. The recommended IDS was implemented using network simulator version2 (NS2). The normal flow traffic environment, sinkhole attack environment and SAD-EIOT environment were taken for simulation scenario. The SAD-EIoT achieved 95.83% detection rate and 1.03 false positive rate. The IDS was used for critical and sensitive operations.

Maliheh et al. [Mal, 12] presented an algorithm to detect sinkhole attack in wireless sensor networks. The algorithm used control message to detect malicious node in the network. The nodes sent the control message to the main base station before sending the message to the base station. The sent data to the base station was compared with the control message received by the main base station. The node was considered as malicious node if there was any change in the transferred message and eliminated from the network. The algorithm reduced packet loss. It was simulated using MATLAB. The presented algorithm was compared with the existing algorithm "Nagai's" and outperformed the existing algorithm.

Christian Cervantes et al. [Chr, 15] proposed an Intrusion Detection System (IDS) called INTI (Intrusion detection of siNhole attack on 6LoWPAN for interneT of thIngs). INTI was used to identify sinkhole attacks in Internet of Things. The proposed IDS used four modules namely cluster configuration, monitoring routing, detecting attacks and attack isolation. The cluster configuration module was used to define a leader for ensuring scalability and extending the lifetime of the network. In this module, nodes were classified as members and leaders by their network function. Monitoring routing module was used for counting the transmission number of input and output performed by the nodes' response to forward messages. Attack detection module was used to identify and reveal the nodes which were affected by the sinkhole

attack. The attack isolation module was used to isolate the sinkhole nodes after identifying them. The proposed system was implemented using Cooja simulator. The results were 92 percentage for detection rate on fixed scenario and 75 percentage in the mobile scenario.

Melancy Mascarenhas et al. [Mel, 18] surveyed various techniques against sinkhole attack in IoT. Routing protocol RPL and sinkhole attack were clearly explained. The existing techniques such VeRA, TRAIL, SVELTE, INTI and specification cluster based techniques were analyzed. Pros and cons of the existing techniques were discussed.

Sabeen Tahir et al. [Sab, 19] presented an Intrusion Detection System (IDS) to detect and prevent from active sinkhole attack. In this system, whole network was divided into cluster of Internet of Things. Each device was connected to concern gateways. Routing information was stored in the gateway. A node ought to request gateway to establish the path for communication. The IDS was deployed into each gateway. The base station was used to keep the records of the connected devices and links in the network. The special module in the IDS called intrusion analyzer was used to detect the attack in the network. If an attack was found in the network, the alert was broadcasted to connected gateways and the base station. The proposed IDS was simulated using NS-2 with 150 nodes.

Ahmad Salehi et al. [Ahm, 13] recommended an algorithm to find out the sinkhole attack in wireless sensor network. The algorithm was comprised of two process. First process was to test the consistency of nodes and isolating the misbehaving nodes. The second process was to identify attack based on the network flow. The accuracy of the proposed algorithm was evaluated using success rate, false positive rate and false negative rate.

Mahmood et al. [Mah, 17b] proposed lightweight technique called Neighbor Passive Monitoring Technique (NPMT) to detect sinkhole attack in RPL based network. The technique used two passive node in the network to gather information about the connected devices in the network. The technique comprised of two phases. The first phase was used to identify the suspicious node based on inconsistent changes in the network. The second phase was used to detect the sinkhole attack from the suspected list of nodes in the network. It consumed less energy while detecting the sinkhole attack. The technique was compared with the existing technique SVELTE. The proposed technique outperformed the existing system. It was evaluated using Cooja simulator.

Stephen et al. [Ste, 16] proposed a method to identify the sinkhole attack in RPL based network. The proposed method comprised of three phases namely DODAG construction, sinkhole attack identification and sinkhole treatment. Alternate parent was used to detect sinkhole attack by gathering history of the preferred parent node. The proposed method was evaluated mathematically by probabilistic normalization.

Mahmood Alzubaidi et al. [Mah, 17a] delved into various internal sinkhole attacks against RPL protocol. A taxonomy of RPL based attacks was figured out neatly. The contemporary works such as SVELET, INTI, VeRA and TRAIL were used to detect and mitigate sinkhole attack and secured parent method distinguished with each other. The pros and cons of the existing techniques, methods, algorithm and IDS were examined.

Stephen et al. [Ste, 17] proposed an Intrusion Detection System (IDS) to identify and mitigate sinkhole attack in Internet of Things. Proposed model used an agent in the root to monitor all the nodes connected to the network. Intrusion

detection ratio was used to detect sinkhole attack. Once the attack was identified, the affected node's information was sent to other devices in the network as alert message. The proposed IDS reduced packet loss.

2.2.3 Sybil Attack

In the sybil attack, an adversary creates multiple fake identities to reduce the network performance in the Internet of Things [Jon, 21].

Kuan Zhang et al. [Kua, 14], delved into sybil attack in Internet of Things. Authors classified the sybil attack as sybil attack-1 (SA-1), sybil attack-2 (SA-2) and sybil attack-3 (SA-3) based on sybil attacker's capabilities. The defense mechanisms such as social graph based mechanism, behavior classification based mechanism and mobile based defense mechanism against sybil attack were presented. The presented mechanisms were compared with each other based on their defense schemes.

Sohail Abbas [Soh, 19] proposed Intrusion Detection System (IDS) to identify direct and indirect sybil attack using localization method. Localization was done based on RSSI value. There were two main process, firstly each node collected its RSSI value and secondly share the value to its neighbor. By localization technique based RSSI value, malicious node was detected. The proposed system was distributed in nature. It was working in static as well as dynamic in nature. The system caused less overhead.

Mian Ahmad Jan et al. [Mia, 18] recommended two tire detection scheme to identify sybil attack for a forest wildfire monitoring application. High energy nodes were used to identify sybil nodes in the network. The sneaked nodes from the detection process were identified using two base stations at higher level.

Salavat Marian et al. [Sal, 15] presented lightweight detection method to detect sybil attack in wireless sensor networks using Received Signal Strength Indicator (RSSI). ZigBee was used for this experiment. In this deployment process, ZigBee was used without Arduino. The proposed method produced better detection accuracy against sybil attack in wireless sensor network.

Faiza Medjek et al. [Fai, 15] introduced a novel detection mechanism to identify sybil attack in RPL based mobile network. Malicious nodes were detected by analyzing DIO and DAO control messages of nodes. The sybil nodes directly affected energy and packet delivery ratio of the nodes. The proposed scheme was compared with static environment concerned with energy and packet delivery ratio. They concluded that sybil attack reduced the life time of the node as well as life time of the network.

Danilo Evangelista et al. [Dan, 16] explored and examined various techniques to detect and mitigate sybil attack in Internet of Things environment. Detection techniques based on relationship between neighbors, cryptography and network features were analyzed deeply. Lightweight sybil attack detection framework was proposed by Abbas et al. [Abb, 21] was evaluated.

Alekha Kumar et al. [Ale, 18] evaluated sybil attack in Internet of Things. Sybil attack process in IoT was classified into three phases such as compromise, deployment and launching based on its characteristics. The differences between node fabrication and node compromised were explained. K-means clustering algorithm was used to identify sybil attack in Internet of Things. The proposed model clearly visualized the behavior of sybil attack.

Faiza Medjek et al. [Fai, 17] introduced new attack called mobile sybil attack in RPL based Internet of Things. RPL protocol was examined in terms of packet delivery ratio, control overhead and energy consumption. After evaluating RPL protocol, authors proposed Trust based Intrusion Detection System (T-IDS) to identify mobile sybil attack in RPL based Internet of Things. The proposed IDS managed control message multicast, mobility and identity issues in Internet of Things.

2.2.4 Selective Forward Attack

In the selective forward attack, an attacker node drops the packets selectively in the network the Internet of Things [And, 21].

Shapla Khanam et al. [Sha, 17] proposed a game theory model to detect selective forwarding attack in heterogeneous Internet of Things. In the proposed game theory model, two players (player 1 and player 2) were used to minimize and maximize throughput of the network. A hop by hop acknowledgement algorithm was used to monitor and detect selective forwarding attack based on the threshold value of packet loss rate in IoT.

Hongliang Zhul et al. [Hon, 18] proposed a detection method to detect selective forwarding attack based on adaptive learning automata and communication quality in wireless sensor network. The proposed method distinguished the normal packet dropping and malicious packet dropping. It identified the malicious nodes which dropped packets and eliminated the affected nodes from the network. The method comprised of three phases such as initialization of the network and action probabilistic of each learning automata, evaluation of communication quality of the neighbor nodes and detection and punishment of selective forwarding behavior of

nodes. The proposed method was compared with the existing methods DSFLACQ and CLAIDS. And it outperformed those methods.

Surinder Singh et al. [Sur, 19] examined various selective forwarding attack detection techniques based on Public Key Encryption (PKE), Rivest Shamir Adelemen (RSA), ELGAMAL and Chinese Reminder Theorem (CRT) in wireless sensor networks. The examined techniques were evaluated based on energy, storage and time taken for key exchange.

Fatma Gara et al. [Fat, 17] proposed an intrusion detection system to detect selective forwarding attack in wireless sensor networks. The IDS was designed by the combination of sequential probability ratio test with an adaptive threshold of acceptable probability of dropped packets. It contained four processes to detect selective forwarding attack namely data gathering, data analysis, decision and elimination of malicious nodes from the network. The proposed IDS worked good in mobile wireless sensor network concern with network overhead.

Sabah Suhail et al. [Sab, 18] recommended provenance based detection scheme to identify selective forwarding attack in RPL based Internet of Things. Packet delivery ratio was used to detect selective forwarding attack. Packet delivery ratio was computed for each node in the network and added in the payload as provenance information. If any node's energy value falls below threshold value of packet delivery ratio, then it called as malicious node.

Carolina et al. [Car, 16] proposed trust management model to detect selective forwarding attack in Internet of Things. Direct information method was used in the proposed trust management scheme to identify selective forwarding attack. Contiki operating system and Cooja simulator were used to simulate the proposed model with

50 Tmote Sky nodes in random environment. It produced hundred percentage of successful detection rate.

Seyyit Alper Sert et al. [Sey, 17] proposed fuzzy path selection approach to detect and mitigate selective forwarding attack in wireless sensor network. The approach comprised of two phases such as detection and mitigation. Sequence numbers of received packets were used in the detection phase. In mitigation phase, fuzzy logic with node's energy was used to mitigate the selective forwarding attack. The proposed approach decreased the effects of selective forwarding attack and increased the routing reliability in wireless sensor networks.

2.2.5 Blackhole Attack

In the blackhole attack, a malicious node blocks all packets and creates high traffic in the network in the Internet of Things [Sho, 18].

Bhalaji et al. [Bha, 19] proposed a trust based mechanism to counter blackhole attack in RPL protocol. Packet delivery ratio was used as trust value in the mechanism. The proposed trust based mechanism was used in intra DODAG level as well as inter DODAG level. Contiki OS and Cooja simulator were used for implementing the proposed work. The mechanism performed good to counter blackhole attack in RPL protocol.

Himanshu B Patel et al. [Him, 19] introduced strained based intrusion detection of blackhole in 6LoWPAN for Internet of Things (STEWE). The proposed Intrusion Detection System (IDS) identified the malicious nodes based on their behavior. The border router had the responsibility of eliminating the affected nodes from the network. It was evaluated using Cooja simulator. The proposed approach worked better than the watchdog mechanism. It increased packet delivery ratio of

nodes in the network. It provided better detection against blackhole attack in Internet of Things.

Rashmi Sahay et al. [Ras, 18] proposed exponential smoothing based algorithm to detect blackhole attack in Internet of Things. The algorithm comprised of three events such as packet receipt, topology change and detection call. The proposed technique used packets' arrival time to sink node to other node to identify malicious nodes in the network. Cooja simulator was used to simulate the proposed technique.

Firoz Ahmed et al. [Fir, 16] proposed mitigation technique against blackhole attack in Routing Protocol for Low Power and Lossy Networks (RPL). The proposed technique consisted of two process namely local decision process and global verification process. Each node monitored its neighbor node by overhearing transmitted packets by its neighbor to identify malicious nodes in the network. The technique increased packet delivery ratio of the nodes.

Karishma Chugh et al. [Kar, 12] analyzed blackhole attack on 6LoWPAN-RPL in Internet of Things using Contiki operating system and Cooja simulator. The malicious activities which caused blackhole attack were studied in detail using the simulator. Authors found that packets suffered higher delay because of the malicious activities in the network.

Avijit Mathur et al. [Avi, 16] examined the issues behind the selective forwarding attack and blackhole attack over Internet of Things. The authors proposed the detection mechanisms to defend against blackhole attack and selective forwarding attack for medical wireless sensor network in Internet of Things. The blackhole detection mechanism consisted of two phases such as pre-deployment phase where unique random numbers were distributed from base station to all access points in the

network and second phase was routing phase where routing messages were verified by timestamp. Selective forwarding detection mechanism comprised of five sections such as neighbor monitoring, attack detection, control packet collection, analysis and new path. The proposed mechanisms worked better to defend against blackhole attack and selective forwarding attack in Internet of Things.

2.2.6 Version Number Attack

This type of attack broadcasts the false DODAG version number and increases the control message overhead in the Internet of Things [Aru, 21].

Anthea Mayzaud et al. [Ant, 17] recommended a distributed monitoring architecture to detect version number attack in RPL networks. Set of monitoring nodes were deployed to monitor the network. The monitoring nodes monitored only their neighbour nodes which were in the communication range. The data collected by the monitoring node were sent to sink node to detect the malicious nodes. The local assessment was done by the monitoring nodes using the proposed localization algorithm. The distributed detection process was done by the sink node using the distributed detection algorithm in the network. The recommended architecture was simulated using Cooja simulator. The false positive rate of attack detection was reduced by the architecture.

Chandni et al. [Cha, 19] proposed a trust based technique to detect version number attack in Internet of Things. The trust for each node was calculated using the packet delivery ratio. The calculation process was done by direct and indirect trust calculation methods to identify malicious nodes. The direct trust value was sent from the current node and the indirect trust value was sent from its neighbour node. It was

implemented in network simulator version2. It achieved better throughput and reduced delay and control message overhead.

Ahmet et al. [Ahm, 20] analyzed the version number attack deeply with multiple attackers in RPL network. The effect of version number attack with multiple attackers in various aspects was evaluated. It was found that once a node was affected by the version number attack then other nodes were easily compromised. The impacts of the multiple attacker node were evaluated using Cooja simulator. It was found that multiple attacker only affected packet delivery ratio of the network. It did not affect delay and the energy consumption.

2.2.7 Hello Flood Attack

In hello flood attack, an attacker node broadcasts the hello packets unnecessarily to increase the traffic in the Internet of Things network [Sau, 21].

Aditya Sai Srinivas et al. [Adi, 20] designed a deep learning based model to detect and prevent hello flood attack in Internet of Things. The Rider Optimization Algorithm (ROA) was improved and used in detecting and preventing the hello flood attack. This model contained k-paths generation, cluster head selection and detection and prevention of hello flood attack. Authors analyzed the performance metrics such as energy of a node, network latency, transmission delay, packet loss ratio and shortest path length of the network. The proposed model achieved better result in terms of attack detection accuracy.

Khosravi et al. [Kho, 16] recommended Intrusion Detection System (IDS) to detect hello flood attack in wireless sensor networks. The attack was detected by the behaviors of the nodes in the network. The behavior of a node was analyzed by the

neighbour nodes' information about the node. The neighbour nodes were identified using Received Signal Strength Indicator (RSSI) to get the information about a particular node to check whether a node was in the same track with other nodes in the network. Alfa-Beta Filtering method was used to detect the malicious nodes. The performance of IDS was evaluated using receiver operating characteristics. The proposed IDS achieved better attack detection accuracy, high packet delivery ratio and low delay.

Gayatri Devi et al. [Gay, 15] proposed mechanism to detect hello flood attack in wireless sensor networks. The mechanism used received signal strength indicator and Broadcast Authentication using cryptographic Puzzles (BAP) to detect hello flood attack. Each node monitored the 'hello message' whether the message received from within the radio signal. The nodes were classified into two types namely friend node which was within the communication range and strange node which was far away from the communication range. The strange nodes were validated with BAP to identify the malicious nodes in the wireless sensor networks.

2.2.8 Wormhole Attack

In the wormhole attack, one or more nodes create tunnel in the network and illegitimately listen to the communication in the IoT network [Haf, 21].

Parvathy et al. [Par, 21] reviewed wormhole attack in Wireless Sensor Network (WSN) and Internet of Things (IoT). The techniques such as Geographic based, Graph Theoretical Approach, Location aware Detection Scheme, Distributed Detection Algorithm and etc. were used to detect and mitigate wormhole attack in IoT. The WSN is analyzed in detail. The impacts of wormhole attack in IoT and WSN were explicated in the review. The detection algorithms and techniques were compared with each other in terms of throughput, packet delivery ratio and average delay.

Pavan Pongle et al. [Pan, 15] introduced a real-time detection mechanism to identify wormhole attack in Internet of Things. The detection mechanism used the location to detect the wormhole attack using received signal strength. The neighbour information of each node in the network was stored in the border router. The border router periodically checked the location of each node to check whether the node was affected by the wormhole attack or not. The proposed mechanism achieved less overhead and high true positive detection rate.

Nandhini et al. [Nan, 20] proposed an Intrusion Detection System (IDS) to identify wormhole attack in RPL based Internet of Things networks. RSSI was used in IDS to detect wormhole attack. The RSSI of neighbour nodes were verified and validated and stored in the border router. Then the stored RSSI value of the nodes were converted into distance. The node was identified as malicious node which was affected by the wormhole attack using the RSSI value.

2.2.9 Rank Attack

In rank attack, an adversary broadcasts false rank to attract neighbor nodes. It leads to packet loss and reduce PDR of the network [Geo, 21]

Anhtuan et al. [Anh, 13] analyzed the different types of internal threats concern with rank property and their impact over WSN. RPL protocol was deeply explained with its operation. The purpose of mitigating rank attack in RPL was given such as route optimization, prevention of loops and managing internal threats. The attacks in RPL were listed out such as sybil attack, selective forwarding attack, blackhole attack and sinkhole attack. The function of DODAG in RPL was explained in clear cut. The parameters which were used for differentiating each DODAG were listed out such as RPL instance ID, DODAGID, DODAG version number and rank. The better method

for selecting parent node was described with three types of control messages namely DIO, DAO and DIS. The Impact of rank attack over network topology was checked using Contiki 2.5 and Cooja Simulator. The impact of nodes made by rank attack in the network was graphically depicted.

Agnieszka Brachman et al. [Agn, 13] described RPL objective function and its impacts over LLNs topology. The core aim of the paper was to elucidate how the selection of objective function influences the network topology. The metrics were categorized as node metrics, link metrics, qualitative metrics, quantitative metrics, dynamic and static metrics. The objective function plays the major role for setting rank for a node in a RPL network. There are many possibilities for rank attack when there is an inconsistency change in the objective function.

Stephen et al. [Ste, 18b] proposed RIAIDRPL: Rank Increased Attack (RIA) identification algorithm for avoiding loop in the RPL DODAG. The proposed algorithm identified the rank increased attack node in Low power and Lossy Networks (LLNs). The algorithm found the attacker node which creates the loop in the destination oriented direct acyclic graph. Packet delay, packet delivery ratio, false positive rate, attack identification rate were used for identifying rank increased attack. The RIAIDRPL used four different types of lists such as blocked list, unblocked list, checked list and parent mapping list for finding the loop in DODAG. The blocked list represented the nodes which had not been visited. Unblocked list consisted of visited nodes in the network. The checked list represented the attacker node which created the loop. The Cooja simulator was used to simulate the performance of the proposed algorithm. The RIAIDRPL gave better result than existing protocol RPL and LRPL algorithms.

Stephen et al. [Ste, 18c] proposed a technique to detect and mitigate Rank Attack (RA) or Rank Inconsistency attack (RInA) in IPv6 Routing protocol for Low

power and lossy networks (RPL). The technique was energy based validation and verification (E2V). There were three phases in the proposed technique such as rank calculation, substation and malicious node elimination. In RPL protocol, the nodes select the parent node based on the rank. The node which has low rank will be selected as a parent node by the neighboring node. The attacker node misuses its rank value. The attacker node convinces the neighboring node that the attacker node is having low rank among the nodes in the network for selecting it as a parent node. The proposed technique gave a solution to overcome the Rank Inconsistency attack.

Mohammad et al. [Moh, 18] analyzed topological attacks in RPL networks and found rank and version number attacks were the most vulnerable attacks among other attacks. The lightweight defense approach was proposed to mitigate these two attacks. Identity Based Offline-Online Scheme (IBOOS) was used to detect and mitigate these attacks. The scheme was divided into two phases such as offline phase and online phase. Offline scheme was used to process the heavy computation part and online scheme was used for the lightweight computation process. IBOOS included five algorithms called Setup, Extract, OffSign, OnSign and Unsign to identify and mitigate the attacks. The RPL network model was picturized and rank attack and version number attack were depicted over the picturized RPL network model. The lightweight scheme was evaluated mathematically based on storage, computational cost, energy consumption and key size. It was compared with TRAIL and VeRA techniques in terms of computational time and energy consumption. It was better than these two techniques.

In [Bou, 20], the security issues by rank attack were expounded in various aspects. Authors enlightened researchers how rank attack affected the resources and

topology in the RPL networks. The existing techniques which were used to provide solution for the security issues in RPL networks were explicated. Various attacks against RPL networks were classified and compared using Friedman test.

Anomaly based rank attack detection technique was proposed [Abd, 20] to detect rank attack in the smart hospital infrastructure in IoT networks. Machine learning was used to detect the rank attack in smart hospital to protect sensitive data from the intruders. Support Vector Machine (SVM) algorithm was selected for developing the technique. The centralized approach was used to deploy the proposed technique. The IDS was deployed in the border router. Cooja simulator was used to simulate the technique. The simulation was done in four scenarios such as network without malicious nodes, network with one malicious node, network with two malicious nodes and network with four malicious nodes. It achieved better attack detection accuracy.

The RPL operations such as optimal topology formation, prevention of loop and the control message management were explicated in [Anh, 13]. The impacts of rank attack in RPL networks were detailed. To test the impacts of rank attack, Cooja simulator was used. The RPL code was modified to trigger the rank attack in the network in order to analyze the rank attack. The rank attack was classified into four types such as type I which updated DIO message but it was permanent against rank rule, type II which updated DIO message but it was non-permanent against rank rule, type III which did not update DIO message but it was permanent against rank rule and type IV which did not update DIO message but it was non-permanent against rank rule. The performance metrics were evaluated for these four types of attack. Type I and II created more control messages and III and IV increased the end to end delay in the RPL network.

David Airehrour et al. [Dav, 19] proposed time-based trust-aware RPL routing protocol (SecTrust-RPL) to detect rank and sybil attacks. Based on the behavior of the nodes, the trust was calculated. The trust was computed based on the successful packet delivery. In SecTrust-RPL, the malicious nodes were detected based on the trust of the individual node and isolated the malicious nodes from the network. The SecTrust-RPL was compared with standard RPL protocol. The proposed technique achieved better results in terms of attack detection accuracy.

Various attacks and countermeasures of this attacks against RPL based IoT network are given in the table 2.1.

Table 2.1 Various Attacks and Countermeasures of this Attacks against RPL based IoT

S. No.	Attack	Countermeasures
1	Sinkhole attack	IDS based solution ([Ger, 15], [Ate, 18], [Sum, 20], [Chr, 15], [Ste, 17], [Sab, 19]), Lightweight Technique [Mah, 17b]
2	Sybil attack	Social Graph based Mechanism [Kua, 14], Two Tire Detection Scheme [Mia, 18], Lightweight Detection Method [Sal, 15], PDR based [Fai, 15], IDS [Fai, 17]
3	Selective forward attack	Game Theory Model [Sha, 17], Adaptive Learning Method [Hon, 18], IDS [Fat, 17], PDR based [Sab, 18], Trust based, [Car, 16], Fuzzy based Method [Sey, 17]
4	Blackhole attack	Trust based [Bha, 19], IDS [Him, 19], Exponential Smoothing based [Ras, 18]
5	Version number attack	Architecture [Ant, 16], Trust based [Cha, 19].
6	Hello flood attack	Deep Learning based [Adi, 20], IDS [Kho, 16], RSSI based [Gay, 15]
7	Wormhole attack	Location based [Pan, 15], IDS [Nan, 20]
8	Rank attack	Verification based [Ste, 18b], Energy based [Ste, 18c], Lightweight Algorithm [Moh, 18], Machine Learning based [Abd, 20], Trust based [Dav, 19]

2.3 Research Road Map

The research road map gives the scope of the research work. It narrows down macro research into micro research based on the literature review. It specifies the particular issue which is carried out in the research work and the solution for the issue. The figure 2.1 shows the research road map.

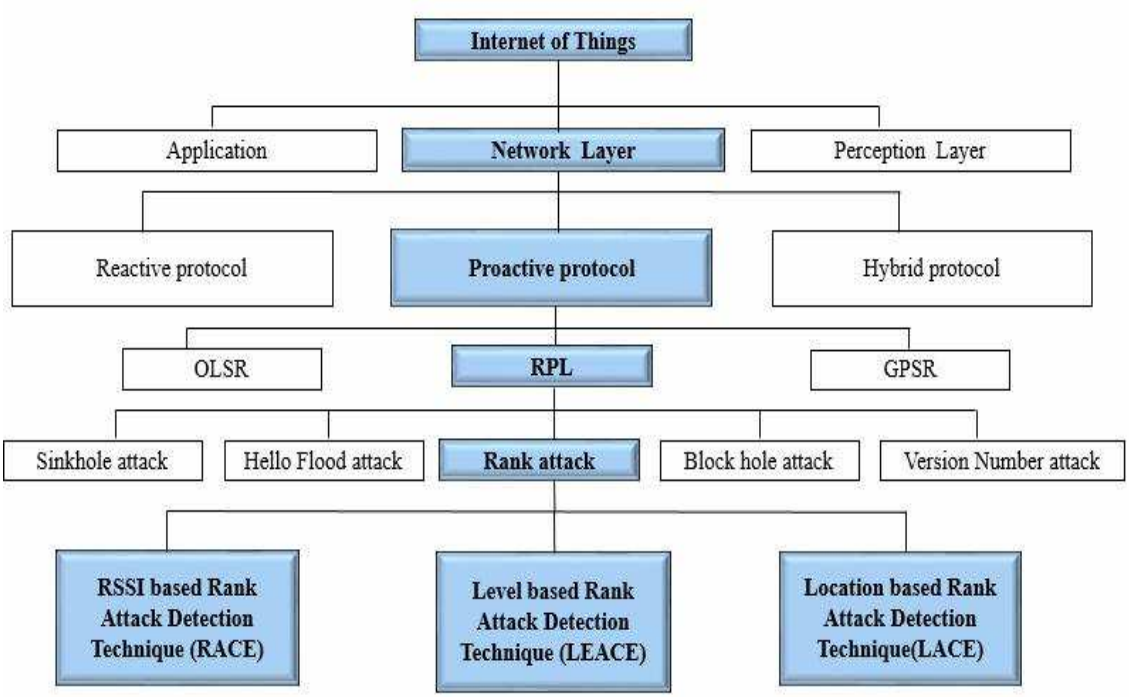


Figure 2.1 Research Road Map

In this research, the Internet of Things is taken as a macro study and rank attack is taken as micro study. There are various issues in Internet of Things but this research work focuses on rank attack which occurs in RPL protocol in network layer in IoT environment.

2.4 Chapter Summary

The usage of IoT increases day-by-day in the speedy life. The global connectivity feature in IoT attracts people to use IoT applications for all the activities in their

regular life. Sensitive data are collected and transferred from one place to another place every day throughout the world. So, the IoT network should be secured. This chapter reviews the literature of the network issues; particularly, attacks occur in RPL based IoT. It exposes the various types of attacks in RPL and the techniques used to detect and mitigate the attacks. Based on the literature review the research road map is designed and explicated the scope of this research work. Eventually, attacks occur in RPL protocol are analyzed and found that rank attack is the severe attack among all the attacks. So, there is need to provide techniques to detect the rank attack in Internet of Things. In the next chapter, RSSI based technique is provided to detect rank attack in Internet of Things.

Chapter – 3

RSSI Based Rank Attack Detection Technique for the Internet of Things (RACE)

CHAPTER - 3

RSSI BASED RANK ATTACK DETECTION TECHNIQUE FOR THE INTERNET OF THINGS (RACE)

3.1 Background

Internet of Things is a recently emerging technology. Now-a-days, IoT makes human work much easier in all the fields such as building construction, agriculture, hospitals and all the industrial works. IoT enables all the works of the human to be easy and efficient. IoT connects anything at anytime from anywhere. The connected things communicate with one another in a network. The IoT networks collect and transfer the most sensitive data from many fields. The IoT network is a Low power and Lossy Networks (LLNs). The nodes in the IoT network can easily be compromised. So, the IoT network could be susceptible to intruders. IoT mostly uses Routing Protocol for Low power lossy network (RPL) which is specifically designed for low power and lossy networks for routing.

RPL protocol uses Destination Oriented Directed Acyclic Graph (DODAG). RPL mostly uses three types of objective function to form a DODAG such as hop count, energy and expected transmission count. The parent selection process is done based on the rank of a node. The node which has lesser rank than the other neighbour nodes is selected to be a preferred parent in a network.

RPL protocol is affected by various attacks such as black hole attack, wormhole attack, sinkhole attack, hello flood attack and rank attack in IoT environment. Rank attack is one of the attacks which affects RPL severely. Rank attack is classified into rank increased attack and rank decreased attack. Only few techniques are proposed to

detect rank attack. The existing techniques are more generalized. But the Rank in RPL is calculated based on the objective function. So the rank attack character is changing based on the nature of objective function. For that, the specialized technique is needed to handle the objective function behavior.

In this chapter, the RSSI based rank attack detection technique is proposed to detect the rank attack in hop count based DODAG construction in RPL network. The proposed technique increases the attack detection accuracy when compared with RDAID technique [Ste, 18a] as well as increases the packet delivery ratio and throughput in the network.

3.2 Related Works

In [Abd, 16], authors explicated operation of RPL and RPL network model with its parent selection process. Rank attack was identified in the RPL network. It was found that the rank attack might decrease 30% to 50% packet delivery ratio in the network and modify the objective function. The rank attack decreased network throughput and increased latency. The identified rank attack was tested in Cooja simulator with Contiki operating system.

RDAID technique [Ste, 18a] was proposed to detect rank decreased attack in RPL network. Packet delivery ratio was used to detect the rank decreased attack. The technique brought the idea that the node which had high packet delivery ratio might cause less possibility of the attack and the node which had less packet delivery ratio might cause more possibility of the attack in the RPL network. The technique was implemented in the Cooja simulator over the Contiki operating system. It achieved better results than the existing work INTI in terms of packet delivery ratio and attack detection accuracy.

3.3 Motivation

IoT can connect a vast number of devices through the Internet at any time. It provides intelligence to work smarter than ever in the world. Consequently, the growth of IoT is increasing exponentially. Since the tremendous growth of IoT, the security issues are concentrated more. Attacks against IoT especially routing attacks are focused more by the researchers. Among all the attacks, the rank attack in the RPL network has been spotlighted by many researchers in recent years. So, it is the motivation to proceed with rank attack detection technique.

3.4 Objective

Objective of this chapter is to propose Received Signal Strength Indicator (RSSI) based rank attack detection technique to increase attack detection accuracy and eliminate the malicious nodes from the network.

3.5 RSSI based Rank Attack Detection Technique (RACE)

The RSSI based Rank Attack Detection Technique (RACE) is proposed to identify rank attack in RPL based Internet of Things. The RACE is used to detect rank attack while the objective function is set as hop count in RPL. Each node in a network has its RSSI value from a node to its parent. There are few methods available to calculate RSSI value. The proposed RACE uses the path loss model. RSSI uses decibel (dB) as a unit to measure the value. The RSSI values would be in negative value. The formula to calculate RSSI is given below.

RSSI(X) = A–10n*logd

A – Received Signal Power

n – Path loss Index

d – Distance

RACE calculates the RSSI value from a node to its parent as well as RSSI value from a node to the root node which is called TRRX. The calculated values are stored in the root node. If there is an inconsistent change of the rank value in any of the nodes then TRRX is compared with its parent's TRRX. The parent's TRRX should be greater than its children. If the parent's TRRX is lesser than the current node then it is considered as a malicious node and affected by rank attack. After identifying malicious nodes in the network, the malicious nodes are isolated for an elimination process. The paths for the available nodes are denoted below for finding the intermediate nodes.

The Network path from Rnode to Nnode and Rnode to Xnode

Path(Rnode, Nnode) = (Rnode, IMn1, IMn2, IMn3,…..IMnn, Nnode)

Path(Xnode, Rnode) = (Xnode, IMn1, IMn2, IMn3,…….IMnn, Rnode)

Where Rnode is Root node and IMn is an intermediate node

If Parent(Xnode) ≠Rnode then, ∃ IMnode ∈ P(Rnode, Nnode)

If Parent(Xnode) = Rnode then ∄ IMnode

RACE technique consists of three phases. Figure 3.1 shows the three phases of RACE technique.

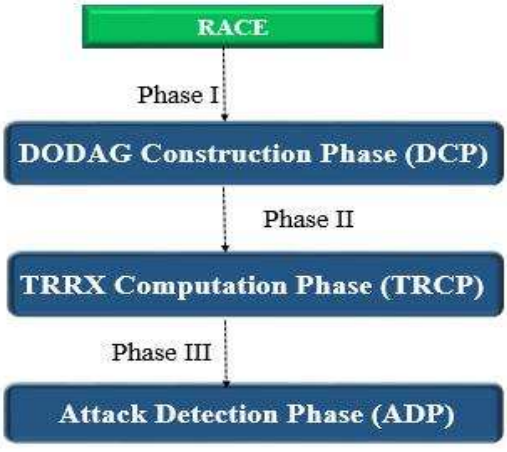


Fig. 3.1 Three Phases in RACE

Phase I - DODAG Construction Phase (DCP)

DODAG Construction Phase (DCP) is the fundamental phase in RPL based Internet of Things. The DODAG construction is done using RPL control messages. Initially the root node starts broadcasting the DIO messages. The neighbor nodes which are nearby the root node receive DIO message if and only if the objective function of neighbor nodes is set as hop count. The neighbor nodes which have received DIO messages from the root node will send the DAO message to the root node. The DIO broadcasting process is done by all the nodes in the network after the root node. All the parents in the network send the DAO_Ack to their children and the DODAG is formed. The rank of each node is computed based on hop count. While constructing DODAG, the rank of the child should be greater than its parent's rank.

Phase II - TRRX Computation Phase (TRCP)

Total RSSI value of a node from the Root node to the node X(TRRX) is calculated by adding the RSSI value of the intermediator nodes of the node X. The nodes which are having root node as their parent, do not have intermediator nodes. For such nodes, the TRRX value and RSSI values are the same. Once the TRRX computation is over, the values are stored in the root node.

Phase III - Attack Detection Phase (ADP)

In the third phase, RACE uses TRRX and Total RSSI value of parent of the current node from the Root node (TRRP(X)) to detect rank attack. If the rank of node X is greater than the rank of the parent node and TRRX is less than TRRP(X) then node X is declared as a legitimate node. If the rank of X is less than the rank of the parent node and TRRX is greater than TRRP(X) then the node X is declared as a malicious node affected by rank attack. Then, the malicious node will be isolated from the network.

RACE Technique

Input : RPL Control messages, TRRX, TRRP(X)
Output: Rank attack
Step 1: Rnode broadcasts the DIO message to start DODAG construction
Step 2: NBnodes receive and accept DIO message ⇔ OF(Rnode) & OF(NBnodes) = HC
Step 3: Compute Rank based on OF (HC) to select Parent Node
Rank(Pnode) < Rank (Child node)
Step 4: Child Node unicasts DAO message to its selected preferred parent node
Step 5: Parent node sends DAO_ACK message to its children then the DODAG is constructed.
Step 6: If Pnode(X) = Rnode Then
TRRX = RSSI(X)
Step 7: If Pnode(X) ≠ Rnode Then
TRRX = RSSI(X+IMn1+IMn2+……IMnn)
Step 8: TRRX is stored in Rnode
Step 9: If Rank(X) >Rank(Pnode(X)) && TRRX < TRRP(X) then
X is legitimate node
Step 10: If Rank(X) <Rank(Pnode(X)) && TRRX < TRRP(X) then
X is affected by Rank Decreased Attack then remove X from the network
Step 11: If Rank(X) >Rank(Pnode(X)) && TRRX > TRRP(X) then
X is affected by Rank increased Attack then remove X from the network
Step 12: Form the new network after eliminating malicious nodes

Terms used in the Technique

TRRX - Total RSSI value from root node to current node

Rnode - Root node

IMn - Inter Mediator node

X - Current node

Pnode - Parent node

NBnodes - Neighbor nodes

OF - Objective Function

HC - Hop Count

TRRP(X) - RSSI value from root node to parent node of current node

3.6 Theoretical Analysis

In theoretical analysis, the RPL network is assumed with fourteen nodes. Among the fourteen, one is the root node, one is a malicious node and other twelve nodes are legitimate nodes. For each node, the RSSI value towards its parent and total RSSI value towards the root node are calculated.

Let S be the set of all nodes in the network then

S = {A,B,C,D,E,F,G,H,I,J,K,L,M,N}

Communication path from root node to N node is denoted as

Path(Rnode, Nnode) = (Rnode, IMn1, IMn2, IMn3,…..IMnn, Nnode)

Communication path from root node to X node is denoted as

Path(Xnode, Rnode) = (Xnode, IMn1, IMn2, IMn3,…….IMnn, Rnode)

All nodes in the network have their intermediator nodes except the nodes which have its parent as the root node.

If Parent(Xnode) $\neq$ Rnode then, $\exists$ IMnode $\in$ P(Rnode, Nnode)

If Parent(Xnode) = Rnode then $\nexists$ IMnode

The RPL network with assumed fourteen nodes with one root node, one malicious node and twelve legitimate nodes is shown in Figure 3.2.

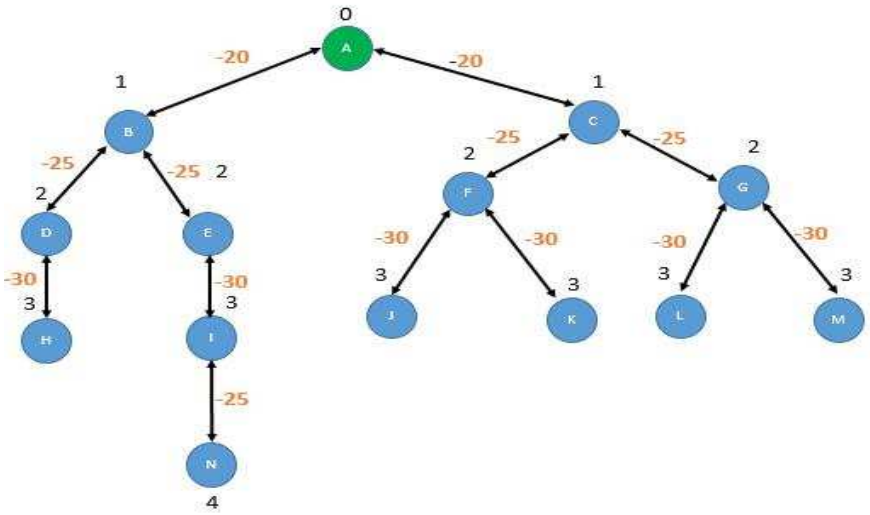


Figure 3.2 RPL Network

The considered RPL network is homogenous. All the nodes in the network are connected using the same communication technology. Because the RSSI based rank attack detection is suitable only for homogenous networks. The RSSI value could vary according to the communication technologies. The low range communication technologies and high range communication technologies have their qualitative range measurement such as good, better and bad according to their specific values for each quality. The RSSI value is measured in decibel (dB). RSSI values are measured in negative integers. In figure 3.2, the rank of the nodes are given in positive integers and zero. The RSSI value of each node is given in negative integers. The node ID is given in upper case of English language. The network is constructed based on the rank of the nodes. The candidate nodes which are having the lesser rank than other nodes are selected as the preferred parent. Figure 3.3 shows the total RSSI value of each node in the given network.

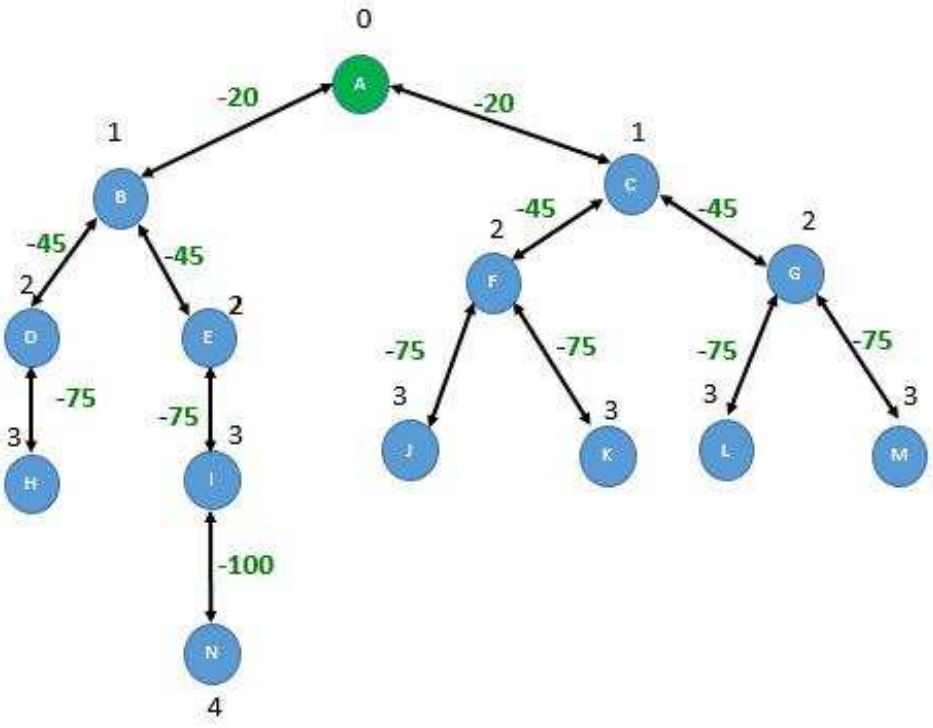


Figure 3.3 Nodes with Total RSSI Values

The total RSSI values are calculated by computing intermediator nodes of each node in the network. For computing total RSSI value for each node, the RSSI value of the intermediator nodes are calculated and shown in figure 3.3. The table 3.1 shows RSSI value towards the parent node and total RSSI value towards root node of all nodes in the network.

Table 3.1 RSSI and TRRX of Each Node

Node	Parent	Rank	IMN	RSSI(dB)	TRRX(dB)
A	…	0	…	…	…
B	A	1	…	-20	-20
C	A	1	…	-20	-20
D	B	2	B	-25	-45
E	B	2	B	-25	-45
F	C	2	C	-25	-45
G	C	2	C	-25	-45
H	D	3	D, B	-30	-75
I	E	3	E, B	-30	-75
J	F	3	F, C	-30	-75
K	F	3	F, C	-30	-75
L	G	3	G, C	-30	-75
M	G	3	G, C	-30	-75
N	K	4	K, F	-25	-100

Table 3.1 presents the nodes available in the network along with the parent of each node and rank of each node. And also the intermediator nodes, RSSI value and total RSSI value of each node are presented in the table. Each node stores the RSSI value and total RSSI value of its children nodes. The malicious network is depicted in figure 3.4.

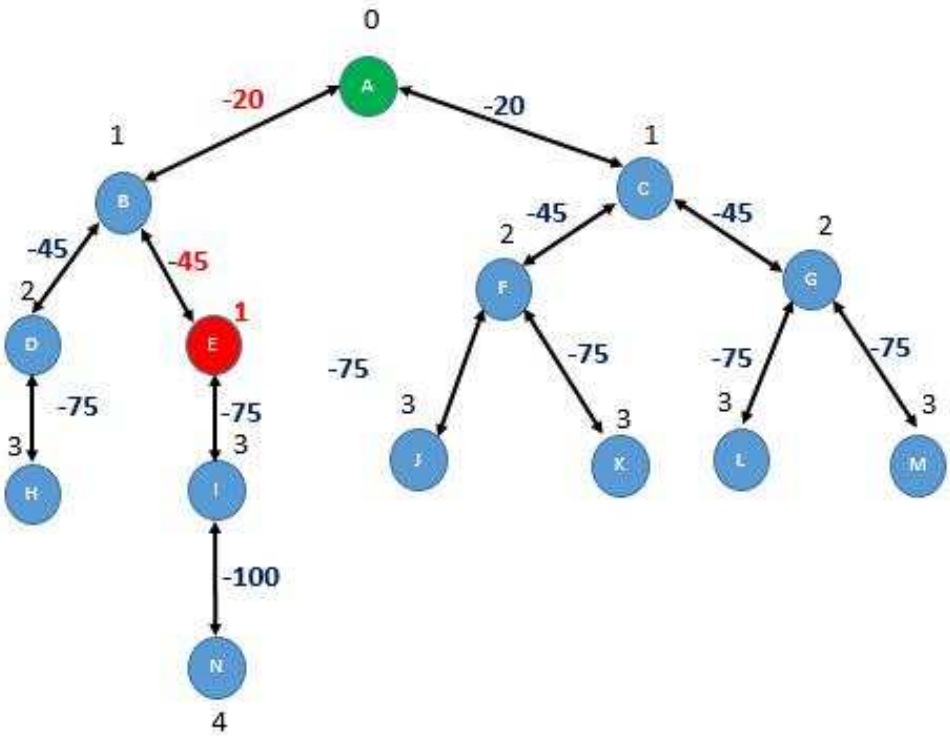


Figure 3.4 Network with Malicious Node

Figure 3.4 presents the rank, total RSSI value of each node and the malicious node in the network. From figure 3.4, the node E is considered as a malicious node which is affected by rank attack in the network. The node has changed its actual rank value two to false rank value one. It tries to attract its neighbor nodes by pretending as it is very near to the root node. To identify whether the node is affected by the rank attack, the total RSSI value of the malicious node E should be verified by its parent along with its modified rank. The total RSSI value of the malicious node is calculated by adding the RSSI value of its intermediator node. The intermediator node to reach root node for the malicious node is node B. The parent of the malicious node is also B. So, the total RSSI value of the malicious node E and its parent node B is used to identify whether the node is affected by rank attack or not. Table 3.2 shows rank and total RSSI value of the malicious node.

Table 3.2 Table with attacker node

Node	Parent	Rank	TRRX(dB)
A	…	0	…
B	A	1	-20
C	A	1	-20
D	B	2	-45
E	B	1	-45
F	C	2	-45
G	C	2	-45
H	D	3	-75
I	E	3	-75
J	F	3	-75
K	F	3	-75
L	G	3	-75
M	G	3	-75
N	K	4	-100

From table 3.2, the rank of the malicious node is one and its parent's rank is also one. So, there is an inconsistent change in the rank of parent and child. Now, the total RSSI values of the node, its parent and the malicious node are compared. The total RSSI value of the parent node towards the root node is -20 and the total RSSI value of the malicious node is -45. The parent node has higher total RSSI value than the malicious node. So, it is declared that the node E is affected by the rank attack. If a node has lesser total RSSI value and lower rank than its parent node then the node is affected by rank decreased attack. If a node has higher total RSSI value and higher rank than its parent then the node is affected by rank increased attack. From table 3.2,

the malicious node E has lesser total RSSI value and lower rank than its parent node B. So, the node is affected by rank decreased attack. The malicious nodes have to be removed from the network. Figure 3.5 shows the elimination of the malicious node from the network and reconstruction of the network.

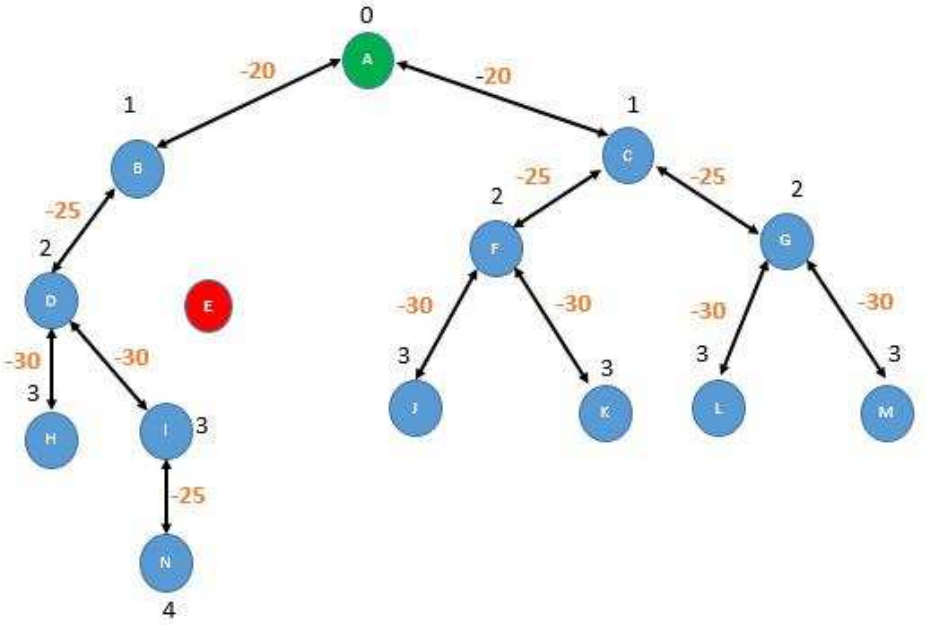


Figure 3.5 Malicious Node Elimination and Reconstruction of the Network

The parent node of the malicious node E has identified that the node is affected by the rank attack that disseminated the information in the network. The nodes connected with node E disconnect their connectivity after listening to the information from node B. The node is isolated from the network. The network is reconstructed after eliminating the affected node from the network.

3.7 Simulation Results and Discussions

Cooja simulator and Contiki operating system are used for simulating the proposed work. Cooja runs on the Contiki operating system. Cooja and Contiki are open source software. Cooja is the best network simulation software which is used by

many researchers. It makes the IoT a real time environment in the network simulation. The RSSI based rank attack detection technique is deployed in every node in RPL network. The network parameters used for simulating RACE technique are given in table 3.3.

Table 3.3 Simulation Parameters

Parameters	Description
No. of Nodes	10, 20, 50
Simulation Area	1000 x 1000 m
Data Rate	250kbps
Node Arrangement	Random
Operating System	Contiki
Simulator	Cooja
Types of Sensor Node	Sky Mote
Packet Analyzer	Wireshark

3.7.1 Network Setup

In the Cooja simulator, ten, twenty and fifty nodes are taken for the implementation process. All the nodes are placed in a random position. The sky mote is used for simulating the nodes for the proposed technique. The proposed technique is compared with existing technique RDAID [Ste, 18a] in terms of packet delivery ratio, throughput and attack detection accuracy. Firstly, the RACE technique is tested with ten nodes. Among ten nodes one node is root node, eight nodes are legitimate nodes and one node is the malicious node. Figure 3.6 shows the RPL network with ten nodes in the Cooja simulator.

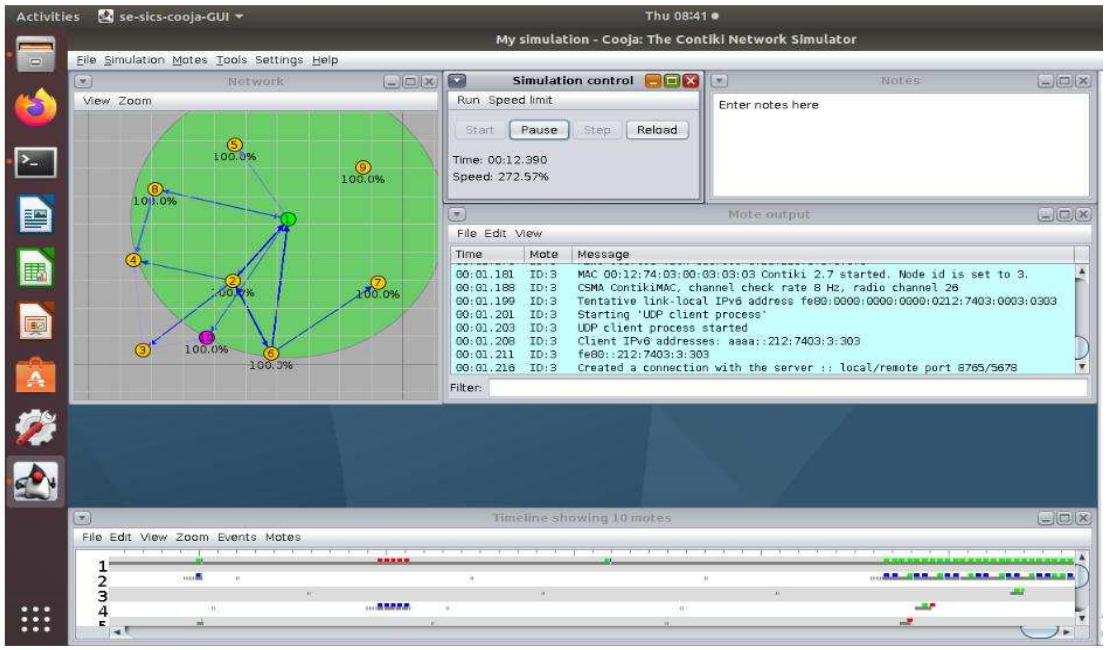


Figure 3.6 RPL Network with 10 Nodes

Secondly, the RACE technique is tested with twenty nodes. Among twenty nodes one node is root node, fourteen nodes are legitimate nodes and five nodes are malicious nodes. Figure 3.7 shows the RPL network with twenty nodes in Cooja simulator.

Figure 3.7 RPL Network with 20 Nodes

Thirdly, the RACE technique is tested with fifty nodes. Among fifty nodes one node is a root node, thirty nine nodes are legitimate nodes and ten nodes are malicious nodes. Figure 3.8 shows the RPL network with fifty nodes in the Cooja simulator.

Figure 3.8 RPL Network with 50 Nodes

3.7.2 Evaluation Metrics

Evaluation metrics are used to evaluate the performance of the proposed technique RACE and with existing technique RDAID. RDAID and RACE both techniques have been deployed in the Cooja simulator. Several metrics such as packet delivery ratio, throughput, attack detection accuracy, reliability, latency and etc. are used for evaluating the techniques. For this research, packet delivery ratio, throughput and attack detection accuracy are taken to evaluate the RACE technique against the rank attack with ten, twenty and fifty nodes.

Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is computed using total number of packets sent from sender and total number of packets received by the receiver. The rank attack decreases packet delivery ratio once the network is affected by rank attack. In this research, PDR is evaluated to check whether the proposed technique increases the packet delivery ratio or not. The Packet Delivery Ratio of proposed technique is compared with RDAID technique. The formula for calculating PDR is as follows

$$\text{Packet Delivery Ratio (PDR)} = \frac{\Sigma(TPR)}{\Sigma(TPS)}$$

Where

TPR = Total number of Packets Received by the receiver

TPS = Total number of Packets Sent by the sender

Table 3.4 presents the packet delivery ratio according to the number of nodes taken. Average of the packet delivery ratio is taken to compare the proposed work RACE with the existing work RDAID. Figure 3.9 graphically represents the difference between RACE and RDAID.

Table 3.4 PDR in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RDAID	91.7	91.5	90
RACE	93.1	92.7	91

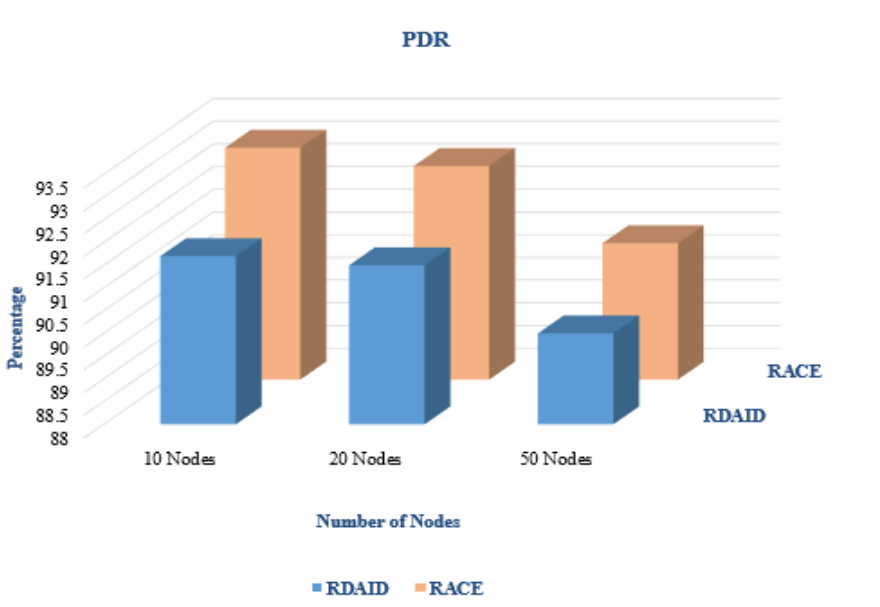


Figure 3.9 Packet Delivery Ratio Analysis

From figure 3.9, it is observed that RACE technique performs better than the existing technique RDAID in terms of packet delivery ratio. The blue colour bar represents the RDAID technique and light brown colour bar represents the RACE technique. X – Axis shows the number of nodes taken for simulation. Y – Axis shows the packet delivery ratio in percentage.

Throughput

Throughput is calculated based on the total number of packets successfully sent within the given timeframe from source to the destination. The formula for calculating the throughput is as follows

$$\text{Throughput} = \frac{FS}{TT(bps)}$$

Where

FS - File Size

TT - Transmission Time

$$\text{Transmission Time} = \frac{FS}{Bandwidth(s)}$$

Table 3.5 presents the throughput ratio according to the number of nodes taken. Average value of the packet throughput is taken to compare the proposed work RACE with the existing work RDAID. Figure 3.10 graphically represents the difference between RACE and RDAID.

Table 3.5 Throughput in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RDAID	90	89.5	89.2
RACE	93.2	92	91.5

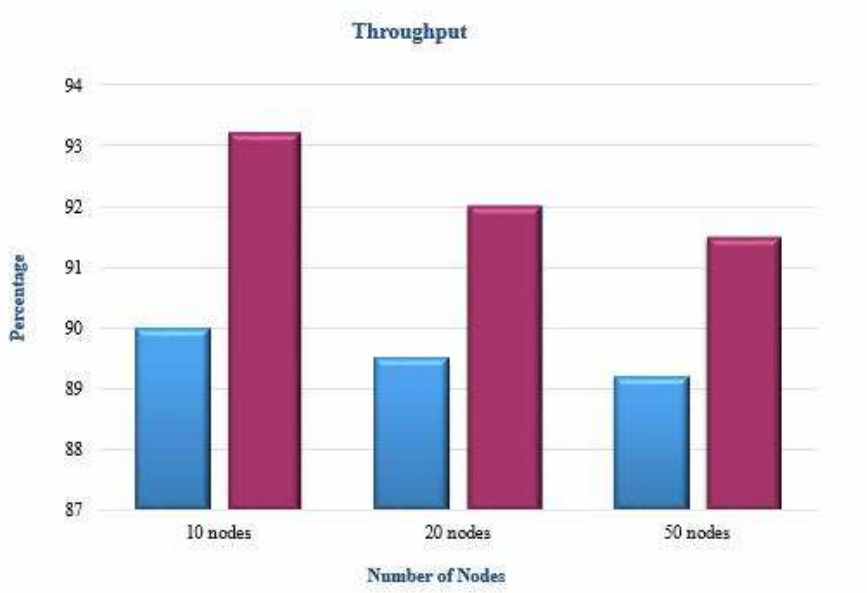


Figure 3.10 Throughput Analysis

From figure 3.10, it is identified that RACE technique performs better than the existing technique RDAID in terms of throughput. The blue colour bar represents the RDAID technique and light pink colour bar represents the RACE technique. X – Axis shows the number of nodes taken for simulation. Y – Axis shows the throughput in percentage.

Attack Detection Accuracy

Attack Detection Accuracy (ADA) is the major evaluation metric among these three evaluation metrics. Attack Detection Accuracy is calculated based on the ratio of true positive and true negative values. The formula for calculating attack detection accuracy is as follows

$$\text{Attack Detection Accuracy (ADA)} = \left(\frac{TP}{TP+TN}\right)\times 100$$

Where

TP - True Positive

TN - True Negative

Table 3.6 presents the attack detection accuracy according to the number of nodes taken. Attack detection accuracy is evaluated for the proposed work RACE and compare with the existing work RDAID. Figure 3.11 graphically represents the attack detection accuracy of RACE compared with RDAID.

Table 3.6 Attack Detection Accuracy in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RDAID	91.6	91.2	90
RACE	93	92.5	91

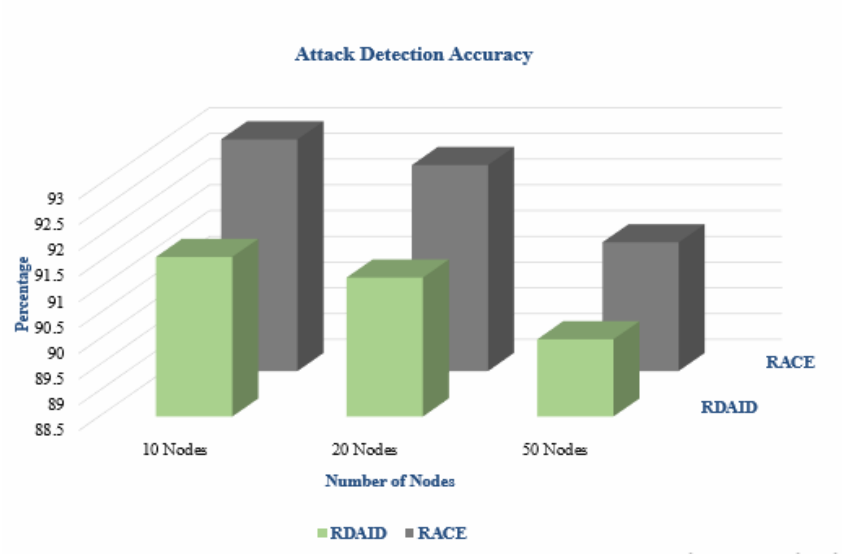


Figure 3.11 Attack Detection Accuracy (ADA) Analysis

From figure 3.11, RACE technique performs better than the existing technique RDAID in terms of attack detection accuracy. The light green colour bar represents the RDAID technique and gray colour bar represents the RACE technique. X – Axis shows the number of nodes taken for simulation. Y – Axis shows the attack detection accuracy in percentage.

3.8 Findings and Interpretations

This section expounds the experimental results of the existing technique RDAID and the proposed technique RACE. It explicates the strength of the RACE technique and how RACE achieves better results compared with RDAID technique. It also justifies how the proposed technique RACE is better than the existing technique RDAID technique.

The RDIAID technique used the packet delivery ratio to detect rank attack in the RPL network. The packet delivery ratio was calculated for each transmission and total transmission in the network. It was concluded that a node having less packet delivery ratio could cause rank attack with more possibility and a node having high packet delivery ratio could cause rank attack with less possibility.

In this research, the RDAID technique and RACE technique are deployed in the Cooja simulator and analyzed both techniques to evaluate the performance of both techniques. For evaluating the packet delivery ratio, 10, 20 and 50 nodes are taken. For 10 nodes with 3040 packets, the RACE increases packet delivery ratio by 1.4%. For 20 nodes with 6550 packets, 1.2% is increased. For 50 nodes with 16537 packets, 1% is increased.

For evaluating average of throughput, 10, 20 and 50 nodes are taken. For 10 nodes with 900 seconds, the RACE increases throughput by 3.2%. For 20 nodes 900 seconds, 2.5% is increased. For 50 nodes with 900 seconds, 2.3% is increased.

For evaluating average of attack detection accuracy, 10, 20 and 50 nodes are taken. For 10 nodes, the RACE increases throughput 1.4%. For 20 nodes, 1.3% is increased. For 50 nodes, 1% is increased.

3.9 Research Summary

There is no specific technique proposed to identify rank attack concerned with the selection of specific objective function. This research focuses specifically on the hop count based DODAG construction rank issues. This work provides the novel technique to detect and mitigate rank attack based on RSSI value while setting Hop count as an objective function. The proposed technique has been implemented with the Cooja simulator over Contiki operating System. The proposed work performs better than the existing work RDAID in terms of packet delivery ratio, throughput and attack detection accuracy.

Chapter – 4

Level Based Rank Attack Detection Technique for the Internet of Things (LEACE)

CHAPTER - 4

LEVEL BASED RANK ATTACK DETECTION TECHNIQUE FOR THE INTERNET OF THINGS (LEACE)

4.1 Background

The Internet of Things' growth was gradually increasing for a few years at the time of its start-up. After ten years, IoT has thrived in all the fields such as medical, building construction, hardware industry, software industry, social environments and transport in the world which nobody has anticipated ever before. The potential benefits of IoT are enormous in each field in the world. The Internet of Things has burgeoned to the extent that everyone knowingly or unknowingly uses the IoT services in the modern world. From the technological standpoint, IoT is the best technology for connecting each and every object in the world through the Internet. IoT has some issues such as security, data integrity, encryption capabilities, architecture and connectivity. Despite of all these issues, everyone likes to use IoT technology because of its incredible services by 24/7. Though resilience of IoT can solve IoT issues, security issues are still a pervasive issue in IoT.

The security issues are classified into network security, data security, device security and cloud security. From all these security issues, network security is the predominant issue. IoT networks can be formed using three types of protocol such as proactive, reactive and hybrid protocol. IoT mostly uses proactive protocol for forming the network. RPL protocol is one of the proactive protocols which is often used in IoT. The RPL network in IoT is susceptible to various attacks such as rank attack, sinkhole attack, black hole attack and version number attack. Finding rank

attack in RPL network is an important research in IoT security. Various techniques for detecting rank attack were proposed by many researchers. But still, there is a need to develop better rank attack detection techniques. In this chapter, level based rank attack detection technique is proposed to achieve better rank attack detection accuracy.

4.2 Related Works

In [Adi, 19], proposed atrust based mechanism to detect rank attack and sybil attack. The trust for a child and parent were calculated based on nodes' behaviours and residual energy. The trust was calculated in two methods namely direct method and indirect method. In direct method, energy depletion of parent and child was used to detect the attacks. In an indirect method, the trust value was evaluated by neighbour nodes' information. The proposed collective trust based mechanism was simulated in the Cooja simulator. It was compared with the SecTrust scheme in terms of attack detection rate, throughput and energy efficiency. The collective trust based mechanism achieved better than the SecTrust scheme.

In [Zah, 20b], a secure RPL Routing Protocol (SRPL-RP) for detecting and mitigating rank and version number attacks in Internet of Things was proposed. The detection process was done by rank comparison strategy. The mitigation process was done based on the timestamp threshold value. The proposed SRPL-RP consisted of four phases. The first phase was to monitor the timestamp threshold value. Second phase was to verify the threshold value for each node. Third phase was to keep the malicious node in the blacklist. And the fourth phase was used for mitigating the malicious node which was affected by rank and version number attacks. It was implemented in the Cooja simulator and was compared with the Sink Based Intrusion

Detection System (SBIDS). It increased packet delivery ratio and reduced the number of control messages compared with SBIDS.

4.3 Motivation

Many techniques were proposed to detect rank attacks in the Internet of Things for different applications environments. But the main aim of all the techniques was to increase attack detection accuracy. Though there are some techniques to detect rank attack, the attack detection accuracy is not sound enough in the existing works. In chapter three, RSSI based rank attack detection technique was proposed to provide better attack detection accuracy in the RPL network. The nature of the RSSI based technique works better in an obstacle free environment. The technique has not provided expected results due to the nature of RSSI. This issue motivated the next work to provide another technique with better attack detection accuracy.

4.4 Objective

Objective of this chapter is to propose Level based rank attack detection technique to increase attack detection accuracy and to eliminate the malicious nodes from the network.

4.5 Level based Rank Attack Detection Technique (LEACE)

In level based rank attack detection technique, all the nodes are divided into levels according to the rank of the nodes. The nodes having the same rank are placed in the same level. The rank of a node corresponds with its level, for example, a node which has its rank as two then it corresponds to level two. The correspondence of rank and level of the nodes are used to detect the rank attack in the RPL networks. The

node which sends its updated rank has to go for the level verification process. The rank and level of the node must be the same. If the rank of the node does not correspond with its level then the node is declared as a malicious node which is affected by rank attack. If the rank of the node is less than its correspondence then it is affected by rank decreased attack. If the rank of the node is higher than its correspondence then it is affected by rank increased attack.

RACE Technique

Input **:** RPL Control messages, L, RK
Output**:** Rank attack detection

1: RT multicasts the DIO messages
2: NR receives DIO messages and send DAO to RT
3: Compute
RK (CU) = RK(PA (CU)) + HC(CU, PA)
4: Children unicast DAO to their selected parents
5: PA sends DAO_ACK message to CH then the DODAG is constructed
6: Compute Level of each node from RT to AN based on RK of nodes
for i=0; i++; i<=n-1 // i is Index of Level, n is total number of nodes in the network
{
L_i = i+0;
}
7: Do corresponding process of nodes' rank with nodes' level
$L_i \leftrightarrow RK_j$
8: Rank attack detection process
If L (CU) = RK(CU)
CU is an legitimate node
If L (CU) < RK(CU)
CU is affected by rank increased attack
If L (CU) > RK(CU)
CU is affected by rank decreased attack
9: Isolate the affected nodes
10: Reconstruct the network

Labels used in the Technique

NHC - Number of hop count

L - Level of a node

CU - Current node

RT - Root node

NR - Neighbor nodes

RK - Rank of a node

PA - Parent node

Ch - Children

AN - All nodes in the network

4.6 Theoretical Analysis

The proposed technique theoretically analyzed the RPL network with fifteen nodes. Among fifteen nodes, one is root node, thirteen are legitimate nodes and one node is malicious node affected by rank attack. The parent selection process is done based on the hop count objective function for the given nodes. The RPL network for the given nodes without malicious nodes is given in figure 4.1.

Let N be the set of all nodes in the network

$$N = \{L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$$

Let L be the set of levels of the nodes in the network

$$L = \{L0, L1, L2, L3, L4\}$$

Let R be the set of ranks of the nodes in the network

$$R = \{R1, R2, R3, R4\}$$

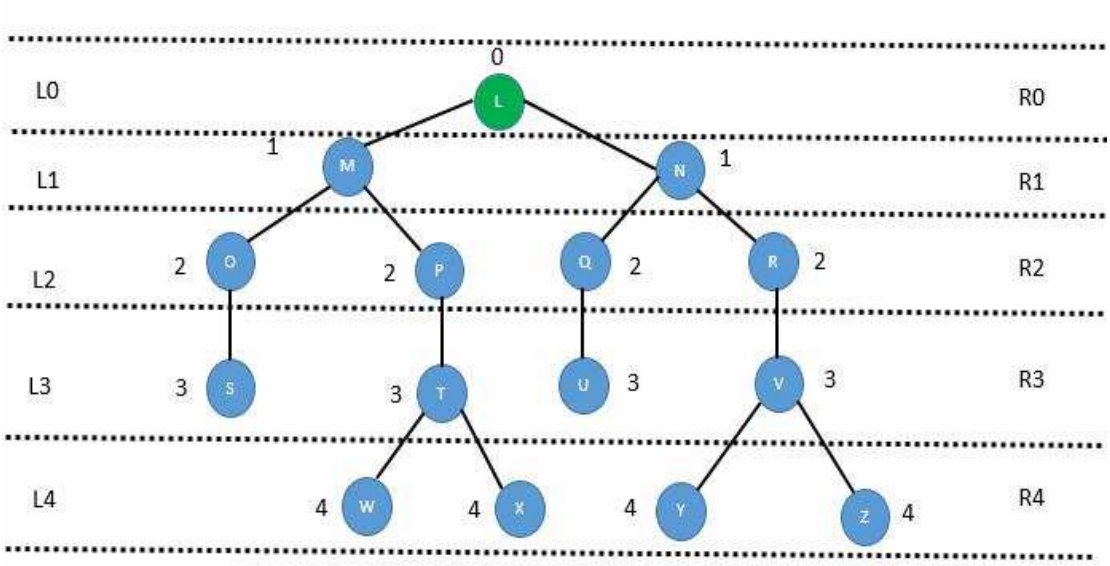


Figure 4.1 RPL Network with Rank and the Level of the Nodes

From figure 4.1, all nodes of the network are divided into different levels according to the rank of the nodes by the dot lines. The level of the nodes are placed in the left side of the figure and the corresponding rank is denoted in right side of the figure. The parent nodes in the network have the rank value lower than their children nodes. The parent selection process is done based on the hop count of the nodes. The correspondence of rank and level is separately given figure 4.2.

Figure 4.2 Correspondence of Level and Rank

Figure 4.2 depicts that the rank and level of the node must be the same in the network. If a node wants to update its rank, it has to verify its level like in the figure 4.2. Table 4.1 shows which nodes are placed in the same level in the given RPL network.

Table 4.1 Nodes with Same Rank

Level	Rank	Nodes
L0	R0	L
L1	R1	M, N
L2	R2	O, P, Q, R
L3	R3	S, T, U, V
L4	R4	W, X, Y, Z

From table 4.1, nodes having the same rank are placed in the same level. This table is stored in the root node. The level of the children nodes are sent to their parents by the root node. If a parent node identifies its child as a malicious node, it sends the information to all the nodes in the network through all possible paths in the network. The RPL network with the attacker node is shown in figure 4.3.

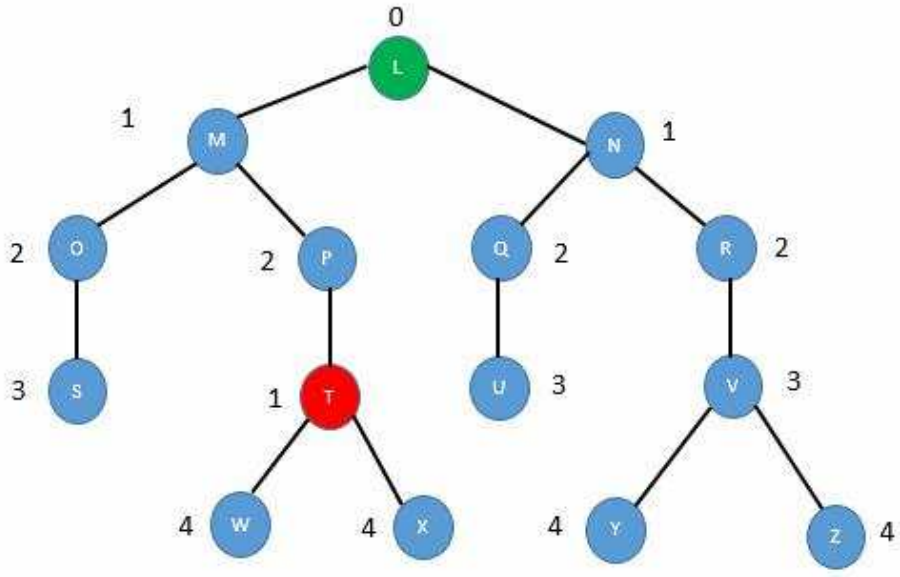


Figure 4.3 Network with Attacker Node

In figure 4.3, node T is considered as a malicious node which is affected by rank attack. The attacker node's actual rank is 3 but it broadcasts its rank as 1. Now, the attacker node has to be detected using the level of the node. The parent node checks the child node's new rank with its level. The new rank of the child is 1 but the level of the child is 3. In figure 4.2, the level of the rank does not correspond with the rank of the child. It is found that the node T is affected by rank attack. If the rank of the node is higher than the corresponding rank then the node is affected by the increased rank attack. If the node rank of the node is lesser than the corresponding level, then the node is affected by the rank decreased attack. From figure 4.3, the network is affected by the rank decreased attack because the new rank of the node is 1 and the level is 3. After detecting a rank attack, the malicious node should be isolated from the network. Figure 4.4 shows the isolation of the malicious node in the network.

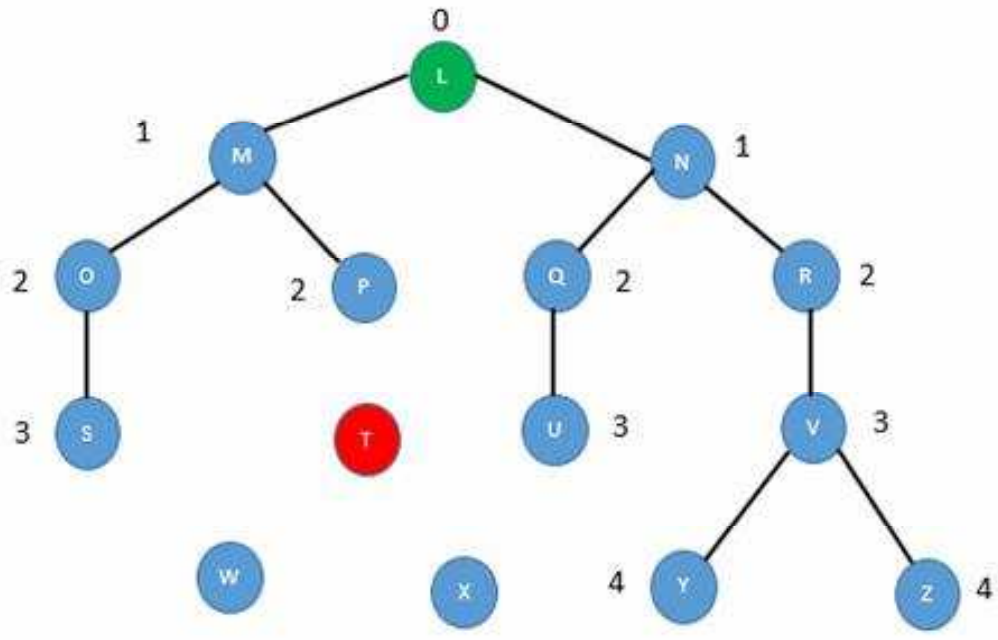


Figure 4.4 Isolation of the Malicious Node

In figure 4.4, node P is the parent of the attacker node T which broadcasts that the node T is affected by rank attack through all possible links in the network. All the nodes in the network check whether the attacker node T is connected with them in order to disconnect the connection from the attacker node T. In figure 4.4, nodes W and X are connected with the attacker node T in the network. The nodes W and X disconnect their connection from the attacker node T after listening to the node P in the network. After the disconnection of the attacker node T from the nodes W and X from the network, the attacker node T is isolated. After the isolation process, the network has to be reconstructed with available legitimate nodes in the network. The nodes W and X have to send DIS to probe that the nodes are within the communication range for them. Figure 4.5 shows the reconstruction of the network after isolating the attacker node from the network.

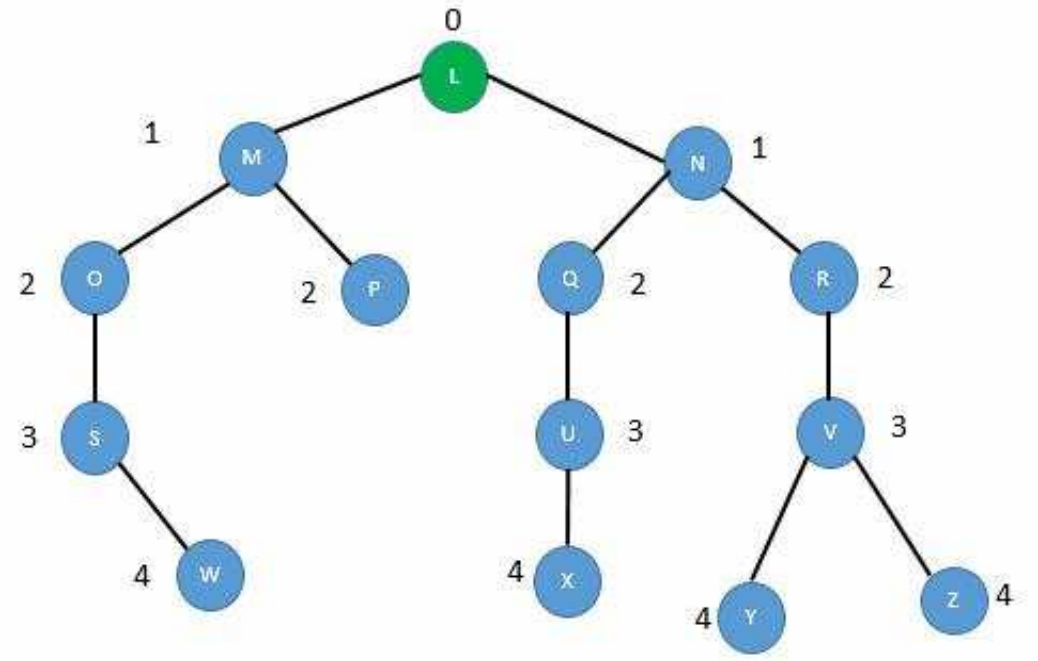


Figure 4.5 Reconstruction of the RPL Network

From figure 4.4, the malicious node T is removed from the network and reconstructed the network with available legitimate nodes. Nodes W and X were connected in the attacker node T. But after identifying the node T as an attacker node, node W joined with node S which is within the communication range of the node W and node X is joined with node U which is within the communication range of the node U. After the connection of these two nodes W and X, new DODAG is formed in the reconstruction process.

4.7 Simulation Results and Discussions

Cooja simulator is used to simulate the level based rank attack detection technique on Contiki operating system. Cooja simulator is the best simulation tool for simulating IoT networks. So, it has been chosen for implementing the proposed work. Cooja can be accessed even in VMware also. But for this work, a physical computer with the Cooja simulator is used. The network parameters used in the level based rank attack detection technique are given in table 4.2.

Table 4.2 Simulation Parameters

Parameters	Description
No. of Nodes	10, 20, 50
Simulation Area	1000 x 1000 m
Data Rate	250kbps
Node Arrangement	Random
Operating System	Contiki
Simulator	Cooja
Types of Sensor Node	Sky Mote
Packet Analyzer	Wireshark

Based on the parameters the Cooja simulator is configured for simulating the level based rank attack detection technique. The simulation setup for the given number of nodes is given in the next section.

4.7.1 Network Setup

The RPL network is configured as shown in table 4.2 for implementing the level based rank attack detection technique. The Cooja uses different types of mote such as sky mote, Z1 mote and ESB mote for the simulation process. According to many researchers, sky mote is the suitable mote for implementing RPL networks. So, sky mote is chosen for implementing the proposed technique. Sets of nodes such as ten, twenty and fifty are taken for testing the proposed work with three cycles. In the first cycle, ten nodes are used. In the second cycle, twenty nodes are used and in the final cycle fifty nodes are used. Each node in the network is placed randomly in a simulation environment. Figure 4.6 shows the implementation of ten nodes in the Cooja simulator.

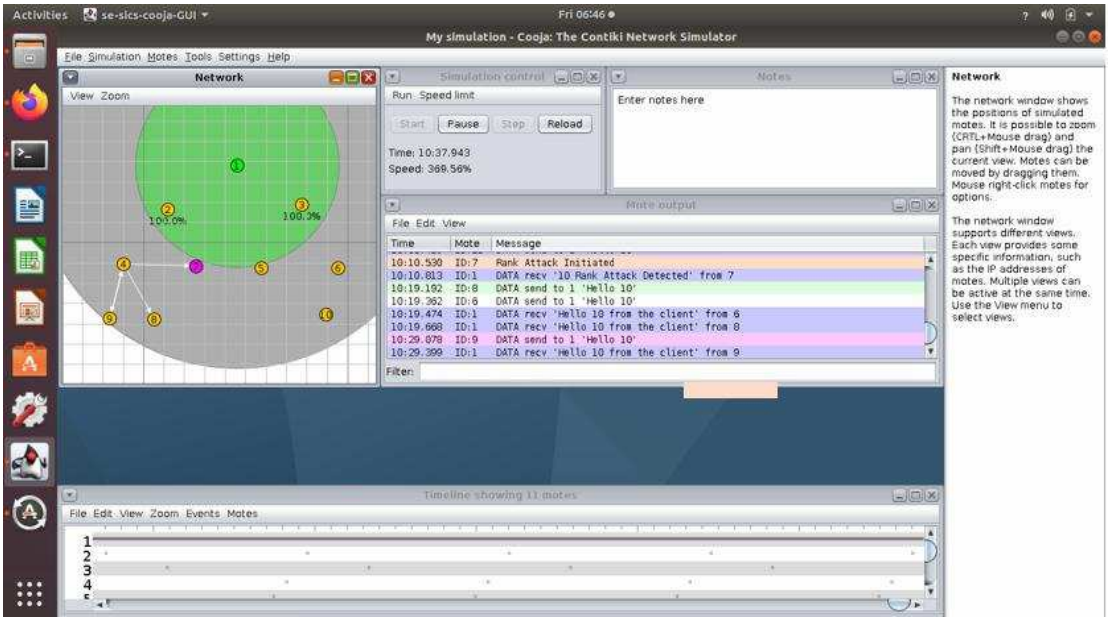


Figure 4.6 RPL Network with 10 Nodes

From figure 4.6, the node types such as root node, legitimate node and malicious node are presented in different colours in the simulation environment. The node 1 is a root node presented in green colour. The legitimate nodes 2, 3, 4, 5, 6, 8, 9, 10 are presented in yellow colour. And the malicious node 7 is presented in pink colour. After the configuration process is over, the simulation can be executed by clicking "start" button in the simulation control window. The rank attack detection message is shown in the Mote Output window. Figure 4.7 shows rank attack detection process with twenty nodes.

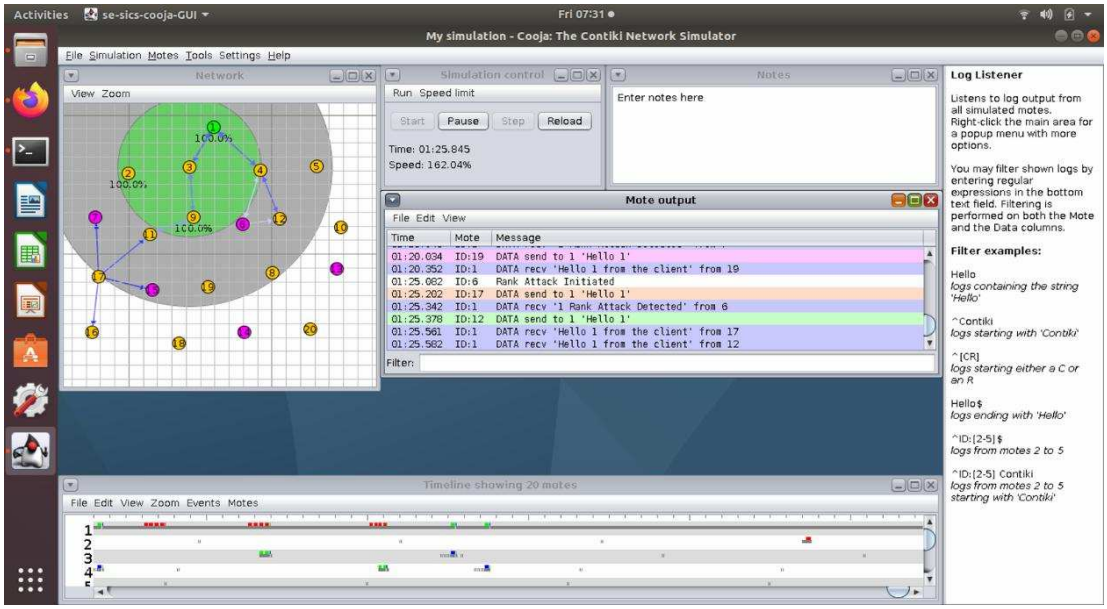


Figure 4.7 RPL Network with 20 Nodes

In figure 4.7, the nodes are deployed as follows: one node is the root node, five nodes are malicious nodes and fourteen nodes are legitimate nodes. The root node 1 is indicated with green colour, the legitimate nodes 2, 3, 4, 5, 8, 9, 10, 11, 12, 16, 17, 18, 19 and 20 are indicated in yellow colour and malicious nodes 6, 7, 13, 14 and 15 are indicated in pink colour. Figure 4.8 explicates the implementation process with fifty nodes.

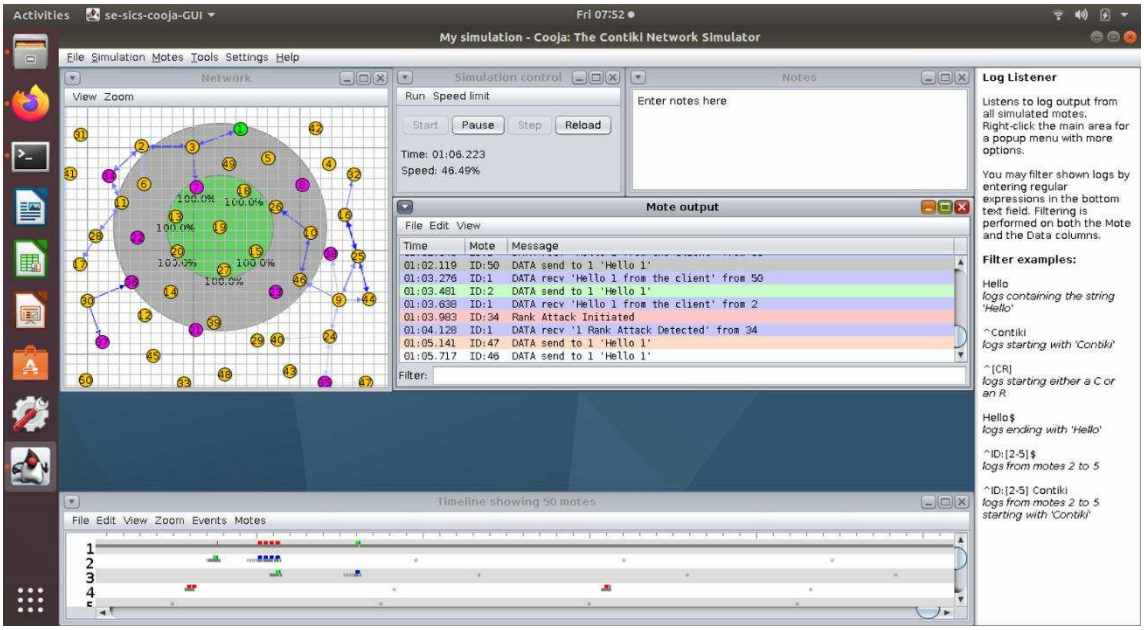


Figure 4.8 RPL Network with 50 Nodes

In figure 4.8, three types of nodes are set up in the Cooja simulator such as root node, legitimate nodes and malicious nodes. Among the set up nodes, one node is the root node, ten nodes are malicious nodes and thirty nine nodes are legitimate nodes. The root node is represented in green colour, the legitimate nodes are represented in yellow colour and malicious nodes are represented in pink colour.

4.7.2 Evaluation Metrics

The proposed technique is evaluated using three evaluation metrics such as packet delivery ratio, throughput and attack detection accuracy. The three metrics are compared with the RACE technique with 10, 20 and 50 nodes.

Packet Delivery Ratio

Packet delivery ratio is calculated based on the packets sent and received by the nodes. The formula for calculating the packet delivery ratio is given in chapter 3.7. The packet delivery ratio of RACE technique is compared with the packet delivery

ratio of the LEACE technique. Table 4.3 shows the packet delivery ratio of the RACE and LEACE. The comparison chart of the RACE and LEACE is given in figure 4.9 as a bar chart.

Table 4.3 PDR in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RACE	93.1	92.7	91
LEACE	94.2	93.8	92.3

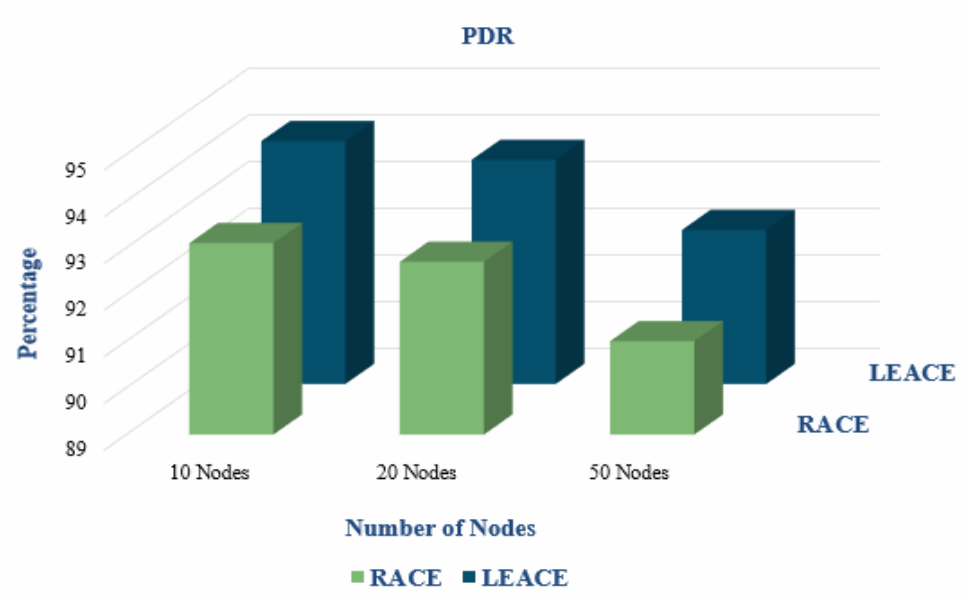


Figure 4.9 Packet Delivery Ratio Analysis

From figure 4.9, it is proved that LEACE technique performs better than the RACE technique in packet delivery ratio. The green colour bar represents the packet delivery ratio of the RACE technique. The dark teal colour bar represents the packet delivery ratio of the LEACE technique.

Throughput

Throughput is calculated based on the successful rate of the packets received in the network. The formula for calculating the throughput is given in chapter 3.7.

The throughput value for the technique LEACE and RACE are given in table 4.4. The comparisons of throughput for these two techniques are given in figure 4.10 as a bar chart.

Table 4.4 Throughput in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RACE	93.2	92	91.5
LEACE	94	93.1	92.4

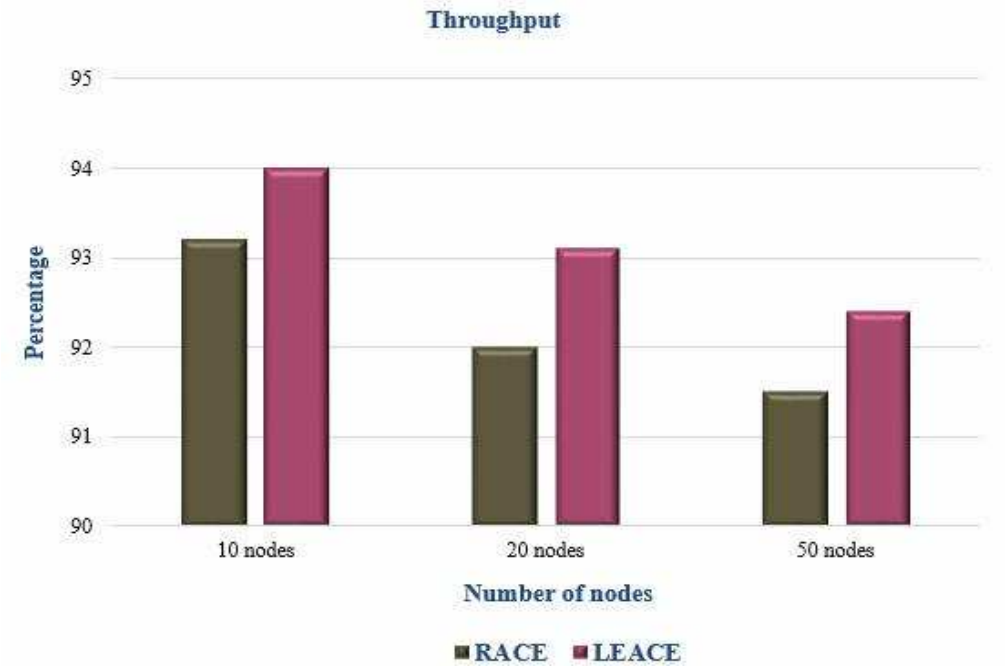


Figure 4.10 Throughput Analysis

From figure 4.10, the bar chart exposes that the throughput of the LEACE technique is better than the RACE technique.

Attack Detection Accuracy

Attack detection accuracy is calculated using the confusion matrix. The formula for the confusion matrix is given in chapter 3.7. The performance of the RACE and LEACE technique in terms of attack detection accuracy is given in the table 4.5. The performance is compared visually using the bar chart in figure 4.11.

Table 4.5 Attack Detection Accuracy in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
RACE	93	92.5	91
LEACE	94.2	93.7	92.1

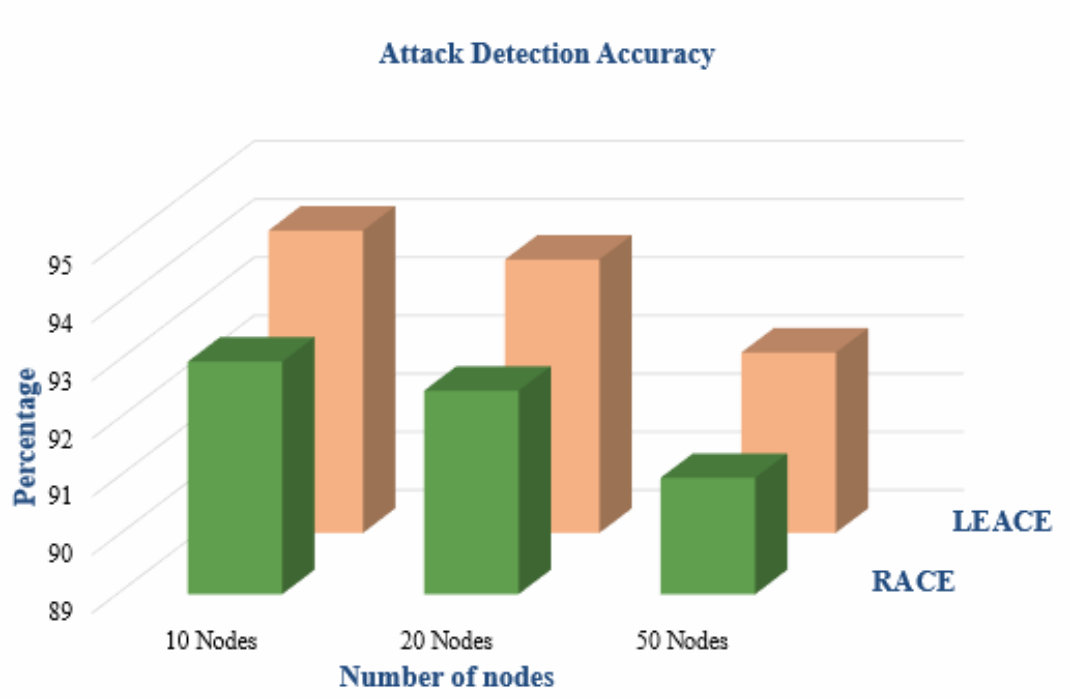


Figure 4.11 Attack Detection Accuracy (ADA) Analysis

Attack Detection Accuracy of the LEACE technique is given in light orange colour and the Attack Detection Accuracy of the RACE technique is given in green colour in figure 4.11. It is proved that LEACE technique performs better than the RACE technique.

4.8 Findings and Interpretations

This chapter explicates the key finding of the LEACE technique. It analyzes the results with RACE technique and shows the potential of the LEACE technique with the RACE technique. This chapter also defends how the proposed technique

LEACE is superior compared with RACE technique. The LEACE technique works better than the RACE technique in terms of packet delivery ratio, throughput and attack detection accuracy.

The RACE technique used the Received Signal Strength Indicator (RSSI) to find the rank attack in RPL protocol. It calculated the RSSI value of each node in the network as well as calculated the RSSI of a node towards the root node. The RACE technique utilized the nature of the RSSI in the technique. The nature of RSSI is, a node which is very near to the root node will get the good RSSI value. Based on the RSSI value, the attacker node is detected in RACE technique. But RACE technique is not suitable when there is an obstacle. Because, RSSI value won't be detected correctly in obstacles areas. The LEACE technique solves the issue in the RACE technique. The LEACE technique detects the attack even in the obstacles areas.

The findings of LEACE technique in terms of packet delivery ratio, throughput and attack detection accuracy for 10, 20 and 50 nodes are evaluated with the findings of RACE technique in terms of packet delivery ratio, throughput and attack detection accuracy for 10, 20 and 50 nodes. For 10 nodes with 900 seconds, the LEACE technique increases packet delivery ratio by 1.1%, throughput by 0.8% and attack detection accuracy by 1.2%. For 20 nodes with 900 seconds, the LEACE technique increases packet delivery ratio by 1.1%, throughput by 1.1% and attack detection accuracy by 1.2%. For 50 nodes with 900 seconds, the LEACE technique increases packet delivery ratio by 1.3%, throughput by 0.9% and attack detection accuracy by 1.1%.

4.9 Research Summary

In this chapter, the LEACE technique is proposed to overcome the issue in the RACE technique and increase attack detection accuracy and eliminate the malicious nodes which are affected by the rank increased and rank decreased attack. The LEACE technique uses the level and rank of the nodes to identify the malicious node in the RPL based IoT network. The proposed technique LEACE corresponds the level and rank of the node to detect the rank attack. The LEACE technique works better than the RACE technique in terms of packet delivery ratio, throughput and attack detection accuracy. The technique is evaluated in Cooja simulator over the Contiki operating system with 10, 20 and 50 nodes. Though, LEACE works better than the RACE technique, there is a need to improve the attack detection accuracy.

Chapter – 5

Location Based Rank Attack Detection Technique for the Internet of Things (LACE)

CHAPTER - 5

LOCATION BASED RANK ATTACK DETECTION TECHNIQUE FOR THE INTERNET OF THINGS (LACE)

5.1 Background

The Internet of Things is one of the latest technologies which connects the objects in the world through the Internet. IoT can connect billions of objects. The connected objects can communicate among each other. IoT is the emblematic of the smart systems. The systematic work of IoT is used in all the fields such as medical, sports, agriculture, transport and retail. IoT is the confluence of several technologies such as Artificial Intelligence, Cloud Computing and Machine Learning. It changes the ordinary human life into smart life by making the entire human work as an automation process using sensors and IoT equipped devices.

The IoT technology has grown threefold in recent years. But, there is no unique architecture for IoT. Many researchers and IoT users have accepted the most widely used three layered architecture with perception layer, network layer and application layer. Among these three layers, the network layer plays a vital role in IoT. In the network layer, routing is the major work which routes the collected data securely. Routing protocol for low power and lossy network (RPL) is one of the routing protocols in IoT.

RPL makes directed acyclic graph to form a network. The network is formed based on the objective functions such as hop count, expected transmission count (ETX) and energy. Four control messages are used to form directed acyclic graph in RPL. Various attacks occur in RPL protocol. But rank attack is the most severe attack. Though there are few techniques proposed to detect the rank attack in IoT, there is a

need to increase the attack detection accuracy. In this chapter, location based rank attack detection technique (LACE) is proposed to increase the rank attack detection accuracy.

5.2 Related Works

Usman Shafique et al. [Usm, 18] proposed Sink Based Intrusion Detection System (SBIDS) to detect rank attack in RPL network. Parent switching threshold mechanism was used to detect the rank attack in the sink node itself. The proposed technique is used in non-storing mode. The rank attack was detected when a node got a lesser rank than the parent switching threshold value. This technique was implemented in a random topology environment using Contiki operating system and Cooja network simulator. SBIDS technique gave better results for packet delivery ratio, attack detection accuracy and end to end delay.

Somnath Karmakar et al. [Som, 21] proposed low overhead rank attack detection for securing RPL based IoT. This technique is deployed in non-storing mode in RPL. It was used to detect rank increased attack and rank decreased attack in RPL based IoT networks. In this technique, message authentication code was used to authenticate control messages in the RPL network. It was theoretically proved and simulated in the Cooja simulator over the Contiki operating system. The technique was compared with SBIDS. It achieved better results than the SBIDS in terms of attack detection accuracy, energy consumption and false positive/negative rate.

5.3 Motivation

The Internet of Things has drawn more attention in the contemporary world. Everyone in the world is moving towards smart work. IoT makes ordinary work into

smart work by switching to automation. Though there are many benefits from IoT, there would be many issues too. Among several issues, attacks against RPL in the network layer is a more noticeable issue. So, this issue is enthralled to propose the rank attack detection technique in IoT.

5.4 Objective

Objective of this chapter is to propose a Location based rank attack detection technique (LACE) to increase attack detection accuracy and eliminate the malicious nodes from the network.

5.5 Location based Rank Attack Detection Technique (LACE)

The location based rank attack detection technique (LACE) is proposed to increase rank attack detection accuracy in RPL based Internet of Things. Computing rank is very important in the RPL protocol. The rank of the node is calculated based on the objective function. The technique is used for hop count based RPL networks. In hop count based RPL network, the rank of a node is calculated by hops' count to reach the parent/root node. The location of a node in the network is identified by computing the node's distance towards the root node using Manhattan distance formula. Since, IoT is resource constraint technology, it supports low energy for computation process. Manhattan consumes low energy and memory for computation process compared with other methods. So, Manhattan is chosen for computing distance among several methods.

In this LACE technique, the RPL network is constructed based on hop count. The location of each node towards its parent and root node is identified by calculating its distance. The distance of each node is stored in the root node. Each node in the

network multicasts its rank periodically to the connected nodes. In RPL, the parent is selected based on the rank. The node which has lesser rank than the other neighbour nodes in the network is selected as preferred parent. So, the parent node is nearer than its child/children in the network. In the same way, the distance of the parent node must be lesser than its child/children in the network. If there is any inconsistent change in the rank and the distance, the rank and distance of a node is evaluated with its parent. If a node is having higher rank and lower distance than its parent, then the node is affected by rank increased attack, if a node is having lower rank and higher distance than its parent, then it is affected by rank decreased attack. The evaluation process is done in the root node. Because, the root has the information about all the nodes in the network. After finding the malicious node, it is isolated from the network. The network is reconstructed with the legitimate nodes after eliminating the attacker nodes from the network.

LEACE Technique

Input **:** RPL Control messages, Distance of a node
Output**:** Rank attack detection
1: X multicasts the DIO message and followed by N to start DODAG construction
X, N $\Longrightarrow$ Yi
2: Yi receive and accept DIO message
3: Compute R
R(K)= R(P) + HC(K, P)
R(P) < R(K)
4: Child Node unicasts DAO message to its selected preferred parent node
C $\longrightarrow$ P
5: P sends DAO_Ack message to C then the DODAG is constructed
6: Identify nodes' location by calculating distance (D) for all nodes from K to P and K to X
D = | x2-x1| + |y2-y1|
7: If R(K) > R(P(K)) &&D(P(K)) < D(K) then
K is legitimate node

8: If R(K) < R(P(K)) &&D(P(K))> D(K) then
K is affected by Rank Decreased Attack then remove K from the network
9: If R(K) < R(P(K)) &&D(P(K)) D(K) then
K is affected by Rank increased Attack then remove K from the network
10: Form the new network after eliminating malicious nodes

Labels used in the Technique

X - Root node

P - Parent node

N - Nodes in the network

Y - Neighbor nodes

K - Current node

R - Rank of a node

C - Child node

5.6 Theoretical Analysis

This section delineates the key concept of the LACE technique. The theoretical analysis clarifies the conceptualization of the proposed technique LACE. The theoretical analysis exemplifies clearly how to identify the rank attack and how to handle the affected nodes in the RPL network. The elimination of the affected nodes and the reconstruction of the RPL network after eliminating the affected nodes are illustrated clearly in the theoretical analysis section. The RPL network is given in such away to understand the concept of RPL with nodes' rank and distance in figure 5.1 for the LACE technique. The logic behind the LACE technique is analyzed and epitomized with ten nodes (A, B, C, D, E, F, G, H, I, J) by encompassing one root (A) node and nine children nodes (B, C, D, E, F, G, H, I, J) in RPL network is given in figure 5.1.

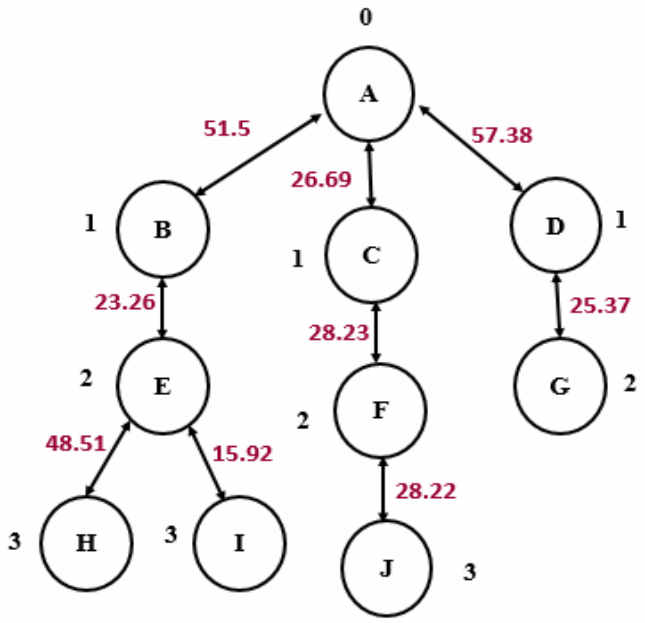


Figure 5.1 RPL Network with Nodes' Rank and Distance

For each node, the distance is calculated using the Manhattan equation and denoted the distance in figure 5.1. The X and Y value for the Manhattan equation is taken from the Cooja simulator by designing the RPL network. The rank of each node is also given in figure 5.1 itself. Figure 5.2 represents the nodes' distance from a node to the root node.

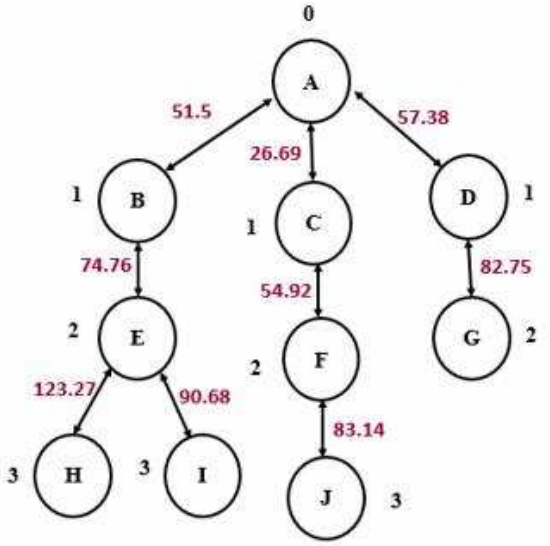


Figure 5.2 Nodes' Distance towards Root Node

Figure 5.1 represents only nodes' rank and the distance from a node to its parent node. But Figure 5.2 represents the distance of each node towards the root node. The distance is measured in meters for the given network. The table 5.1 shows the required information about each node for the proposed technique LACE.

Table 5.1 Nodes' Information

Node	Parent	Rank	X	Y	Distance to its parent	Distance to the root
A	---	0	76.42	23.14	---	---
B	A	1	46.95	45.17	51.5	51.5
C	A	1	78.29	47.96	26.69	26.69
D	A	1	112.7	44.24	57.38	57.38
E	B	1	45.71	67.19	23.26	74.76
F	C	2	81.70	72.78	28.23	54.92
G	D	2	111.4	70.91	25.37	82.75
H	E	3	126.17	96.66	48.51	123.27
I	E	3	56.88	94.28	15.92	90.68
J	F	3	82.94	99.76	28.22	83.14

In table 5.1, the parent of each node, rank of each node, distance towards a node to its parent and the distance from a node towards the root node are given clearly. The distance of a node to its parent is calculated by taking the X and Y values of a node and its parent. In the same way, for calculating the distance of a node towards the root node, the X and Y values of a node and the root node are taken from the table which is stored in the root node. The LACE technique uses this table for identifying whether a node is located near or far from the root node to detect the rank attack. Figure 5.3 shows the rank attack scenario for a given network.

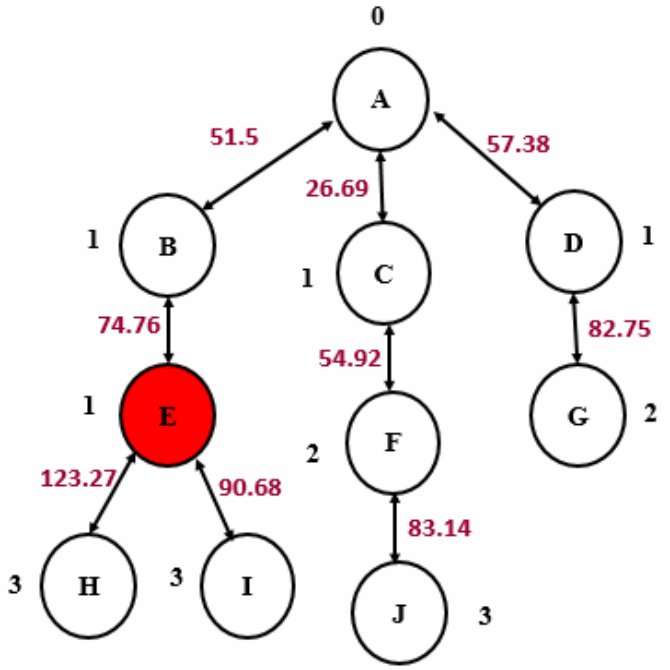


Figure 5.3 Rank Attack Scenario

In figure 5.3, the node E is considered as a malicious node which is affected by rank decreased attack. The malicious node E has changed its rank into one. But the actual rank of the node E is two. So, there is an inconsistent change in the rank. To identify the affected node in the network, the distance of the node and its parent towards the root node is verified from table 5.1. The distance of the node towards the root node is 74.76 meters and the distance of the parent of node E towards the root is 51.5. So, it is identified that the node E is located far from the root node but broadcasts its rank as one. It is declared that the node E is affected by the rank decreased attack. In the same way, the nodes' distance is verified whenever there is an inconsistent change in the rank of parent and the child. After identifying the malicious node, the root node will multicast that the node is affected by the rank attack. The malicious nodes are isolated from the network. Figure 5.4 shows the isolation of the malicious node in the network.

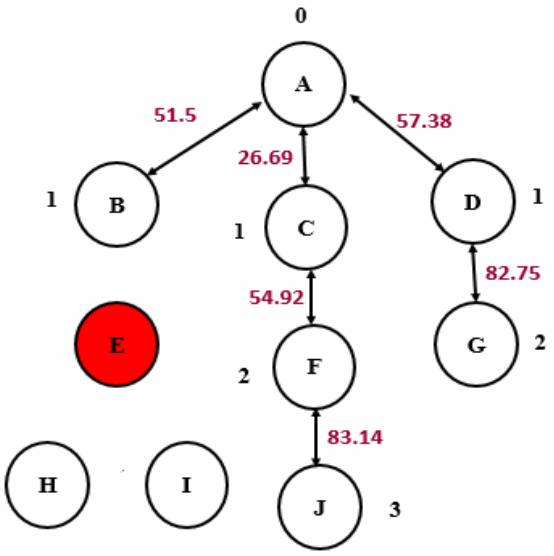


Figure 5.4 Isolation of the Malicious Node

In figure 5.4, after receiving the message from the root node, all nodes connected to node E are disconnected. The node E is isolated from the network. After the isolation process, the network is reconstructed with the legitimate nodes (B, C, D, F, G, H, I, J). The nodes' information is/are updated in the root node when the reconstruction is over. The reconstruction of the network is shown in figure 5.5.

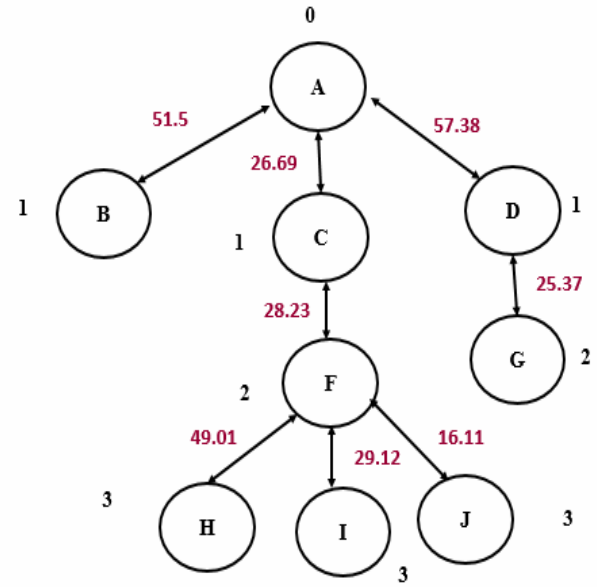


Figure 5.5 Reconstruction of the Network

In figure 5.5, the reconstruction network with nodes' rank and the distance towards the parent is clearly depicted. After isolating the malicious node E, the new DODAG is constructed by broadcasting the control messages to form the new network. Nodes H and I which were connected with node E are connected with node F now. Once malicious node is isolated, the nodes connected with the malicious node are disconnected from the node and seek for the parent to form the network.

5.7 Simulation Results and Discussions

One of the efficient network simulation tools for the Internet of Things is the Cooja simulator. Many researchers proposed the Cooja simulator for simulating the IoT network. So, for implementing the proposed location based rank attack detection technique for Internet of Things, the Cooja simulator is used with the support of Contiki operating system. Table 5.2 represents the list of parameters taken for simulating the proposed work.

Table 5.2 Simulation Parameters

Parameters	Description
No. of Nodes	10, 20, 50
Simulation Area	1000 x 1000 m
Data Rate	250kbps
Node Arrangement	Random
Operating System	Contiki
Simulator	Cooja
Types of Sensor Node	Sky Mote
Packet Analyzer	Wireshark

5.7.1 Network Setup

It is so easy to set up the network environment in the Cooja simulator. As mentioned in table 5.2, the network setup is configured for 10, 20 and 50 nodes in random positions with sky mote. The nodes in the simulator can be dragged and dropped in any places in the network setup window. The node represented in green colour is the root node. The yellow colour nodes are legitimate nodes. And the pink colour nodes are malicious nodes. Firstly, a set of ten nodes is configured to test the proposed work. Figure 5.6 shows the simulation process with 10 nodes.

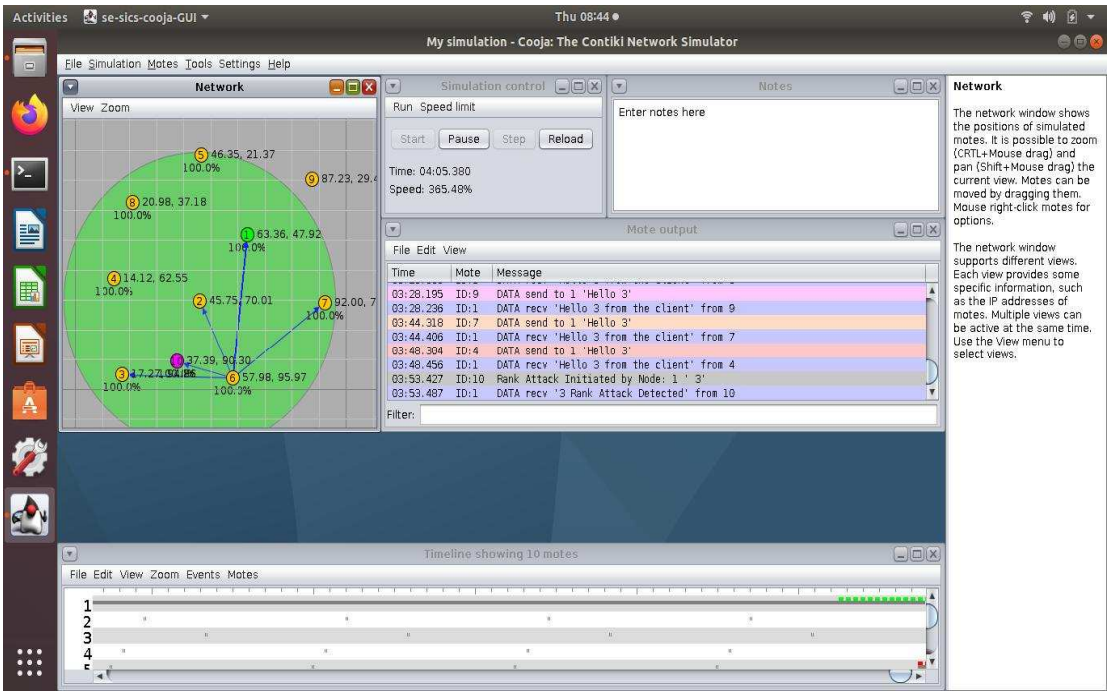


Figure 5.6 Simulation Window for 10 Nodes

Among the 10 nodes, one is root node and eight nodes are legitimate nodes and one node is a malicious node which is affected by rank attack. Secondly, 20 nodes are taken. Figure 5.7 shows the simulation process with 20 nodes for detecting the rank attack.

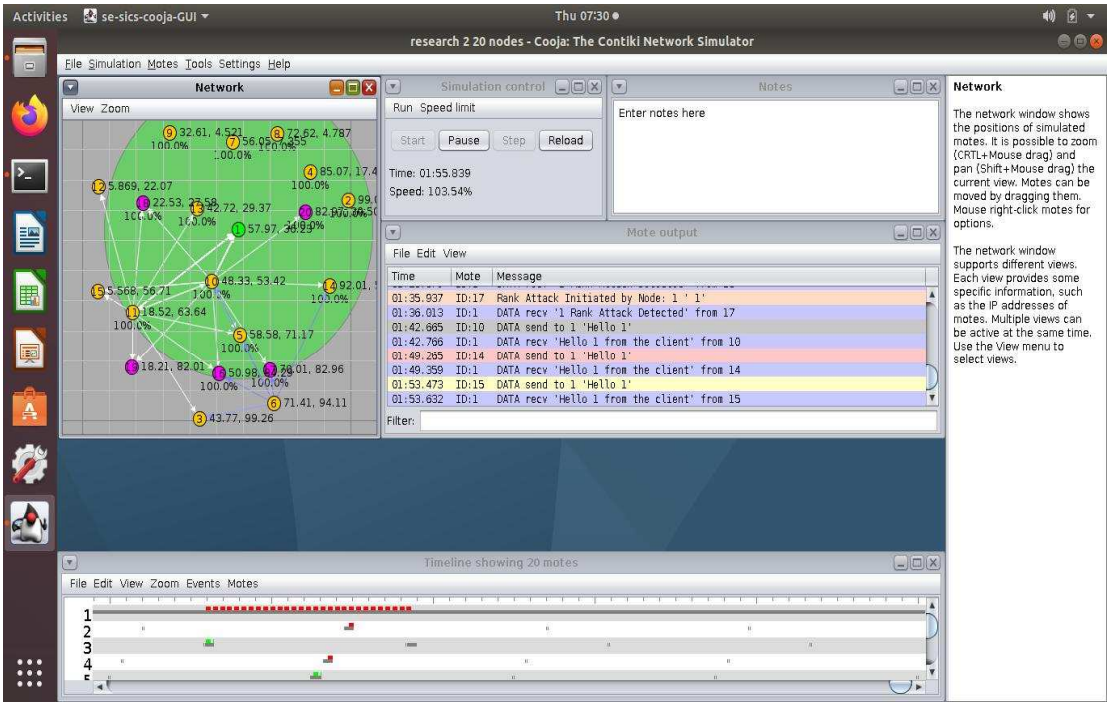


Figure 5.7 Simulation Window for 20 Nodes

Among the 20 nodes, one node is the root node, five nodes are set as malicious nodes and other fourteen nodes are legitimate nodes in the network.

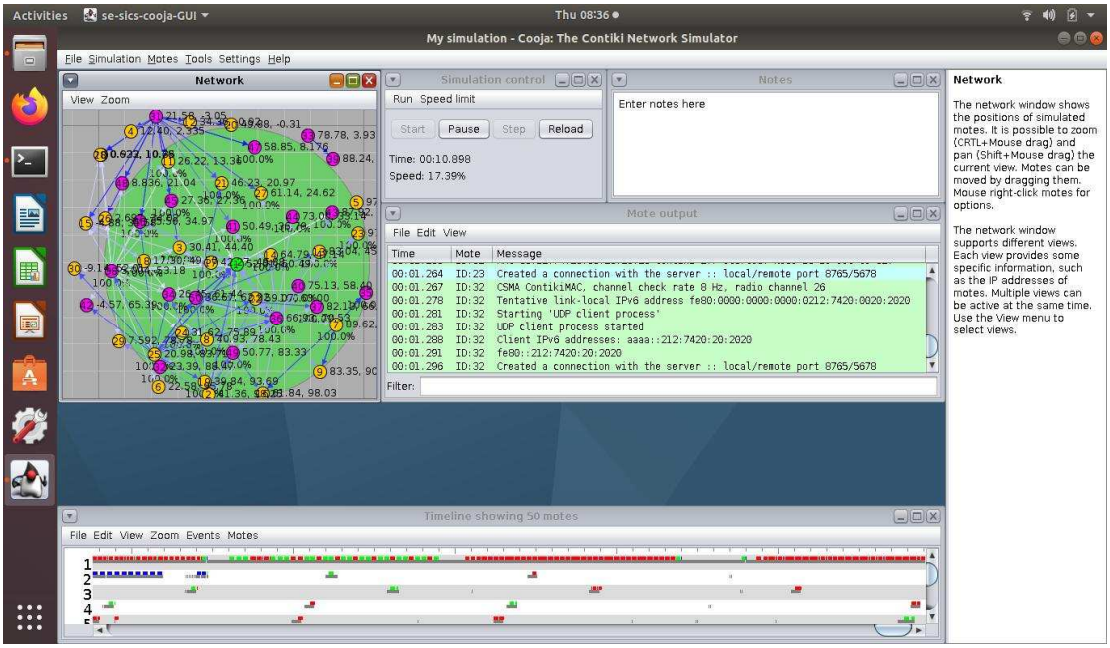


Figure 5.8 Simulation Process with 50 Nodes

In figure 5.8, the simulation is done with 50 nodes which is consisted of one root node ten malicious nodes and thirty nine legitimate nodes.

5.7.2 Evaluation Metrics

LACE technique detects the rank attack in RPL based IoT networks. But, it has to be evaluated with other two techniques such as RACE and LEACE. For evaluating the proposed technique "LACE", three metrics are used such as Packet Delivery Ratio (PDR), throughput and attack detection accuracy. The formulas for this three metrics are given in chapter 3.7.

Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is one of the evaluation metrics for analyzing the rank attack detection technique. There is more possibility for packet loss when the network is affected by the rank attack. The packet delivery ratio of the proposed technique is compared with LEACE technique. Table 5.3 shows the packet delivery ratio comparisons with the LEACE and LACE techniques. LEACE technique is proved to yield better PDR than the RACE technique. Figure 5.9 shows graphical representation of the comparisons of LEACE and LACE techniques using bar chart according to the number of nodes taken for the simulation.

Table 5.3 PDR in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
LEACE	94.2	93.8	92.3
LACE	95	94.5	92.9

Figure 5.9 Packet Delivery Ratio Analysis

The X axis represents the number of nodes taken and the Y axis represents the packet delivery ratio in percentage. The LEACE technique is differentiated by the blue colour bar and the LACE technique is differentiated by the tan colour bar in the chart. From figure 5.9, it is clearly depicted that the proposed technique LACE provides better packet delivery ratio than the LEACE technique.

Throughput

The second metric which is used for evaluating the proposed technique is Throughput. Throughput is chosen to calculate the packets which are successfully received for a particular time unit in the given network. The throughput comparison for LEACE and LACE technique is given in table 5.4. The bar chart is used to differentiate the LEACE and LACE technique and to give the graphical representation of the comparison between two techniques.

Table 5.4 Throughput in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
LEACE	94	93.1	92.4
LACE	95.5	94.3	93

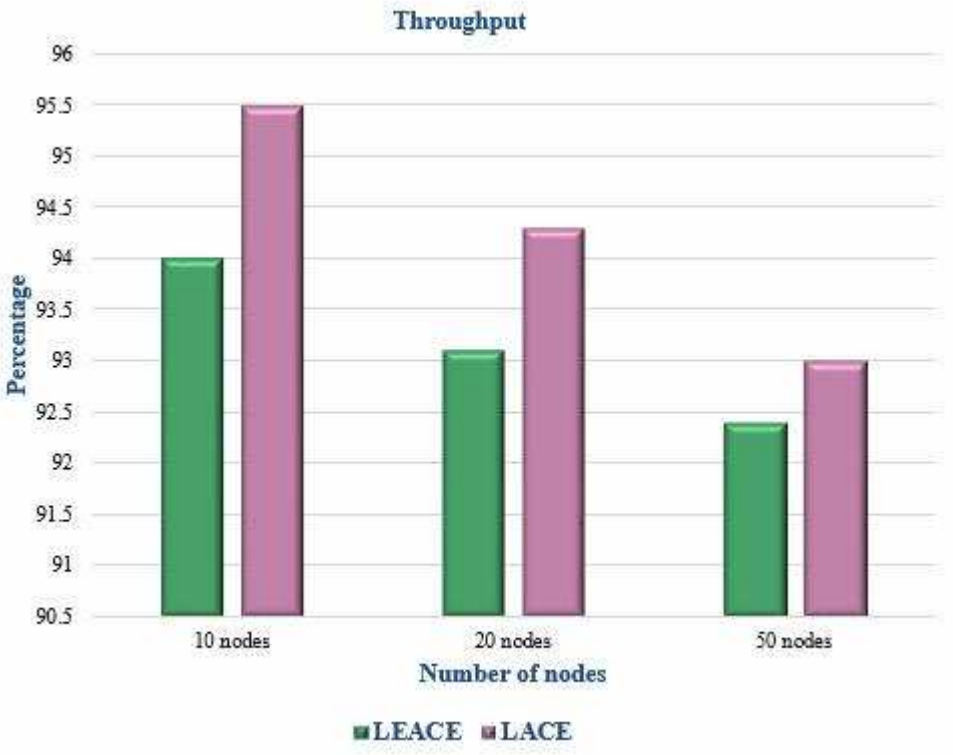


Figure 5.10 Throughput Analysis

Throughput is analyzed using the bar chart which is given in figure 5.10. LEACE technique is represented in green colour and the LACE technique is represented in light pink colour. From figure 5.10, it is exposed that the LACE technique performs better than the LEACE technique in terms of throughput.

Attack Detection Accuracy

Among these three evaluation metrics, attack detection accuracy plays the major role in the rank attack detection. Based on the attack detection accuracy only,

the techniques are analyzed whether the proposed technique is better than the other techniques for detecting the rank attack in the Internet of Things environment. Table 5.5 shows the comparisons of LEACE and LACE techniques for attack detection accuracy. Figure 5.11 depicts the analysis of the attack detection accuracy for LEACE and LACE techniques.

Table 5.5 Attack Detection Accuracy in Percentage

Techniques	10 Nodes	20 Nodes	50 Nodes
LEACE	94.2	93.7	92.1
LACE	95.5	94.7	93

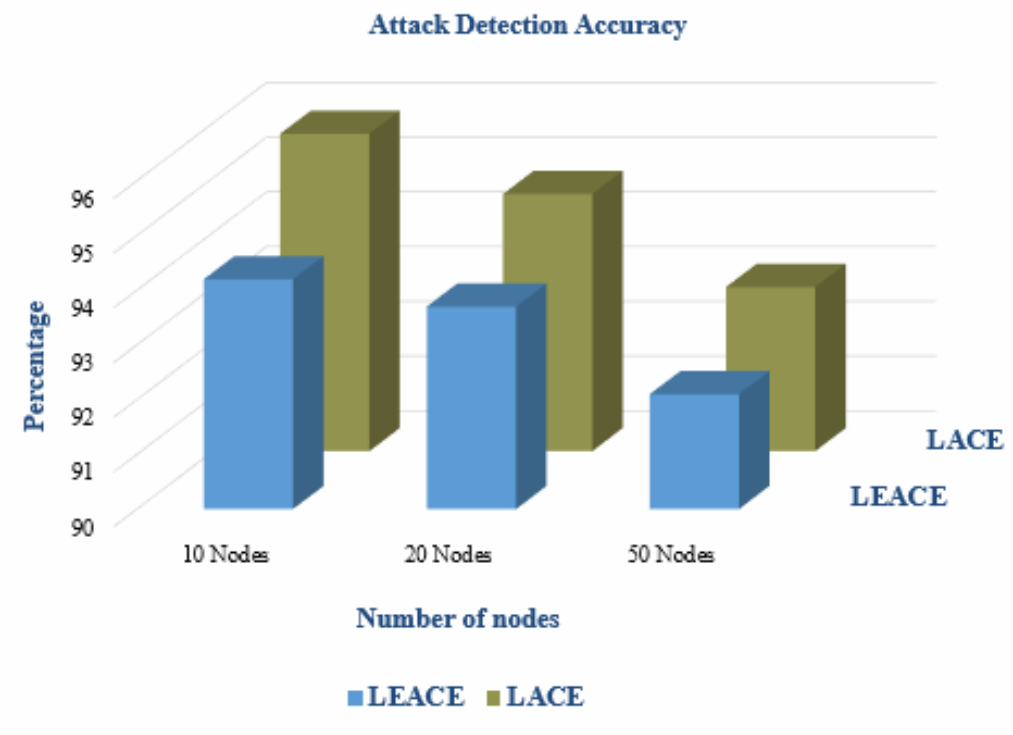


Figure 5.11 Attack Detection Accuracy Analysis

The blue colour bar represents the LEACE technique and the tan colour bar represents the LACE technique in the bar chart given in figure 5.11.

5.8 Findings and Interpretations

This section summarizes the key findings of the proposed technique and how the proposed technique is competed with other techniques in terms of packet delivery ratio, throughput and attack detection accuracy. LACE technique is compared and interpreted with the LEACE technique. LEACE technique used level and rank of each node for detecting rank attack in RPL based Internet of Things. There was a difficulty in detecting the rank attack when the nodes were in the same level. So, to solve this issue LACE technique is proposed.

Set of nodes are taken such as 10, 20 and 50 and simulated based on the proposed technique in the Cooja simulator for 900 seconds. The LACE technique achieves better result than the LEACE technique in terms of packet delivery ratio, throughput and attack detection accuracy. The LACE technique increases packet delivery ratio by 0.8% for 10 nodes, 0.7% for 20 nodes and 0.6% for 50 nodes. The LACE technique increases through put by 1.5% for 10 nodes, 1.2% for 20 nodes and 0.6% for 50 nodes. The LACE technique increases the attack detection accuracy by 1.3% for 10 nodes, 1% for 20 nodes and 0.9% for 50 nodes.

5.9 Research Summary

In this chapter, location based rank attack detection technique (LACE) is proposed to detect the rank attack in Internet of Things. This technique uses the location of a node by identifying the node's distance towards the root node. The distance is calculated using the Manhattan distance formula. Since Manhattan is very simple to calculate distance, it has been chosen for the proposed work. The technique is simulated with a set of nodes such as ten, twenty and fifty nodes in the Cooja

simulator. Compared with RACE and LEACE techniques, LACE technique outperforms better in terms of packet delivery ratio, throughput and attack detection accuracy. The key findings of this chapter are clearly interpreted and distinguished with the RACE and LEACE techniques.

Chapter – 6

STARO Framework

CHAPTER - 6

STARO FRAMEWORK

6.1 Background

The Internet of Things is an emerging technology which fascinates the human beings with its tremendous applications throughout the world. IoT provides extraordinary service through the IoT applications. Confidential data are communicated and transferred through the IoT network from the IoT applications. Framework is used to utilize the IoT applications efficiently. There are many frameworks that are proposed for using IoT applications powerfully. Though there are many frameworks are available for IoT, there is a need to provide secure framework.

This chapter provides the framework called STARO Framework for smart hostel environment. It provides the solution for the rank attack for obstacle free and obstacle environment in IoT.

6.2 Related Works

Faisal Hussain et al. [Fai, 21] designed a framework to detect the malicious traffic in IoT healthcare environment. The framework consisted of six modules such as use case setup, traffic generation, traffic capturing IoT data set creation, classifying the traffic and the output process module. The framework used machine learning algorithms to classify the normal traffic and the malicious traffic. There were six machine learning algorithms tested to classify the traffic, among the six algorithms Random Forest Classifier performed better than others in terms of precision, recall and accuracy.

6.3 Objective

Objective of this chapter is to propose a framework to detect rank attack for obstacle zone and obstacle free zone in Internet of Things. The proposed framework selects the suitable technique for detecting rank attack according to the obstacle zone and obstacle free zone.

6.4 STARO Framework

STARO Framework is proposed to secure the RPL based IoT network from the Rank attack. Three techniques such as RACE, LEACE and LACE are utilized in the framework according to the environment such as obstacle zone and obstacle free zone. In IoT, the major obstacles could be path loss due to weak signal. The maximum path loss is occurred by the nature of the heterogeneity characteristics of IoT. The IoT environment is connected by various communication technologies such as WiFi, Bluetooth, Near Field Communication (NFC) and other conventional communication technologies. The STARO Framework is given in figure 6.1.

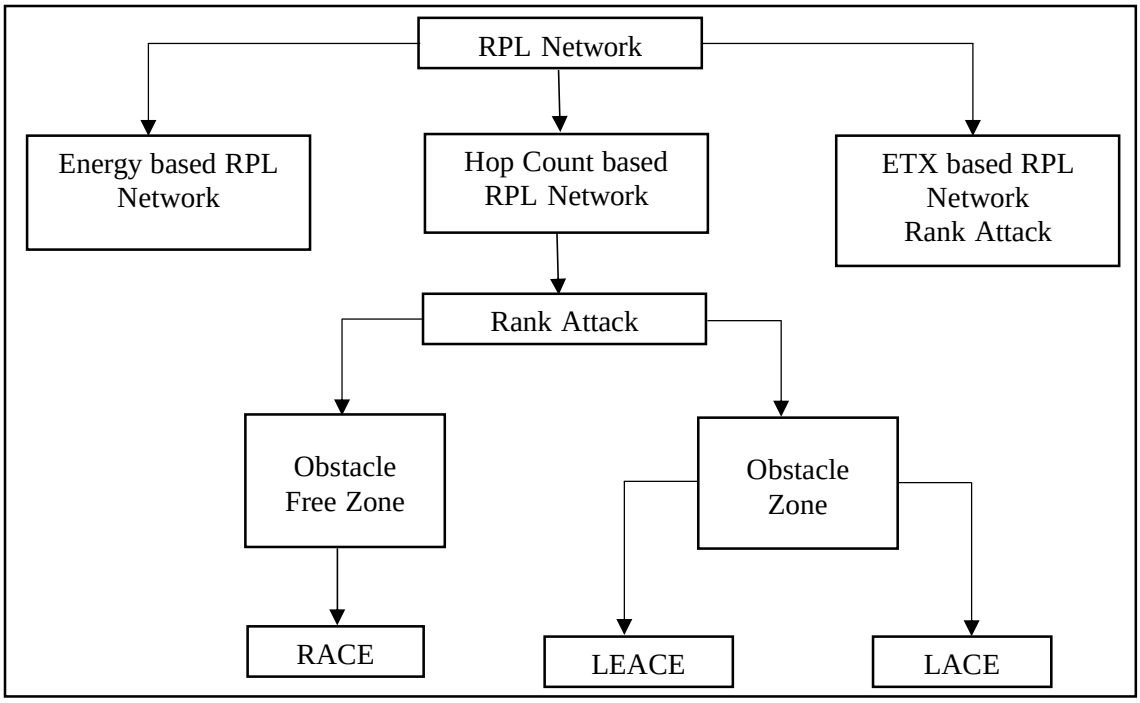


Figure 6.1 STARO Framework

From figure 6.1, for securing the RPL network in the Internet of Things for the obstacle free zone, the RSSI based rank attack detection technique (RACE) is selected. There are several obstacles are faced while using IoT technology. Weak signal in the network is one of the obstacles in IoT. So, the weak signal is considered as the obstacle in the framework. The level based rank attack detection technique (LEACE) or location based rank attack detection technique (LACE) can be selected for the obstacle zone. The techniques are deployed in the root node to detect the rank attack. Because the root node of the network has the information about all the nodes in the network.

From figure 6.1, Framework checks whether the network is constructed using the hop count objective function. Then it checks whether the RPL network is affected by rank attack or not. Once these two process is over, the environment is chosen based on the signal quality. If it is weak signal then the LACE or LEACE is selected, else RACE is selected.

STARO Framework Working Model

Input **:** STARO Framework
Output**:** Rank attack detection

1: Deploy the STARO framework in RPL based IoT network
2: Check whether RPL based IoT network is constructed by Hop Count
   If yes, proceed for the next process go to step 3
   If no, terminates the process
3: Check whether the RPL network is affected by rank attack
   If yes, utilize the STARO framework go to step 4
   If no, exit from the framework
4: Check whether it is obstacle zone or obstacle free zone
5: If obstacle free zone select RACE technique to detect rank attack
   If obstacle zone select LEACE or LACE technique to detect rank attack
6: End the process

6.5 Experimental Results and Discussions

STARO Framework is implemented in the smart hostel environment in Bellarmine Hostel, St. Joseph's College, Trichy, Tamil Nadu, India. Arduino Integrated Development Environment (IDE) is used to write and upload code. C and C++ programming are used in the Arduino IDE. NodeMCU ESP8266 is a WiFi enabled microcontroller which is used as a node in the smart hostel. Hardware such as relay, jumper wires, 12V battery and small fan are used. And sensors such as gas sensor, ultrasonic sensor and temperature sensors are used in the smart hostel.

In the three proposed techniques, LACE technique is deployed in STARO framework for the smart hostel. Based on the Cooja simulation result, LACE technique is chosen for the smart hostel because it gives better attack detection accuracy compared with other two techniques. Smart hostel is designed with five nodes. Among the five nodes, one is root node and other nodes are child nodes of the root node. The framework with the LACE deployment process model structure is shown in figure 6.2.

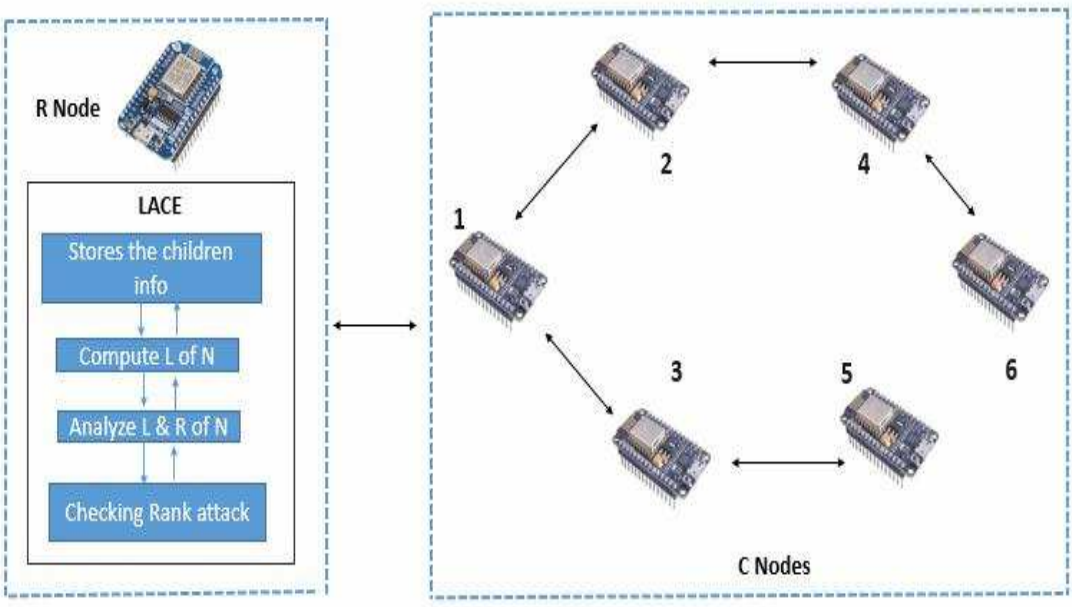


Figure 6.2 STARO Framework for Smart Hostel with LACE Technique Model

From figure 6.2, the L denotes the location, R denotes rank and N denotes node. The deployment of the STARO Framework with LACE technique for smart hostel is clearly depicted in figure 6.2. The root node stores the information about the children and compute the location of the node. Then the location and rank of the nodes are analyzed for identifying the rank attack in the smart hostel. The real time implementation of the smart hostel is shown figure 6.3.

Figure 6.3 Smart Hostel

The Bellarmine smart hostel is used to collect the hostel environmental conditions and collect the number students coming and going from the hostel. Figure 6.4 shows the nodes fixed in the hostel.

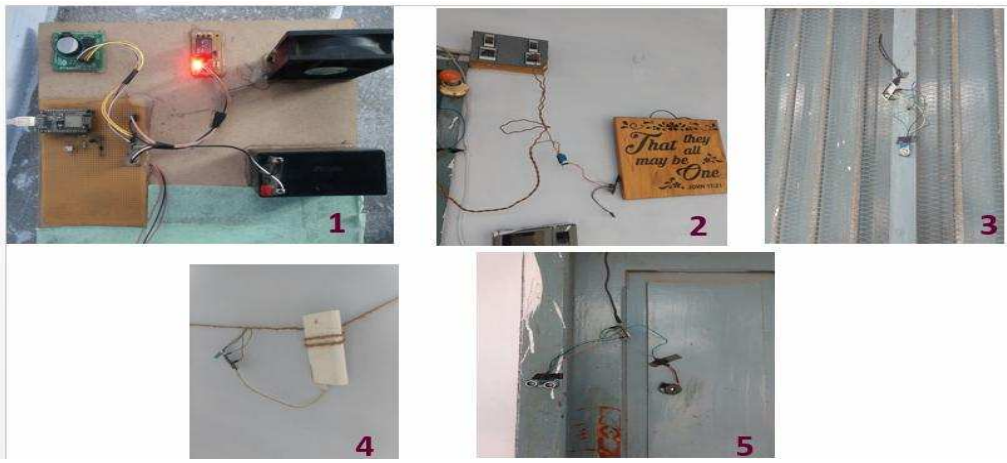


Figure 6.4 Nodes in Smart Hostel

In this environment, the STARO Framework is deployed to identify the rank attack in the smart hostel. The rank attack identification message will be displayed in the serial monitor which is there in the Arduino IDE.

6.6 Research Summary

The proposed STARO Framework is used to identify the rank attack in RPL based IoT networks. The STARO Framework is deployed in the smart hostel. The framework utilizes three techniques such as RACE, LEACE and LACE. The Framework chooses any one of the techniques based on the environment. The environments classified in the STARO Framework are obstacle free environment and obstacle environment.

Chapter – 7

Conclusion

CHAPTER - 7

CONCLUSION

7.1 Overview

The technology “Internet of Things (IoT)” gives comfort zone for the mankind. IoT makes difficult works of human into very simple work through the automation system. The physical objects in the world are interconnected by the IoT technology using Internet. Million and billons of objects can be connected through IoT technology. IoT brought the revolution in the digital era. The usage of the IoT is spreading everywhere to make the life more sophisticated by the automation process. IoT cracks into all the fields and provides better service for twenty four hours in all the fields. In one hand, the usage of IoT increases and other hand the issues also raising very fast as quick as bunny. There are lots of issues in IoT. But network related issues are the most common problems which clog the IoT network.

Routing Protocol for Low power and Lossy Networks (RPL) is one of the routing protocols which is often used in IoT network. The attacks against the RPL protocol strike the network services. Among several attacks, rank attack attenuates the network services and causes more security problem in the network. Many researchers grasp at straws for the rank attack. Only few techniques and methods are proposed to tackle the rank attack. Many techniques are quick fix for the rank attack but there is a need to think out of the box according to the characteristics of the IoT to provide better solution for rank attack.

This chapter epitomizes the entire research work. It exposes how the research work provides security against rank attack in RPL based Internet of Things. This

chapter explicates the key concept and future direction of the research according to the behavior of the RPL protocol in IoT. The goal of the research is spotlighted in this chapter.

7.2 Summary of the Research Work

The research work is about the rank attack detection techniques in Internet of Things. The research work consists of three techniques such as RSSI based rank attack detection technique (RACE), Level based rank attack detection technique (LEACE) and Location based rank attack detection technique and a framework namely STARO which is used to utilize the three techniques in RPL based Internet of Things. The techniques are novel and working better for identifying the rank attack.

7.2.1 RSSI based Rank Attack Detection Technique (RACE)

The first technique in the research work is RSSI based rank attack detection technique (RACE). The Received Signal Strength Indicator based rank attack detection is the novelty of this technique. The technique consists of three phases namely DODAG construction phase (DCP), TRRX Computation phase (TRCP) and Attack detection phase (ADP). In the DCP, the DODAG is constructed using hop count objective function. Several objective functions are used in RPL protocol for constructing the DODAG to form the network but hop count is taken as objective function for this research. TRRX computation phase is the core phase of this technique. The RSSI value of each node is calculated towards its parent node. And, the total RSSI value of each node towards the root node is calculated using the intermediator nodes. The rank attack is identified using the RSSI value of each node and its total RSSI value towards the root node. The TRRX value of the parent should be greater than its children

nodes. If the TRRX value of a parent is lesser than its child node, then it is declared that the parent node is affected by the rank attack. After identifying the malicious node, the node is removed from the network. Once the malicious node is removed from the network, the network is reconstructed with available legitimate nodes. Since RSSI is signal based, it works better for detecting the rank attack in obstacle free IoT environment.

7.2.2 Level based Rank Attack Detection Technique (LEACE)

Level based rank attack detection technique (LEACE) is the second technique in the research work. The motivation of the LEACE technique is to solve the problem identified in RSSI based rank attack detection technique (RACE). It is difficult to detect rank attack in obstacle zone using the RACE technique. To solve the identified problem in RACE, the LEACE technique is proposed. In LEACE technique, the nodes are divided into levels according to the rank of the nodes. The nodes which are having the same rank are placed in same level. In this technique, the level and rank of a node is synchronized with each other. The level and rank of the node should be same. The rank and level of the node is checked when node updates its rank and broadcasts to the neighbour nodes. If the rank and level of a node are not same then the node is affected by the rank attack and declared as the malicious node. After detecting the malicious node, the node is removed from the network and new network is formed. It works even in the obstacle zone. But, there is a need to improve attack detection accuracy in this technique.

7.2.3 Location based Rank Attack Detection Technique (LACE)

Location based rank attack detection technique (LACE) is the last technique proposed for detecting the rank attack. The second technique LEACE is lacking in

attack detection accuracy. To solve this issue, the LACE technique is proposed. In this technique, the location of each node is identified by finding the distance using Manhattan distance. The distance of each node towards the root node is calculated and stored in the root node. When a node's distance is less, it is near to the root node. When a node's distance is high, the node is far from the root node. The distance of parent node should be lesser than its child node. If a node's distance is lesser than its parent node then the node is affected by the rank attack. The affected node is removed from the network and a new network is formed with the available nodes.

7.2.4 STARO Framework

STARO Framework is used to utilize these three proposed techniques efficiently according to the environments such as obstacle free zone and obstacle zone in IoT. The framework provides the way to select the rank attack detection techniques based on the environment. If the environment is obstacle free zone, the RACE technique is selected. If the environment is obstacle zone, the LEACE or LACE technique is selected. The STARO Framework is implemented in smart hostel with LACE technique. NodeMCU 8266 is taken as node in the smart hospital. Five nodes and few sensors are installed in the smart hostel. Rank attack free smart hostel is created by deploying the STARO Framework in the smart hostel. The root node takes care of the responsibility of monitoring the children nodes. If any malicious node is detected, the root node will broadcast the message to all nodes in the network.

Simulation Tool

Cooja simulator and Contiki operating system are used to simulate all three techniques. Cooja is the best simulation tool for simulating the IoT networks. It

provides the full-fledged IoT environment setup for the users. It is very easy to deploy any IoT based techniques to analyze the IoT networks. To analyze the techniques, three sets of nodes are taken for simulation such as 10 nodes, 20 nodes and 50 nodes. Though various motes are available, sky mote is the suitable one for analyzing the RPL network in IoT environment. All nodes are set in the random position.

Performance Metrics

There are various metrics available for analyzing the performance of the network. But the research work is fully focused on detecting the rank attack in RPL network in the IoT environment. So, Attack detection accuracy, packet delivery ratio and throughput are taken to analyze the performance of the proposed three technique. Attack detection accuracy is the major metric in the performance analysis process.

7.3 Summary of Research Findings

This section brings the key findings of each technique and analyzes the techniques based on the performance metrics. The results of the performance metrics of each technique are compared with the existing technique for sets of nodes such as 10 nodes, 20 nodes and 50 nodes. The first technique RACE is compared with existing technique RDAID technique. RACE uses RSSI of each node to detect the rank attack and RDAID uses packet delivery ratio to detect the rank attack. RACE technique achieves better result than the RDAID technique. The second technique LEACE is compared with RACE technique. LEACE uses the level of each node and the rank to detect the rank attack in the network. LEACE outperforms than the RACE technique. The third technique LACE used location of the node to detect the rank attack. It is compared with LEACE technique. It performs better than LEACE technique. Table 7.1

shows the key findings of the three techniques according to the number of nodes taken for the simulation process.

Table 7.1 Key Findings of All Three Techniques

No. Nodes	10 Nodes			20 Nodes			50 Nodes		
Technique	**RACE**	**LEACE**	**LACE**	**RACE**	**LEACE**	**LACE**	**RACE**	**LEACE**	**LACE**
PDR	93.1%	94.2%	95%	92.7%	93.8%	94.5%	91%	92.3%	92.9%
Throughput	93.2%	94%	95.5%	92%	93.1%	94.3%	91.5%	92.4%	93%
A.D.A.	93%	94.2%	95.5%	92.5%	93.7%	94.7%	91%	92.1%	93%

7.4 Future Directions

Internet of Things is chosen for doing research. There are various issues in Internet of Things. But only the network layer issues are selected. To narrow down the research, rank attack issues in RPL is focused. In this research work, techniques are proposed only to detect the rank attack in RPL networks. These techniques cannot be used to detect other attacks such as blackhole attack, wormhole attack, version number attack and sinkhole attack. And also, there are several objective functions such as hop count, ETX and energy are used for constructing the RPL network. But this research selects the hop count based RPL network only. The techniques cannot be used for other objective functions based network.

For implementation purpose, three sets of nodes are taken such as 10, 20 and 50. The techniques work better for these sets of nodes. In future, different sets of nodes can be used to simulate the RPL network to detect the rank attack. The random position environment is chosen for the simulation in the Cooja simulator, other environments can be selected to test the rank attack detection process in the Cooja simulator.

Only three metrics are selected to analyze the performance of these three proposed techniques. There are other metrics such as end to end delay, bandwidth and

congestion which can be used to measure the performance of the techniques. The suitable metrics which are interrelated with attack detection accuracy are better to use for analyzing the recommended techniques. The proposed technique is implemented for smart hostel. In future, other IoT applications will be tested with these techniques. And also, the techniques can be enhanced much better to increase the attack detection accuracy. Other technologies like Artificial Intelligence, Machine Learning and Deep Learning can be used in rank attack detection techniques to increase the attack detection accuracy.

References

REFERENCES

[Abb, 21] Abbas Shah Syed, Daniel Sierra Sosa, Anup Kumar and Adel Elmaghraby, "IoT in Smart Cities: A Survey of Technologies, Practices and Challenges", Smart Cities, Volume 4, Issue 2, pp. 429-476, 2021.

[Abd, 16] Abdul Rehman, Meer Muhammad Khan, M. Ali Lodhi and Faisal Bashir Hussain, "Rank Attack using Objective Function in RPL for Low Power and Lossy Networks", International Conference on Industrial Informatics and Computer Systems (CIICS), pp. 1-5, DOI: 10.1109/ICCSII.2016.7462418, 2016.

[Abd, 20] Abd Mlak Said, Aymen Yahyaoui, Faicel Yaakoubi and Takoua Abdellatif, "Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure", International Conference on Smart Homes and Health Telematics, Springer, Cham, DOI: 10.1007/978-3-030-51517-1_3, pp. 28-40, 2020.

[Abd, 21] Abdur Rahim, Md. Arafatur Rahman M.M. Rahman, A. Taufiq Asyhari, Md. Zakirul Alam Bhuiyan and D. Ramasamy, "Evolution of IoT-enabled Connectivity and Applications in Automotive Industry: A Review", Vehicular Communications, Volume 27, ISSN 2214-2096, pp. 1-15, 2021.

[Abh, 20] Abhiram MSD, Jyothsnavi Kuppili and N. Alivelu Manga, "Smart Farming System using IoT for Efficient CropbGrowth", IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), DOI: 10.1109/SCEECS48394.2020.147, pp. 1-4, 2020.

[Abh, 19] Abhishek Singh, Ashish Payal and Sourabh Bharti, "A Walkthrough of the Emerging IoT Paradigm: Visualizing Inside Functionalities, Key Features, and Open Issues", Journal of Network and Computer Applications, Volume 143, pp. 111-151, 2019.

[Adi, 20] Aditya Sai Srinivas T and S.S. Manivannan, "Prevention of Hello Flood Attack in IoT using Combination of Deep Learning with Improved Rider Optimization Algorithm", Computer Communications, Volume 163, pp. 162-175, 2020.

[Adi, 19] Aditya Tandon and Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT", IEEE, Twelfth International Conference on Contemporary Computing (IC3), Noida, India, DOI:10.1109/IC3.2019.8844935, pp. 1-7, 2019.

[Agn, 13] Agnieszka Brachman, "RPL Objective Function Impact on LLNs Topology and Performance", Internet of Things, Smart Spaces and Next Generation Networking, Springer, pp. 340-351, 2013.

[Ahm, 13] Ahmad Salehi, M. A. Razzaque, Parisa Naraei and Ali Farrokhtala. "Detection of Sinkhole Attack in Wireless Sensor Networks", IEEE, International Conference on Space Science and Communication (IconSpace), pp. 361-365, 2013.

[Ahm, 20] Ahmet Aris and Sema F. Oktug, "Analysis of the RPL Version Number Attack with Multiple Attackers", IEEE, International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-8, 2020.

[Ale, 18] Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal and Laurence T. Yang, "Analytical Model for Sybil Attack Phases in Internet of Things", IEEE, Internet of Things Journal, Volume 6, Issue 1, pp. 379-387, 2018.

[Amo, 16] Amol Dhumane, Rajesh Prasad and Jayashree Prasad, "Routing Issues in Internet of Things: A Survey", Proceedings of the International Multi Conference of Engineers and Computer Scientists, Volume 1, ISBN: 978-988-19253-8-1, pp. 1-9, 2016.

[And, 21] Andrea Agiollo, Mauro Conti, Pallavi Kaliyar, Tsung Nan Lin and Luca Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT", IEEE Transactions on Network and Service Management, Volume 18, Issue 2, pp. 1178-1190, 2021.

[Anh, 13] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen and Michael Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks", IEEE Sensors Journal, Volume 13, Issue 10, 2013.

[Ann, 18] Anna Triantafyllou, Panagiotis Sarigiannidis and Thomas D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges and Trends", Wireless Communications and Mobile Computing, DOI:10.1155/2018/5349894, pp. 1-24, 2018.

[Ant, 16] Anthea Mayzaud, Remi Badonnel and Isabella Christment, “A Taxonomy of Attacks in RPL-based Internet of Things”, International Journal of Network Security, Volume 18, Issue 3, pp. 459-473, 2016.

[Ant, 17] Anthea Mayzaud, Remi Badonnel and Isabelle Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", IEEE Transactions on Network and Service Management, Volume 14, Issue 2, pp. 472-486, 2017.

[Aru, 21] Arul Anitha A and Arockiam L, "VeNADet: Version Number Attack Detection for RPL based Internet of Things", Solid State Technology, Volume 64, Issue 2, pp. 2225-2237, 2021.

[Ate, 18] Atena Shiranzaei and Rafiqul Zaman Khan, "An Approach to Discover the Sinkhole and Selective Forwarding Attack in IoT", Journal of Information Security Research, Volume 9, Issue 3, pp. 107-118, 2018.

[Asi, 21] Asif Ali Laghari, Kaishan Wu, Rashid Ali Laghari, Mureed Ali and Abdullah Ayub Khan, "A Review and State of Art of Internet of Things (IoT)", Archives of Computational Methods in Engineering, DOI: 10.1007/s11831-021-09622-6, pp. 1-9, 2021.

[Avi, 16] Avijit Mathur, Thomas Newe and Muzaffar Rao, "Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT", Sensors, Volume 16, Issue 1, pp. 1-25, 2016.

[Bar, 18] Baraq Ghaleb, Ahmed Al Dubai, Elias Ekonomou, Ayoub Alsarhan, Youssef Nasser, Lewis Mackenzie and Azzedine Boukerche, "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-power and Lossy Networks: A Focus on Core Operations", IEEE Communications Surveys & Tutorials, Volume 21, Issue 2, pp. 1607-1635, 2018.

[Bha, 20] Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy and Srikanta Patnaik, "Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology", Volume 11, DOI:/10.1016/j.iot.2020.100227, pp. 1-50, 2020.

[Bha, 19] Bhalaji N, K. S. Hariharasudan and K. Aashika, "A Trust based Mechanism to Combat Blackhole Attack in RPL Protocol", International Conference on Intelligent Computing and Communication Technologies, pp. 457-464, 2019.

[Bha, 21] Bharti Rana, Yashwant Singh and Pradeep Kumar Singh, "A Systematic Survey on Internet of Things: Energy Efficiency and Interoperability Perspective", Transactions on Emerging Telecommunications Technologies, Volume 32, Issue 8, pp. 1-41, 2021.

[Bou, 20] Boudouaia, Adda Ali Pacha, Abdelhafid Abouaissa and Pascal Lorenz, “Security Against Rank Attack in RPL Protocol”, IEEE Xplore, Volume 34, Issue 4, pp. 133-139, 2020.

[Car, 16] Carolina V. L. Mendoza and Joao H. Kleinschmidt, "Defense for Selective Attacks in the IoT with a Distributed Trust Management Scheme", IEEE, International Symposium on Consumer Electronics (ISCE), pp. 53-54, 2016.

[Cha, 19] Chandni and Rakesh Kumar, "Trust Based Technique for the Mitigation of Version Number Attack in Internet of Things", International Journal of Recent Technology and Engineering (IJRTE), Volume 8, Issue 3, pp. 1197-1203, 2019.

[Chr, 15] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606-611, 2015.

[Cri, 21] Cristina Stolojescu Crisan, Calin Crisan and Bogdan Petru Butunoi, "An IoT-Based Smart Home Automation System", Sensors, Volume 21, Issue 11, pp. 1-23, 2021.

[Dam, 20] Damian Arellanes and Kung Kiu Lau, "Evaluating IoT Service Composition Mechanisms for the Scalability of IoT Systems", Future Generation Computer Systems, Volume 108, pp. 827-848, 2020.

[Dan, 16] Danilo Evangelista, Farouk Mezghani, Michele Nogueira and Aldri Santos, "Evaluation of Sybil Attack Detection Approaches in the Internet of Things Content Dissemination", Wireless Days (WD), pp. 1-6, 2016.

[Dav, 19] David Airehrour, Jairo A Gutierrez and Sayan Kumar Ray, "SecTrust-RPL: A Secure Trust-aware RPL Routing Protocol for Internet of Things", Future Generation Computer Systems, Springer, Volume 23, pp. 860-876, 2019.

[Dee, 19] Deepti Sehrawat and Nasib Singh Gill, "Smart Sensors: Analysis of Different Types of IoT Sensors", IEEE, International Conference on Trends in Electronics and Informatics (ICOEI), pp. 523-528, 2019.

[Ele, 14] Eleonora Borgia, “The Internet of Things vision: Key Features, Applications and Open Issues”, DOI:10.1016/j.comcom.2014.09, pp.1-55, 2014.

[Fad, 17] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem and Faiz Alotaibi, "Internet of Things Security: A survey", Journal of Network and Computer Applications, Volume 88, pp. 10-28, 2017.

[Fai, 21] Faisal Hussain, Syed Ghazanfar Abbas, Ghalib A. Shah, Ivan Miguel Pires, Ubaid U. Fayyaz, Farrukh Shahzad, Nuno M. Garcia and Eftim Zdravevski, "A Framework for Malicious Traffic Detection in IoT Healthcare Environment", Sensors, Volume 21, Issue 9, pp. 1-19, 2021.

[Fai, 15] Faiza Medjek, Djamel Tandjaoui, Mohammed Riyadh Abdmeziem and Nabil Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility", International Symposium on Programming and Systems (ISPS), pp. 1-9, 2015.

[Fai, 17] Faiza Medjek, Djamel Tandjaoui, Imed Romdhani and Nabil Djedjig "Performance Evaluation of RPL Protocol under Mobile Sybil Attacks", IEEE Trustcom/BigDataSE/ICESS, pp. 1049-1055, 2017.

[Far, 20] Farshad Firouzi, Krishnendu Chakrabarty and Sani Nassif, "Intelligent Internet of Things: From Device to Fog and Cloud", Springer Nature, ISBN 978-3-030-30366-2, 2020.

[Fat, 17] Fatma Gara, Leila Ben Saad and Rahma Ben Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs", 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 276-281, 2017.

[Fir, 16] Firoz Ahmed and Young Bae Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Security and Communication Networks, Volume 9, Issue 18, pp. 5143-5154, 2016.

[Gay, 15] Gayatri Devi, Rajeeb Sankar Bal and Nibedita Sahoo, "Hello Flood Attack Using BAP in Wireless Sensor Network", International Journal of Advanced Engineering Research and Science (IJAERS),Volume 2, Issue 1, pp. 80-86, 2015.

[Geo, 21] George Simoglou, George Violettas, Sophia Petridou and Lefteris Mamatas, "Intrusion Detection Systems for RPL Security: A Comparative Analysis", Volume 104, DOI:10.32604/cmc.2021.015259, pp. 1-56, 2021.

[Ger, 15] Geroge W Kibirige and Camilius Sanga, “A survey on Detection of Sinkhole Attack in Wireless Sensor Network”, International Journal of Computer Science and Information Security, pp. 1-9, 2015.

[Gor, 16] Gordana Gardasevic, Mladen Veletic, Nebojsa Maletic, Dragan Vasiljevic, Igor Radusinovic, Slavica Tomovic and Milutin Radonjic, “The IoT Architectural Framework, Design Issues and Application Domains”, DOI: 10.1007/s11277-016-3842-3, pp. 1-22, 2016.

[Goy, 21] Goyal, Ashok Kumar Sahoo, Tarun Kumar Sharma and Pramod K. Singh, "Internet of Things: Applications, Security and Privacy: A survey", Materials Today: Proceedings, Volume 34, pp. 752-759, 2021.

[Gup, 20] Gupta B.B. and Megha Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols", Concurrency and Computation: Practice and Experience, Volume 32, Issue 21, pp. 1-24, 2020.

[Haf, 16] Hafizur Rahman and Md. Iftekhar Hussain, “Internet of Things: Challenges and Research Opportunities”, DOI 10.1007/s40012-016-0136-6, pp. 1-9, 2016.

[Haf, 21] Hafsa Shahid, Humaira Ashraf, Hafsa Javed, Mamoona Humayun, Nz Jhanjhi and Mohammed A. Aizain, "Energy Optimized Security Against Wormhole Attack in IoT-based Wireless Sensor Networks", CMC-Computers Materials & Continua, Volume 68, Issue 2, pp. 1967-1981, 2021.

[Han, 19] Hanane Lamaazi and Nabil Benamar, "A Comprehensive Survey on Enhancements and Limitations of the RPL Protocol: A Focus on the Objective Function", Ad Hoc Networks, Volume 96, ISSN 1570-8705, pp. 1-53, 2019.

[Him, 19] Himanshu B. Patel and Devesh C. Jinwala, "Blackhole Detection in 6LoWPAN based Internet of Things: An Anomaly based Approach", In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 947-954, 2019.

[Hon, 18] Hongliang Zhu1, Zhihua Zhang, Juan Du1, Shoushan Luo1 and Yang Xin, "Detection of Selective Forwarding Attacks based on Adaptive Learning Automata and Communication Quality in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Volume 14, Issue 11, pp. 1-15, 2018.

[Hos, 19] Hossein Shahinzadeh, Jalal Moradi, Gevork B. Gharehpetian, Hamed Nafisi and Mehrdad Abedi, "IoT Architecture for Smart Grids", IEEE, International Conference on Protection and Automation of Power System (IPAPS), DOI: 10.1109/IPAPS.2019.8641944, pp. 22-30, 2019.

[Iev, 19] Ievgeniia Kuzminykh, Anders Carlsson, Maryna Yevdokymenko and Vladimir Sokolov, "Investigation of the IoT Device Lifetime with Secure Data Transmission", Springer Cham, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, DOI: 10.1007/978-3-030-30859-9_2, pp. 16-27, 2019.

[Jia, 21] Jianxin Wang, Ming K. Lim, Chao Wang and Ming Lang Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years", Computers & Industrial Engineering, Volume 155, pp. 1-17, 2021.

[Jie, 20] Jie Ding, Mahyar Nemati, Chathurika Ranaweera and Jinho Choi, "IoT Connectivity Technologies and Applications: A Survey", arXiv preprint arXiv:2002.12646, pp. 1-26, 2020.

[Jon, 21] Jonathan Tournier, Francois Lesueur, Frederic Le Moue, Laurent Guyon and Hicham Ben Hassine, "A Survey of IoT Protocols and their Security Issues through the Lens of a Generic IoT Stack", Internet of Things, Volume 16, pp. 1-53, 2021.

[Jue, 19] Juenjie Yin, Zheng Yang, Hao Cao, Tongtong Liu and Zimu Zhou, "A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT", ACM Transactions on Sensor Networks (TOSN), Volume 15, Issue 3, pp.1-29, 2019.

[Kai, 18] Kais Mekki, Eddy Bajic, Frederic Chaxel and Fernand Meyer, "Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT", IEEE, International Conference on Pervasive Computing and Communications Workshops (Percom Workshops), pp. 197-202, 2018.

[Kar, 12] Karishma Chugh, Aboubaker Lasebae and Jonathan Loo "Case Study of a Blackhole Attack on LoWPAN-RPL", Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), pp. 157-162, 2012.

[Kev, 09] Kevin Ashton, "That 'Internet of Things' thing", RFID Journal, Volume 22, Issue 7, pp. 97-114, 2009.

[Key, 16] Keyur K Patel and Sunil M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International Journal of Engineering Science and Computing, Volume 6, Issue 5, pp. 6122-6131, 2016.

[Kho, 16] Khosravi H, Azmi R and Sharghi M, "Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks", International Journal of Future Computer and Communication, Volume 5, Issue 2, pp. 99-103, 2016.

[Kua, 14] Kuan Zhang, Xiaohui Liang, Rongxing Lu and Xuemin Shen, "Sybil Attacks and their Defenses in the Internet of Things", IEEE, Internet of Things Journal, Volume 1, Issue 5, pp. 372-383, 2014.

[Kun, 21] Kun Xia, Hongliang Fan, Jianguang Huang, Hanyu Wang, Junxue Ren, Qin Jian and Dafang Wei, "An Intelligent Self-Service Vending System for Smart Retail", Sensors, Volume 21, Issue 10, pp. 1-20, 2021.

[Lin, 13] Linus Wallgren, Shahid Raza and Thiemo Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of Things”, International journal of Distributed Sensor Networks, pp. 1-11, 2013.

[Mah, 17a] Mahmood Alzubaidi, Mohammed Anbar, Samer Al Saleem, Shadi Al Sarawi and Kamal Alieyan, "Review on Mechanisms for Detecting Sinkhole Attacks on RPLs", IEEE, 8th International Conference on Information Technology, pp. 369-374, 2017.

[Mah, 17b] Mahmood Alzubaidi, Mohammed Anbar and Sabri M. Hanshi, "Neighbor-passive Monitoring Technique for Detecting Sinkhole Attacks in RPL networks", International Conference on Computer Science and Artificial Intelligence, pp. 173-182, 2017.

[Mal, 12] Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, and Sanaz Sadeghi "A Novel Algorithm for Detecting Sinkhole Attacks in WSNs", International Journal of Computer Theory and Engineering, Volume 4, Issue 3, pp. 418-422, 2012.

[Mar, 19] Mardiana Binti Mohamad Noor and Wan Haslina Hassan, "Current research on Internet of Things (IoT) Security: A survey", Computer Networks, Volume 148, pp. 283-294, 2019.

[Mar, 21] Marco Lombardi, Francesco Pascale and Domenico Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications", Information, Volume 12, Issue 2, pp. 1-20, 2021.

[Mel, 18] Melancy Mascarenhas and Vineet Jain, "A Survey on Mechanisms for Detecting Sinkhole Attack on 6LoWPAN in IoT", International Journal of Latest Trends in Engineering and Technology, Volume 10, Issue 1, pp.134-137, 2018.

[Mia, 18] Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He and Ren Ping Liu. "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application", Future Generation Computer Systems, Volume 80, pp. 613-626, 2018.

[Mir, 17] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill and Saleem Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", International Journal of Advanced Computer Science and Applications, Volume 8, Issue 6, pp. 383-388, 2017.

[Moh, 18] Mohammad Nikravan, Ali Movaghar and Mehdi Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Volume 99, Issue 2, pp. 1035-1059, 2018.

[Moh, 20] Mohamed Tabaa, Fabrice Monteiro, Hassna Bensag and Abbas Dandache, "Green Industrial Internet of Things from a Smart Industry Perspectives", Energy Reports, Volume 6, Issue 6, pp. 430-446, 2020.

[Mey, 21] Meysam Yadollahzadeh Tabari and Zahra Mataji, "Detecting Sinkhole Attack in RPL-based Internet of Things Routing Protocol", Journal of Artificial Intelligence and Data Mining (JAIDM), Volume 9, Issue 1, pp. 73-85, 2021.

[Muh, 18] Muhammad Burhan, Rana Asif Rehman, Bilal Khan and Byung Seo Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey", Sensors, Volume 18, Issue 9, pp. 1-37, 2018.

[Nan, 20] Nandhini P S, S. Malliga, B. Madhumitha, P. Elango and C. Kayalvizhi, "Thwarting Wormhole Attack in RPL based IoT Networks", International Journal of Advanced Science and Technology, Volume 29, Issue 3, pp. 1031-1038, 2020.

[Nar, 20] Narasimha Swamy and Solomon Raju Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)", IEEE Access, Volume 8, pp. 188082-188134, 2020.

[Nas, 20] Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt and Behnam Zakeri, "Internet of Things (IoT) and the Energy Sector", Energies, Volume 13, Issue 2, pp. 1-27, 2020.

[Neh, 19] Neha Sharma, Madhavi Shamkuwar and Inderjit Singh, "The History, Present and Future with IoT", Internet of Things and Big Data Analytics for Smart Generation, Springer Nature, DOI: 10.1007/978-3-030-04203-5_3, pp. 27-51, 2019.

[Olf, 12] Olf Gaddour and Anis Koubba, “RPL in Nutshell: A Survey”, Computer Networks, Volume 56, Issue 14, pp. 3163-3178, 2012.

[Olu, 21] Oludare Isaac Abiodun, Esther Omolara Abiodun, Moatsum Alawida, Rami S Alkhawaldeh and Humaira Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions", Wireless Personal Communications, Volume 119, Issue 3, pp. 2603-2637, 2021.

[Pao, 21] Paolo Mezzanotte, Valentina Palazzi, Federico Alimenti and Luca Roselli, "Innovative RFID Sensors for Internet of Things Applications", IEEE, Journal of Microwaves, Volume 1, Issue 1, pp. 55-65, 2021.

[Goy, 21] Goyal, Ashok Kumar Sahoo, Tarun Kumar Sharma and Pramod K. Singh, "Internet of Things: Applications, Security and Privacy: A survey", Materials Today: Proceedings, Volume 34, pp. 752-759, 2021.

[Par, 21] Parvathy K, "Wormhole Attacks in Wireless Sensor Networks (WSN) & Internet of Things (IoT): A Review", International Journal of Recent Technology and Engineering (IJRTE), Volume 10, Issue 1, 2021.

[Pan, 15] Pavan Pongle and Gurunath Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things", International Journal of Computer Applications, Volume 121, Issue 9, pp. 1-9, 2015.

[Qih, 19] Qihao Zhou, Kan Zheng, Lu Hou, Jinyu Xing and Rongtao Xu, "Design and Implementation of Open LoRa for IoT", IEEE Access, Volume 7, pp. 100649-100657, 2019.

[Rah, 20] Rahul Reddy Nadikattu, "Data Safety and Integrity Issue in IoT", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 8, Issue 6, pp. 1268-1276, 2020.

[Ras, 18] Rashmi Sahay, G. Geethakumari, Barsha Mitra and V. Thejas, "Exponential Smoothing based Approach for Detection of Blackhole Attacks in IoT", IEEE, International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2018.

[Sab, 18] Sabah Suhail, Shashi Raj Pandey and Choong Seon Hong, "Detection of Selective Forwarding Attack in RPL-Based Internet of Things through Provenance", pp. 965-967, 2018.

[Sab, 19] Sabeen Tahir, Sheikh Tahir Bakhsh and Rayan A Alsemmeari "An intrusion Detection System for the Prevention of an Active Sinkhole Routing Attack in Internet of Things", International Journal of Distributed Sensor Networks, Volume 15, Issue 11, pp. 1-10, 2019.

[Sal, 15] Salavat Marian and Popa Mircea, "Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator Detection Scheme", IEEE, 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, pp. 121-124, 2015.

[San, 21] Sana Abdelaziz Bkheet and Ohnson I. Agbinya, "A Review of Identity Methods of Internet of Things (IOT)", Advances in Internet of Things, Volume 11, Issue 4, pp. 153-174, 2021.

[Sau, 21] Saurabh Sharma and Vinod Kumar Verma, "Security explorations for Routing Attacks in Low Power Networks on Internet of Things", The Journal of Supercomputing, Volume 77, Issue 5, pp. 4778-4812, 2021.

[Sey, 17] Seyyit Alper Sert, Carol Fung, Roy George and Adnan Yazici, "An efficient fuzzy Path Selection Approach to Mitigate Selective Forwarding Attacks in Wireless Sensor Networks", IEEE, International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6, 2017.

[Sha, 21] Shakawat Hossain, Nur Mohammad Ali Chisty, Donyea Lamont Hargrove and Ruhul Amin, "Role of Internet of Things (IoT) in Retail Business and Enabling Smart Retailing Experiences", Asian Business Review, Volume 11, Issue 2, pp. 75-80, 2021.

[Sha, 17] Shapla Khanam, Ismail Ahmedy and Mohd Yamani Idna Idris, "An Efficient Detection of Selective Forwarding Attacks in Heterogeneous IoT Networks", pp. 1-8, 2017.

[Sho, 18] Shoukat Ali, Muazzam A Khan, Jawad Ahmad, Asad W. Malik and Anis Ur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN", Third International Conference on Fog and Mobile Edge Computing (FMEC), pp. 217-226, 2018.

[Sil, 20] Silvia Liberata Ullo and G. R. Sinha, "Advances in Smart Environment Monitoring Systems Using IoT and Sensors", Sensors, Volume 20, Issue 11, pp. 1-18, 2020.

[Sob, 20] Sobin C.C, "A Survey on Architecture, Protocols and Challenges in IoT", Wireless Personal Communications, Volume 112, Issue 3, pp. 1383-1429, 2020.

[Soh, 19] Sohail Abbas, "An Efficient Sybil Attack Detection for Internet of Things", In World Conference on Information Systems and Technologies, pp. 339-349, 2019.

[Som, 21] Somnath Karmakar, Jayasree Sengupta and Sipra Das Bit, "LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT", IEEE, International Conference on Communication Systems & Networks, DOI: 10.1109/COMSNETS51098.2021.9352937, pp. 429-437, 2021.

[Son, 21] Sonia Kolhe and Heena Sheikh, "Internet of Things (IoT) Applications in Power System", Journal of Emerging Technologies and Innovative Research, Volume 8, Issue 3, pp. 39-42, 2021.

[Ste, 16] Stephen R, A. Dalvin Vinoth Kumar and L. Arockiam, "Deist: dynamic detection of Sinkhole attack for Internet of Things", International Journal of Engineering and Computer Science, Volume 5, Issue 12, pp. 19358-19362, 2016.

[Ste, 17] Stephen R and L. Arockiam, "Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things", International Journal of Electrical Electronics and Computer Science, Volume 4, Issue 4, pp. 16-20, 2017.

[Ste, 18a] Stephen R and L. Arockiam, "RDAID: Rank Decreased Attack IDentification Algorithm for Internet of Things", International Journal of Scientific Research in Computer Science Applications and Management Studies, Volume 7, Issue 3, pp. 1-5, 2018.

[Ste, 18b] Stephen R and L. Arockiam, "RIAIDRPL: Rank Increased Attack IDentification Algorithm for Avoiding Loop in the RPL DODAG", International Journal of Pure and Applied Mathematics, Volume 119, Issue 16, pp. 1-8, 2018.

[Ste, 18c] Stephen R and L. Arockiam, "E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things", Journal of Physics, DOI:10.1088/1742-6596/1142/1/012009, pp. 1-13, 2018.

[Sum, 20] Sumit Pundir, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, Joel J. P. C. Rodrigues and Youngho Park, "Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment", Sensors, Volume 20, Issue 5, pp. 1-27, 2020.

[Sur, 19] Surinder Singh and Hardeep Singh Saini, "Detection Techniques for Selective Forwarding Attack in Wireless Sensor Networks", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 6, pp. 380-383, 2019.

[Sus, 19] Susan G. Varghese, Ciji Pearl Kurian, V.I. George, Anupriya John, Varsha Nayak and Anil Upadhyay, "Comparative study of zigBee topologies for IoT-based lighting automation", IET Wireless Sensor Systems, Volume 9, Issue 4, pp. 201-207, 2019.

[Swa, 20] Swathi B and Yerrolla Chanti, "Review on Simplifying IoT: The Usage of Near Field Communication (NFC) in Digital Gadget", Journal of Mechanics of Continua and Mathematical Sciences, Volume 15, Issue 8, pp. 464-472, 2020.

[Tar, 17] Tara Salman and Raj Jain, "A Survey of Protocols and Standards for Internet of Things", Advanced Computing and Communications, Volume 1, Issue 1, pp. 1-20, 2017.

[Tin, 20] Tina Samizadeh Nikoui, Amir Masoud Rahmani, Ali Balador and Hamid Haj Seyyed Javadi, "Internet of Things architecture challenges: A systematic review", International Journal of Communication Systems, Volume 34, Issue 4, pp. 1-42, 2020

[Tra, 21] Trayush, Ruchika Bathla, Sonia Saini and Vinod Kumar Shukla, "IoT in Healthcare: Challenges, Benefits, Applications and Opportunities", IEEE, International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), DOI: 10.1109/ICACITE51222. 2021.9404583, pp. 107-111, 2021.

[Usm, 18] Usman Shafique, Abid Khan, Abdur Rehman, Faisal Bashir and Masoom Alam, "Detection of Rank Attack in Routing Protocol for Low Power and Lossy Networks", Annals of Telecommunications, Volume 73, Issue 7, pp. 429-438, 2018.

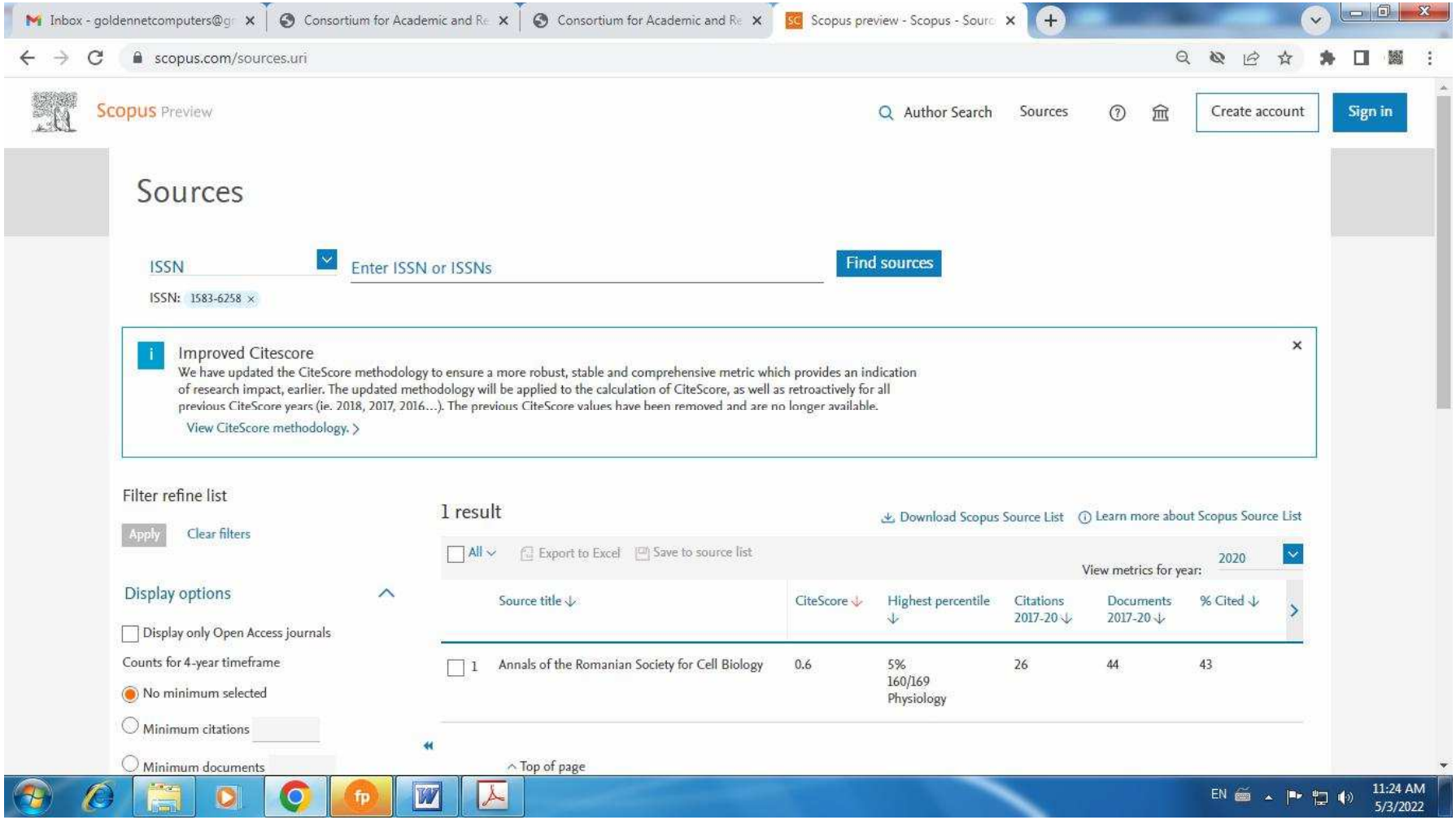
[Vip, 17] Vipindev Adat and B. B. Gupta, "Security in Internet of Things: Issues, Challenges, Taxonomy, and Architecture", DOI: 10.1007/s11235-017-0345-9, pp. 1-99, 2017.

[Yus, 19] Yusuf Perwej, Kashiful Haq, Firoj Parwej and Mumdouh M. Mohamed Hassan, "The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications, Volume 182, Issue 49, pp. 36-49, 2019.

[Zah, 20a] Zahrah A. Almusaylim, Abdulaziz Alhumam and N.Z. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review", Ad Hoc Networks, Volume 101, pp 1-29, 2020.

[Zah, 20b] Zahrah A. Almusaylim, NZ Jhanjhi and Abdulaziz Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP", Volume 20, Issue 21, pp. 1-25, 2020.

Appendices


Inbox - goldennetcomputers@g
Consortium for Academic and Re
Consortium for Academic and Re
Scopus preview - Scopus - Sourc
scopus.com/sources.uri
Scopus Preview
Author Search
Sources
Create account
Sign in
Sources
ISSN
Enter ISSN or ISSNs
Find sources
ISSN: 1583-6258
Improved Citescore
We have updated the CiteScore methodology to ensure a more robust, stable and comprehensive metric which provides an indication of research impact, earlier. The updated methodology will be applied to the calculation of CiteScore, as well as retroactively for all previous CiteScore years (ie. 2018, 2017, 2016...). The previous CiteScore values have been removed and are no longer available.
View CiteScore methodology. >
Filter refine list
Apply
Clear filters
Display options
Display only Open Access journals
Counts for 4-year timeframe
No minimum selected
Minimum citations
Minimum documents
1 result
Download Scopus Source List
Learn more about Scopus Source List
All
Export to Excel
Save to source list
View metrics for year:
2020
Source title
CiteScore
Highest percentile
Citations 2017-20
Documents 2017-20
% Cited
1
Annals of the Romanian Society for Cell Biology
0.6
5%
160/169
Physiology
26
44
43
Top of page
EN
11:24 AM
5/3/2022

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

Attacks against RPL in IoT: A Survey

A.Stephen[1], Dr. L. Arockiam[2]
Research Scholar[1], Associate Professor[2]
Department of Computer Science,
St. Joseph‟s College (Autonomous),
(*Affiliated to Bharathidasan University*),
Tiruchirappalli – 620002, India.

Abstract

Internet of Things is one of the trending technologies in the cotemporary world which allows all the technologies to work together as a single system. The "things" connected in the IoT environment could be anything such as objects, physical/virtual things and human beings. The communication between these connected things should be secured. Otherwise, intruders can misuse the data collected from the IoT environment. So, there is a necessity of providing better routing mechanism for IoT to provide secure communication against various attacks in IoT. Several protocols are used for routing in IoT. IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is one of the protocols in IoT based system. In this paper, various attacks against RPL protocol are listed out, analyzed and distinguished from each other.

Keywords: IoT, Attacks, Security, RPL

1. Introduction

1.1 Internet of Things

Internet of Things is a technology where the physical things are interconnected through the internet which have unique identities and their own functionalities. The functionalities can be sensing, actuation, sharing information, analyzing and processing the sensed data. Since sensitive data are collected using IoT technology, the communication path should be secured. The attackers can misuse the data in the communication process.

1.2 IoT Architecture

Different types of layered architectures are used by many researchers. There is no standard architecture for IoT. But three layered architecture is most frequently used which was proposed by IETF. The fig 1.1 presents three layered architecture.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

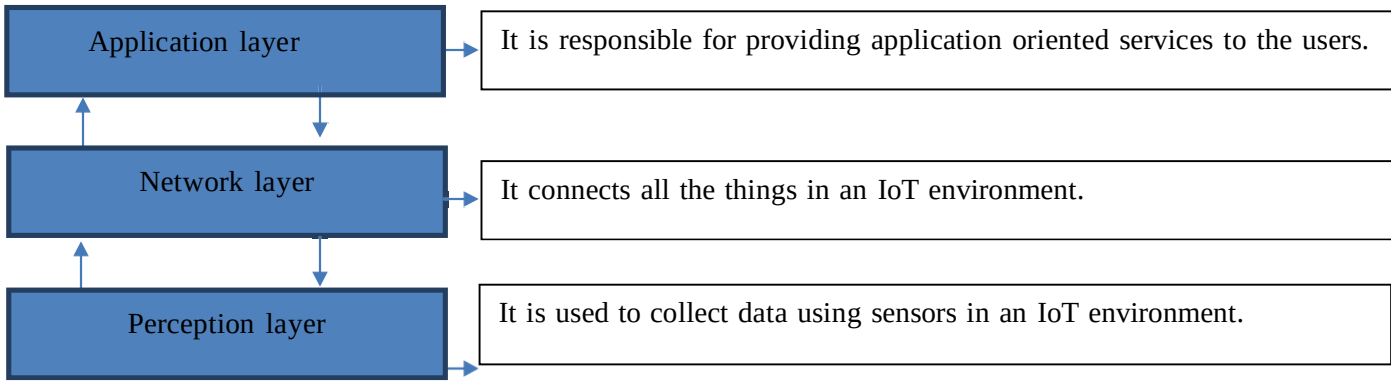


Fig 1.1 Three layered architecture

There are lots of issues in these three layers. This paper focuses various attacks against the routing protocol RPL.

1.3 Routing in IoT

Routing protocol is used in the communication process among the nodes in the network. Routing in Internet of Things is classified into two types such as proactive (dynamic path selection process) and reactive (senders nodes trigger the route discovery).

1.4 RPL

Routing Protocol for low power and Lossy networks (RPL) is an IPv6 routing protocol used in IoT environment. RPL falls in proactive category which dynamically seeks for the routing path.

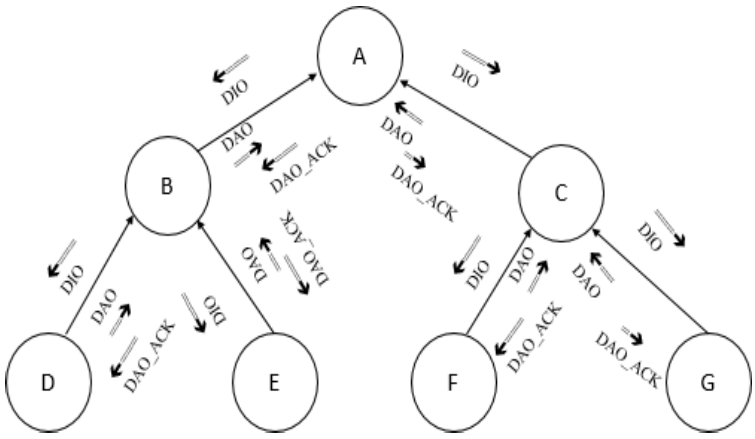


Fig 1.2 DODAG construction process

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

The attacks during the communication process can be mitigated by using proactive techniques. It uses Destination Oriented Directed Acyclic Graph (DODAG) for routing. It uses control messages to form DODAG. Fig 1.2 shows the DODAG construction process. A parent node broadcasts DODAG Information Object (DIO) message to neighboring nodes. The neighboring nodes which receive the DIO message will send DODAG Advertisement Object (DAO) to the parent node. After accepting the DAO messages from the neighboring node, the parent node will send the DAO_Acklogement (DAO_ACK) message to its children to join in the network. If a new node comes, it has to broadcast DODAG Information Solicitation (DIS) message to join the network which has the configuration. Table 1.1 describes the RPL control messages.

Table 1.1 RPL control messages

RPL Control Message	Description
DODAG Information Object (DIO)	It contains information about a parent node
DODAG Advertisement Object (DAO)	It advertises that a node is within the range with same configuration that wants to join in the concern network
DAO_Acklogement (DAO_ACK)	It acknowledges its children to join in the network
DODAG Information Solicitation (DIS)	It is used to request for DIO message to join in the existing network.

This paper is organized into different sections. Section 2 lists out the various attacks against RPL protocol; Section 3 distinguishes the various attacks; Section 4 gives Literature review; Section 5 gives the results and discussions and Section 6 concludes the paper.

1.5 Attacks against RPL

Various attacks such as sinkhole attack, Sybil attack, selective forwarding attack, black hole attack, hello flood attack, wormhole attack, rank attack and version number attack were occurred while using RPL routing protocol in IoT.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

Sinkhole attack

Sinkhole attack is an attack where compromised node tries to entice network traffic by masquerading as legitimate node in routing process. The sinkhole attack blocks the base station from obtaining legitimate information; it causes threat and makes the way for occurrences of other attacks too.

Sybil attack

Sybil is an attack where a malicious node creates multiple fake identities at the same time in the network. It does not allow the packets of a node to be sent to the destination.

Selective forwarding attack

Selective forwarding is an attack where the malicious nodes neglect to forward the messages to precise destination nodes or simply drop the messages not to propagate anymore.

Blackhole attack

A black hole is an attack where the attacker node claims as it has shortest path to the destination. It drops the routing packets and does not propagate the packets to the precise destination.

Hello flood attack

Hello flood attack is an attack where an adversary node sends the hello messages to the neighbor nodes to disturb the network.

Wormhole attack

Wormhole attack is an attack where two or more adversary nodes are connected with the link called wormhole link and the nodes form the tunnels to broadcast the data packets into the network. It makes the network to be confused and disrupt the communication process over the network.

Rank attack

In RPL protocol, the rank value determines the position of each node in the network. The rank value of a node is used to select the parents and routes. The rank of a node increases in a

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

downward direction and decreases in an upward direction. A malicious node is changing the legitimate rank value into falls rank value is called rank attack.

2. Literature Review

2.1 Internet of Things overview and security issues & challenges based on RPL

Eleonora Borgia et al.[9] described the key features, driving technologies and issues and challenges in Internet of Things. The different phases involved in IoT environment were clearly explained. The IoT applications were listed out with brief descriptions.

MdIftekhar Hussain et al.[26] explained the various components used in Internet of Things. The research opportunities in IoT were explained and also the challenges concerned with security and privacy issues in IoT were listed out. The requirements to provide the better quality of service in IoT were explained.

Gordana et al.[16] described the various standard organizations which had given architectural framework for the Internet of Things. The design issues of hardware and software were explained with precise examples. The contribution of Nano technology in IoT was articulated.

VipindevAdat et al.[46] had given the overview with the design of architecture in IoT. The authors analyzed various attacks in the IoT routing protocols such as 6LoWPAN and RPL. The challenges and the security issues were explained.

Anthea et al.[3] articulated a taxonomy of attacks in RPL based Internet of Things. The taxonomy consisted of three main categories such as attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic. These categories of attacks were distinguished from each other. The risk management concern with the attacks was clearly discussed.

Linus wallgren et al.[22] presented an overview of IoT technologies and routing attacks. The network protocols such as 6LoWPAN, CoPA/COAPS and RPL were clearly discussed. The concept behind IDS in IoT was explained. The attacks against RPL namely selective forwarding attack, sink hole attack, hello flood attack, wormhole attack, clone ID and Sybil attack were described, checked and implemented using Contiki and Cooja simulator.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2.2 Sinkhole attack

In [44], intrusion detection system was designed to detect sinkhole attack at edge level internet of thing environment. The proposed intrusion detection system was efficient to detect all possible types of sinkhole attack in edge based Internet of Things. The proposed IDS named as SAD-EIOT. NS2 simulator was used to simulate the SAD-IOT system. The SAD-IOT was suitable for surveillance security and monitoring system. A detection accuracy of 95.83% was achieved with the false positive rate of 1.93%. Throughput, packet delivery ratio, packet lose rate and end to end delay were distinguished in the form of normal flow, under attack and proposed schema.

In [24], the authors proposed an algorithm to detect sinkhole attack based on energy consumption. In the algorithm, a node will send the control message to the main base station before sending its data to its base station. The control message is compared with its corresponding data hop by hop. The malicious node was detected based on the variation in the control messages. The proposed sinkhole attack detection algorithm was compared with Ngai's algorithm. The algorithm worked better than the Ngai's algorithm. It was also used for detecting wormhole attack.

Geroge et al.[14] analyzed the existing techniques to detect sinkhole attack in wireless sensor network such as rule based, anomaly based detection, statistical method, hybrid based intrusion detection and key management. The sinkhole attack was defined and explained with graphical representation. The challenges in detection of sinkhole attack like communication pattern in wireless sensor networks, unpredictable sinkhole attack, insider attack and resource constraints and physical attack were discussed.

In [7], an intrusion detection system (IDS) was proposed to detect sinkhole attack. The proposed IDS detected the sinkhole attack and mitigated the destructive effects which were identified in the networks. They combined watchdog, reputation and trust strategies to detect attacker based on the behavior of the devices. The proposed technique was divided into four modules namely cluster configuration routing monitoring, attack detection and attack isolation. The system was implemented in the Cooja simulator. The UDS was compared with SVELTE in terms of detection accuracy in fixed scenario and mobile scenario and false positive rate. The detection accuracy for SVELTE in fixed scenario was 90%, the detection accuracy for INTI in fixed scenario was 92%. The detection accuracy for SVELTE in mobile scenario was 24%, the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

detection accuracy for INTI in fixed scenario was 70%. The false positive rate for SVELTE was 38%, the false positive rate for INTI was 28%.

In [25], the mechanisms to detect sinkhole attack on ipv6 over low power wireless personal area network were surveyed. The paper analyzed the mechanisms called VERA, TRAIL, Secure Parent, and SVLTE. INTI and Specification based mechanisms were distinguished with each other.

In [32], the intrusion detection system to prevent an active sinkhole attack in Internet of things was presented. In this proposed system, the whole network was divided into clusters of Internet of Things. All the devices were connected with their concerned gateways. The intrusion system was deployed into the gateways. The gateways analyzed the communication over the devices and detected the anomalies using the proposed IDS. The base station had all the records and all the activities over the IOT environment. At the situation of sinkhole attack in the connected network, the base station sent the alert to all the connected devices in the network. The proposed IDS model outperformed in terms of packet delivery ratio (PDR) and energy consumption.

Stephen et al.[42] proposed an active detection technique to detect sinkhole attack. The technique comprised of three phases. The first phase was construction of DODAG, the second phase was detection of sinkhole attack, and the third was sinkhole attack treatment. The technique was simulated using Cooja simulator.

In [23], the light weight technique called Neighbor Passive Monitoring Technique for detecting sinkhole attacks in RPL networks (NPMT) was proposed. The proposed technique comprised of two phases. The first phase was used to identify the suspicious nodes in the network based on inconsistent changes in the nodes rank. The second phase was used to detect the sinkhole attack from the suspicious nodes. The proposed technique was compared with the existing technique SVELTE. The proposed technique NPMT performed better than SVELTE. The technique was implemented using Cooja simulator.

Geroge et al.[13] described the existing techniques to identify sinkhole attack in wireless sensor networks(WSNs). The challenges in WSNs were elucidated in detail. The different approaches used for mitigating sinkhole attacks were explained.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

Leovigible et al.[21] proposed a new methodology for detecting sinkhole attacks in MANETs. The proposal leverages on the existence of "contamination border" formed by the legitimate nodes under the influence of the sinkhole attack. The proposed methodology was implemented using network simulator OMNCT++ (Varga)

Stephen et al.[43] proposed intrusion detection system to detect sinkhole attack on RPL protocol. The IDS used number of packets transmitted and received to detect sinkhole attack based on the intrusion ratio. The alert message was sent to leaf nodes after identifying the intruder node in the network.

2.3 Sybil attack

In [20], the authors took the survey on Sybil attacks and their defense scheme in internet of things. The authors classified the Sybil attack into three types such as SA-1, SA-2and SA-3, based on the capabilities of the Sybil attack. The comparisons of three types of attack were given in a table. The Sybil attack defense scheme like social graph based Sybil detection (SGSD),behavior classification based Sybil detection (BCSD), and mobile sybil detection were explained in detail. The research issues based on sybil attack were discussed.

In [33], the mechanism to solve sinkhole attack was introduced. The mechanism was robust and lightweight. The sinkhole attack was identified based on received signal strength indicator (RSSI). The proposed mechanism was stable enough in the static environment.

In [38], the system for detecting both direct and indirect Sybil attack in Internet of Things was recommended. The system utilized localization information dissemination such as received signal strength indicator and the ratio of RSSI for each neighbor nodes. The proposed detection system produced low overhead in network.

In [27], authors proposed two different techniques to detect sybil attack for a forest wild fire monitoring application. The first technique was a two tire method which used the high energy nodes operating at lower level. The second technique was residual energy based detection. After detecting the sybil attack, the cluster head was elected by the nominee packets. The legitimate packets were identified by looking at the cluster head in the packet. The proposed technique resulted high detection accuracy and low false-negative rate.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

In [10], various attacks were analyzed against RPL. Sybil attack was analyzed in detail. The RPL protocol was affected more by the sybil attack in mobile environment compared with static environment. It was found that the sybil attack decreased the packet delivery ratio and increased the control messages overhead in RPL protocol.

In [8], the study was done on techniques to detect sybil attack based on network features, cryptography and relationship between neighbors nodes in IoT. After analyzing the several techniques, the authors concluded that there is a need to develop an efficient technique for detecting and mitigating sybil attack in IoT.

In [1], authors presented a comprehensive analytical survey on sybil attack in IoT. The authors classified the sybil attack into three phases namely compromise phase, deployment phase and launching phase. The algorithm using K-means clustering was proposed to visualize the deployment selection procedure of the attacker. The algorithm achieved 48.7% in clustering affected nodes and the legitimate nodes in the IoT.

In [28], a technique to detect sybil attack based on RSSI value in wireless sensor networks (WSN) was introduced. The technique was tested by multiple receivers using their RSSI ratio. The proposed technique achieved 100% to detect sybil attack and produced less false positive.

2.4 Selective forward attack

In [36], authors focused selective forwarding attack in IoT network. A non-cooperative zero-sum gave theoretic model for detecting intruders in the network. The malicious nodes were detected based on hop by hop inspection using packet loss rate threshold value. The proposed model was simulated using Cooja simulator. The model efficiently worked in the heterogeneous environment.

In [18], a method to detect and eliminate selective forwarding attack using adaptive learning automata and communication quality was proposed. This method was used for ordinary selective forwarding attack and special case of selective forwarding attack. Packet loss was considered as metric to detect selective forwarding attack. The proposed method was simulated using OMNeT++. The method was compared with the existing method CLAIDS which was proposed by Fathinavid and Ansari.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

In [45], authors discussed four selective forwarding detection techniques such as Public Key Encryption (PKE), Rivest Shamir Adelemen (RSA), ELGMAL and Chinese Remainder Theorem (CRT). These four techniques were evaluated based on storage space required, energy consumption and time consumption for key management. The authors concluded that minimum storage was required for public key encryption and minimum energy consumption were required for CRT based RSA techniques.

In [11], an Intrusion Detection System (IDS) to prevent nodes from selective forwarding attack based on mobile wireless sensor networks was proposed. The proposed IDS was novel with the combination of sequential probability ratio test with an adaptive threshold of acceptable probability of dropped packets. The IDS used four steps namely data gathering, data analysis, detection, elimination and compromised node setup. It was evaluated using Cooja simulator and performed 100% of detection probability.

In [31], provenance based method to detect selective forwarding attack in RPL based internet of Things was introduced. Each data in the network was consisted of unique sequence number, payload and packet delivery ratio. Packet delivery ratio was used to identify the malicious nodes in the IoT network. The proposed method was simulated using Cooja simulator. Provenance generation time and provenance size were taken as performance metrics.

In [5], authors discussed on trust management scheme to defend against selective forwarding attack in internet of Things. The trust value of each node was stored in a table. It was found that, if the trust value was decreased then there was the possibility of selective forwarding attack in the network. Various existing distributed trust management scheme were tested using Cooja simulator with Tmote Sky environment.

In [35], an algorithm to detect and mitigate selective forwarding attack using efficient fuzzy path selection approach in wireless sensor networks was proposed. The proposed algorithm was comprised of two phases. The first phase was detecting compromised nodes in the network. The second phase was to mitigate selective forwarding attack by generating new disjoint path using average link residual energy and relative hop count. The proposed algorithm was evaluated in the real environment by deploying various sensors in a rectangular area.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2.5 Blockhole Attack

In [4], authors proposed a trust based mechanism to tackle blackhole attack in RPL protocol. Packet delivery ratio of the node was taken as the trust value. The proposed mechanism was used in two levels namely inter-DODAG level and intra-DODAG level. It was implemented using Cooja simulator.

Himanshu et al.[17] proposed an intrusion detection system to detect and mitigate blackhole attack in internet of things. The proposed IDS was divided into two modules namely local module and global module. The local module was used in the node level. The global module was used in border routed level. The suspicious nodes list was created based on the behavior of the nodes. The suspected nodes were only observed in the network. Malicious event was created when there was change in the observed nodes. The malicious nodes were eliminated when the nodes crossed the malicious event threshold value. The IDS was simulated using Cooja simulator. It was proved that the proposed IDS worked better than the watchdog approach.

In [38], blackhole attack in Internet of Thigs (IoT) and Wireless Sensor Networks (WSN) were discussed. Authors gave comparative analysis of various existing techniques of blackhole attack. The analysis was done based on energy consumption, network traffic, packet delivery ratio, throughput and end to end delay. The simulation tools used for detecting and mitigating blackhole attack were discussed.

In [30], statistical technique called exponential smoothing approach to detect blackhole attack was explained. This approach was based on time serious analysis of data. The data collection process was done in sink level in the proposed technique. It was used in the dynamic environment. The proposed technique was tested using Cooja simulator.

Firoz et al.[12] proposed an algorithm to mitigate blackhole attack in routing protocol for low power and lossy networks. The proposed technique consisted of local decision and global verification process. Each node in the network monitored the communication behavior of its neighboring nodes by overhearing packets transmitted by neighboring nodes. The second process was to identify the suspicious nodes. The suspicious nodes were verified by changes in their

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

behavior. The confirmed malicious nodes‟ IDs were broadcasted to the other nodes by the alternative path in the network. The technique was simulated by Cooja simulator.

In [19], case study was done on blockhole attack in 6LoWPAN-RPL. Blackhole attack was tested using Cooja simulator. It was found that blackhole attack increased end to end delay and packet delivery ratio of the nodes in the network. It was also found that the malicious nodes rapidly affected the legitimate nodes.

2.6 Rank Attack

Anhtuan et al.[2] explained types of internal threats and their impact on WSN. RPL protocol was clearly explained with its operation in the WSN. RPL attacks were described in detail. The parameters of DODAG and the control messages of DODAG were clearly explained. Contiki OS and Cooja simulator were used for the simulation process.

Stephen et al.[38] proposed the technique called energy based validation and verification (E2V) for detecting and mitigating rank attack (RA) over RPL. The proposed technique used three phases namely rank calculation, substation and malicious node elimination. The technique was used to solve the rank inconsistency attack.

Ghada et al.[15] proposed a secure routing technique based on RPL for Internet of things. The proposed method was used to prevent nodes from the malicious nodes in the network. The author had taken the rank property to provide secure routing. Rank threshold and hash chain authentication were used to deal with the attackers nodes. The proposed method was implemented using Contiki OS and Cooja simulator. It outperformed the existing techniques

Stephen et al.[39] proposed a technique named “Rank Decreased attack IDentification (RDAID)” for identifying the malicious nodes and mitigating the malicious node. Packet delivery ratio (PDR) was used for securing the routing process.

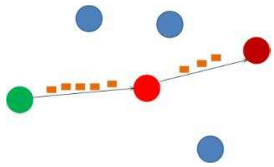
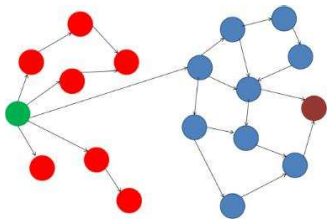
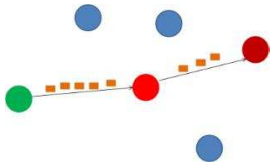
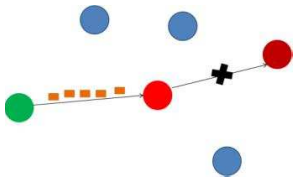
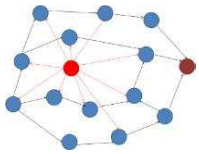
Stephen et al.[40] proposed Rank Increased Attack (RIA) identification algorithm to avoid loop in the RPL DODAG. The proposed technique detects the nodes which were affected by the rank increased attack. It gave the better result than the existing techniques.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

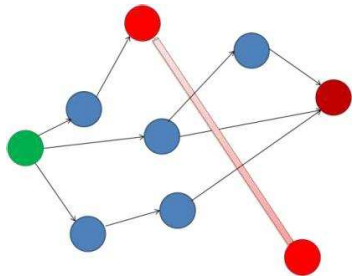
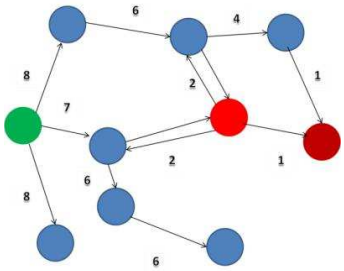
3. Different attack scenario in RPL

Section three explains various attack scenario with concerned diagram. Green color node indicates source node. Red colour node indicates malicious node. Brown colour indicates destination node. Blue colour nodes indicate neighbor nodes

Table 3.1 RPL attacks scenario

S. No	Name of the attack	Description	Diagram
1	Sinkhole Attack	Compromised node tries to drop the packets	
2	Sybil Attack	Malicious node creates multiple fake identities	
3	Selective Forwarding Attack	The malicious nodes selectively drops or forward the packets	
4	Black Hole Attack	The attacker node claims as it has shortest path and drops all the packets.	
5	Hello Flood Attack	Adversary node sends the hello messages to the neighbors‟ node to disturb the network.	

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

6	Wormhole Attack	Two or more adversary nodes are connected with the link called wormhole link and the nodes form the „tunnel“ to broadcast the data packets into the network.	
7	Rank Attack	The rank value determines that the position of each node in the network. The rank value of a node is used to select the parents and routes	

4. Detection and Mitigation Mechanism of RPL based Attacks.

The different types of mechanisms which are used for detecting and mitigating RPL attacks are listed out in the table 4.1 based on the attack type.

Table 4.1 List of RPL attack detection and mitigation mechanisms

S.No	Attack type	Mechanism
1	Sinkhole attack	Energy based detection [24],[27], K-means clustering [1], Watchdog Mechanism[7], Cluster based Detection[32], Neighbor Passive Monitoring Technique[23].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2	Sybil attack	Social graph based Sybil detection [20], Technique based on received signal strength indicator (RSSI) [33], [38], [28].
3	Selective forwarding attack	Hop by Hop in section [36], Adaptive learning mechanism [18], Public key encryption technique[45], Provenance based method[31], Trust management scheme[5] and fuzzy path selection approach [35].
4	Blockhole attack	Trust based mechanism [4], Strained based intrusion detection system [17], Exponential smoothing approach [30], Nodes' behaviour approach[12].
5	Rank attack	Energy based technique [38], PDR based approach[39], Nodes' behaviour approach[15].

5. Conclusion

IoT is the current trending technology. It requires global connectivity and accessibility so that anyone can access IoT devices anywhere at any time. So security plays a vital role in the IoT technology to provide the access control and the secure communication. In this paper, IoT security issues and attacks related to RPL are clearly explained. Based on the survey on RPL attacks, it is a necessary to provide a novel technique to mitigate these attacks.

REFERENCES

[1] Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal, and Laurence T. Yang, "Analytical model for sybil attack phases in internet of things", IEEE Internet of Things Journal, Vol. 6, Issue 1, pp. 379-387, 2018.

[2] Anhtuan Le, Jonathan Loo, AboubakerLasebae, Alexey Vinel, Yue Chen and Michael Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sensors Journal, Vol. 13, Issue 10, pp.3685-3692, 2013.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[3] AntheaMayzaud, Remi Badonnel and Isabella Christment, “A Taxonomy of Attacks in RPL-based Internet of Things”, International Journal of Network Security, Volume 18, Issue 3, pp. 459-473, 2016.

[4] Bhalaji, N., K. S. Hariharasudan, and K. Aashika, "A trust based mechanism to combat blackhole attack in RPL protocol", In International Conference on Intelligent Computing and Communication Technologies, pp. 457-464, 2019.

[5] Carolina V. L. Mendoza and Joao H. Kleinschmidt, "Defense for selective attacks in the IoT with a distributed trust management scheme", In 2016 IEEE International Symposium on Consumer Electronics (ISCE), pp. 53-54. IEEE, 2016.

[6] Cervantes, Christian, Diego Poplade, Michele Nogueira, and Aldri Santos. "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606-611. 2015.

[7] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606-611, 2015.

[8] Danilo Evangelista, Farouk Mezghani, Michele Nogueira, Aldri Santos ,"Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination", In 2016 Wireless Days (WD), pp. 1-6, 2016.

[9] Eleonora Borgia, “The Internet of Things vision: Key Features, Applications and Open Issues”,DOI : http://dx.doi.org/10.1016/j.comcom.2014.09, pp.1-55, 2014.

[10] FaizaMedjek, DjamelTandjaoui, Mohammed Riyadh Abdmeziem, Nabil Djedjig "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility", In 2015 12th International Symposium on Programming and Systems (ISPS), pp. 1- 9, 2015.

[11] FatmaGara, Leila Ben Saad and Rahma Ben Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs",In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 276-281, 2017.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[12] Firoz Ahmed and Young-Bae Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Security and Communication Networks, Vol. 9, Issue 18, pp 5143-5154, 2016.

[13] George W. Kibirige and Camilius Sanga, "A survey on detection of sinkhole attack in wireless sensor network", arXiv preprint arXiv:1505.01941, 2015.

[14] Geroge W Kibirige and Camilius Sanga, "A survey on Detection of Sinkhole Attack in Wireless Sensor Network", International Journal of Computer Science and Information Security, pp. 1-9, 2015.

[15] GhadaGlissa, AbderrezakRachedi and ArefMeddeb, "A secure routing protocol based on RPL for Internet of Things", In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-7, 2016.

[16] GordanaGardasevic, MladenVeletic, NebojsaMaletic, DraganVasiljevic, Igor Radusinovic, SlavicaTomovic and MilutinRadonjic, "The IoT Architectural Framework, Design Issues and Application Domains", DOI 10.1007/s11277-016-3842-3, pp. 1-22, 2016.

[17] Himanshu B. Patel and Devesh C. Jinwala, "Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach",In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 947-954, 2019.

[18] Hongliang Zhu1, Zhihua Zhang , Juan Du1, Shoushan Luo1 and Yang Xin, "Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks", International Journal of Distributed Sensor Networks, Vol. 14, Issue 11, pp. 1-15, 2018.

[19] KarishmaChugh, AboubakerLasebae and Jonathan Loo, "Case study of a black hole attack on LoWPAN-RPL", In Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012), pp. 157-162, 2012.

[20] Kuan Zhang, Xiaohui Liang, Rongxing Lu and Xuemin Shen, "Sybil attacks and their defenses in the internet of things", IEEE Internet of Things Journal, Vol.1, Issue 5, pp. 372-383, 2014.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[21] Leovigildo Sanchez-Casado, Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, and Nils Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs", Journal of Network and Computer Applications, pp. 62-77, 2015.

[22] Linus Wallgren, Shahid Raza and Thiemo Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of things”, International journal of Distributed Sensor Networks, pp. 1-11, 2013.

[23] Mahmood Alzubaidi, Mohammed Anbar and Sabri M. Hanshi, "Neighbor-passive monitoring technique for detecting sinkhole attacks in RPL networks", In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, pp. 173-182, 2017.

[24] MalihehBahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat HeydariYazdi, and SanazSadeghi, "A novel algorithm for detecting sinkhole attacks in WSNs", International Journal of Computer Theory and Engineering Vol. 4, Issue 3, pp. 418 -422, 2012.

[25] MelancyMascarenhas and Vineet Jain, "A survey on mechanisms for detecting sinkhole attack on 6LoWPAN in IoT", International Journal of Latest Trends in Engineering and Technology, Vol. 10, Issue 1, pp.134-137, 2018.

[26] Md. IftekharHussain, “Internet of Things: challenges and research opportunities”, DOI 10.1007/s40012-016-0136-6, pp. 1-9, 2016.

[27] Mian Ahmad Jan,Priyadarsi Nanda, Xiangjian He and Ren Ping Liu, "A Sybil attack detection scheme for a forest wildfire monitoring application", Future Generation Computer Systems, Vol. 80, pp. 613-626, 2018.

[28] Murat Demirbas and Youngwhan Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks", In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), pp. 1-7, 2006.

[29] OlfGaddour and AnisKoubba, “RPL in nutshell: A survey”, computer networks, Vol. 56, Issue 14, pp.3163-3178, 2012.

[30] Rashmi Sahay, G. Geethakumari, BarshaMitra and V. Thejas, "Exponential smoothing based approach for detection of blackhole attacks in IoT", In 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2018.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[31] Sabah Suhail, Shashi Raj Pandey and ChoongSeon Hong, "Detection of Selective Forwarding Attack in RPL-Based Internet of Things through Provenance", pp 965-967, 2018.

[32] Sabeen Tahir, Sheikh Tahir Bakhsh and Rayan A Alsemmeari, "An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things", International Journal of Distributed Sensor Networks Vol 15, Issue 11, pp. 1-10, 2019.

[33] Salavat Marian, PopaMircea, "Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme", In 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, pp. 121-124, 2015.

[34] Salehi, S. Ahmad, M. A. Razzaque, ParisaNaraei, and Ali Farrokhtala, "Detection of sinkhole attack in wireless sensor networks", In 2013 IEEE International Conference on Space Science and Communication (IconSpace), pp. 361-365, 2013.

[35] SeyyitAlperSert, Carol Fung, Roy George and Adnan Yazıcı, "An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks", In 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6, 2017.

[36] ShaplaKhanam, Ismail Ahmedyand Mohd Yamani Idna Idris, "An efficient detection of selective forwarding attacks in heterogeneous IoT Networks", pp 1-8, 2017.

[37] Shoukat Ali, Dr. Muazzam A Khan, Jawad Ahmad, Asad W. Malik, and AnisurRehman, "Detection and prevention of Black Hole Attacks in IOT & WSN", In 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), pp. 217-226, 2018.

[38] Sohail Abbas, "An Efficient Sybil Attack Detection for Internet of Things", In World Conference on Information Systems and Technologies, pp. 339-349, 2019.

[39] Stephen. R and Arockiam. L, “RDAID: Rank Increased Attack IDentification Algorithm for Internet of Things”, International Journal of Scientific Research in Computer Science Applications and Management Studies, Volume. 7, Issue 3, pp 1-5, 2018.

[40] Stephen. R and Arockiam. L, “RDAIDRPL: Rank Increased Attack IDentification Algorithm for Avoiding Loop in the RPL DODAG”, International Journal of Pure and Applied Mathematics, Vol. 119, Issue 16, pp.1-8, 2018.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[41] Stephen. R and Arockiam. L, “E2V: Techniques for Detecting and Mitigating Rank \Inconsistency Attack (RInA) in RPL based Internet of Things”, Journal of Physics, doi:10.1088/1742-6596/1142/1/012009, pp. 1-13, 2018.

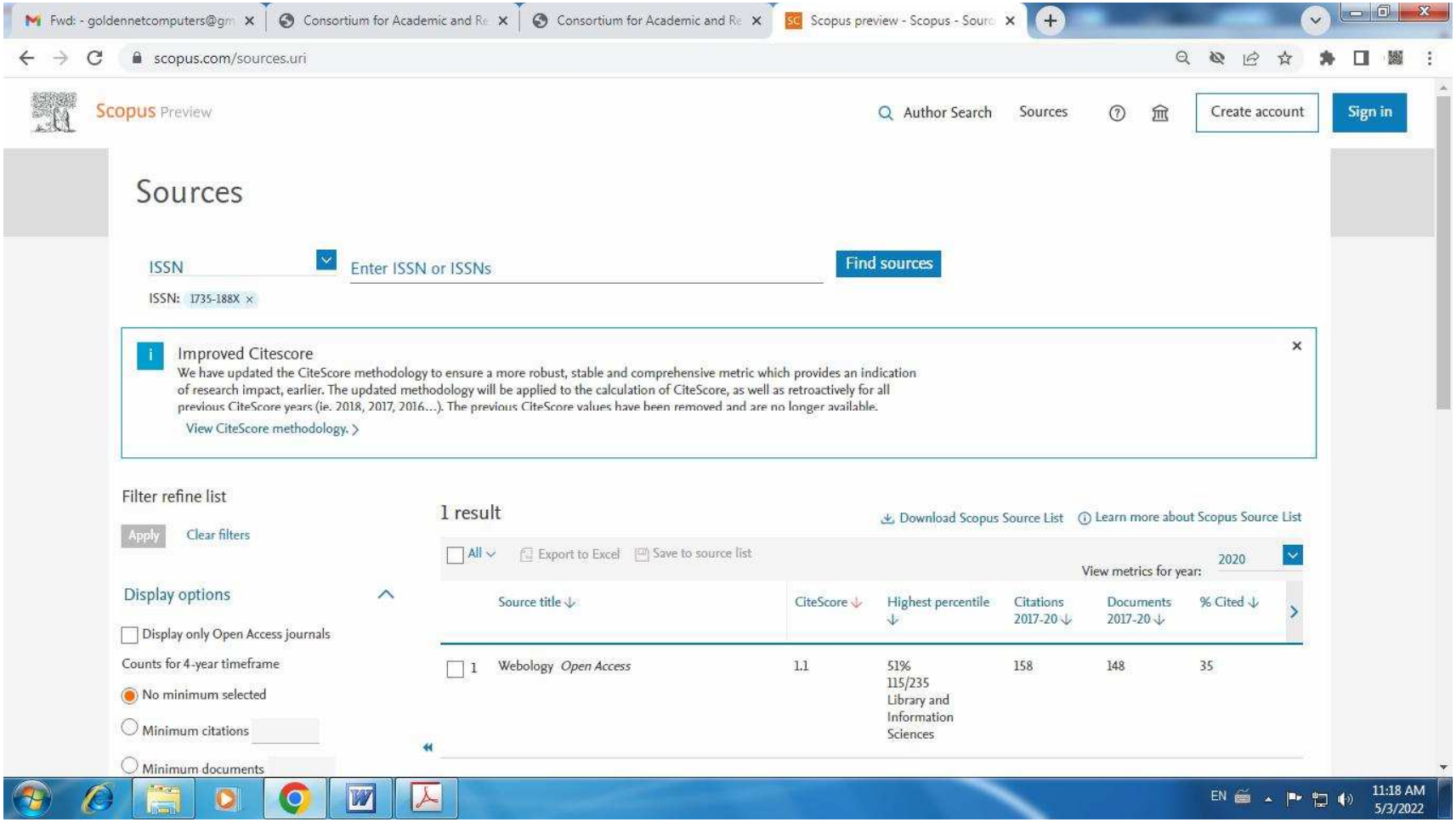
[42] Stephen, A. Dalvin Vinoth Kumar and L. Arockiam, "Deist: dynamic detection of Sinkhole attack for Internet of Things", International Journal of Engineering and Computer Science, Vol. 5, Issue 12, pp. 19358-19362,2016.

[43] Stephen, R., and L. Arockiam, "Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things", International Journal of Electrical Electronics and Computer Science, Vol 4, Issue 4, pp. 16-20, 2017.

[44] SumitPundir, Mohammad Wazid, DeveshPratap Singh, Ashok Kumar Das, Joel J. P. C. Rodrigues and Youngho Park, "Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment", Sensors Vol. 20, Issue 5, 1-27, 2020.

[45] Surinder Singh, Hardeep Singh Saini, "Detection Techniques for Selective Forwarding Attack in Wireless Sensor Networks", International Journal of Recent Technology and Engineering (IJRTE), Vol. 7, Issue 6S, pp. 380-383, 2019.

[46] VipindevAdat and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture”, DOI 10.1007/s11235-017-0345-9, pp. 1-99, 2017.


Fwd: - goldennetcomputers@gm
Consortium for Academic and Re
Consortium for Academic and Re
Scopus preview - Scopus - Sourc
scopus.com/sources.uri
Scopus Preview
Author Search
Sources
Create account
Sign in
Sources
ISSN
Enter ISSN or ISSNs
Find sources
ISSN: 1735-188X
Improved Citescore
We have updated the CiteScore methodology to ensure a more robust, stable and comprehensive metric which provides an indication of research impact, earlier. The updated methodology will be applied to the calculation of CiteScore, as well as retroactively for all previous CiteScore years (ie. 2018, 2017, 2016...). The previous CiteScore values have been removed and are no longer available.
View CiteScore methodology. >
Filter refine list
Apply
Clear filters
Display options
Display only Open Access journals
Counts for 4-year timeframe
No minimum selected
Minimum citations
Minimum documents
1 result
Download Scopus Source List
Learn more about Scopus Source List
All
Export to Excel
Save to source list
View metrics for year:
2020
Source title
CiteScore
Highest percentile
Citations 2017-20
Documents 2017-20
% Cited
1
Webology Open Access
1.1
51% 115/235 Library and Information Sciences
158
148
35
EN
11:18 AM
5/3/2022

Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

RSSI Based Rank Attack Detection Technique For RPL

A.Stephen[1] , Dr. L. Arockiam[2]

[1]Research Scholar**,** Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620 002, India.

[2]Associate Professor Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620 002, India.

Abstract

"Internet of Things (IoT)" is ahead of the curve in the digital era for the last ten years. IoT is the best thing since sliced bread which makes hard work into smart work in our day- to-day life. IoT connects things over the internet to communicate with each other in a network as an automated system. Routing Protocol for Low-Power and Lossy Networks (RPL) is a routing protocols which is used in IoT network. Several attacks have happened in RPL protocol. Rank attack is the most vulnerable attack among all other attacks. In this paper, rank attack detection technique based on Received Signal Strength Indicator (RSSI) is proposed. The technique is used only when objective function is set as hop count. The work has been mathematically tested by taking random RSSI values of the nodes and found to be more efficient.

Key words: Rank attack, RSSI, IoT, Objective function

Introduction

IoT

"IoT" is a resource constrained technology which has low power, low memory, and low energy. IoT connects many technologies into one technology to make human work much easier. So, it is booming globally day by day in all the fields such as home automation, smart health care, industrial, military and agricultural fields [11]. In IoT, everything is automated and sensitive data are communicated over IoT network. RPL is one of the network protocols which is used for transferring data from one device to another device.

RPL

RPL is created especially for IoT. RPL uses Destination Oriented Directed Acyclic Graph (DODAG) to form a network. Four control messages are used for constructing DODAG in RPL. The control messages are DODAG Information Object (DIO) which is used for broadcasting a

node information, DODAG Advertisement Object (DAO) which is used for broadcasting destination information, DAO_ACK which is used for responding to the DAO message and DODAG Information Solicitation (DIS) which is used for discovering neighbor nodes to join in the network. The DODAG is formed based on the objective function [12].

Objective Function

Objective function selects and optimizes the route in RPL. The widely used objective functions are Hop Count, Energy, Expected Transmission Count (ETX) and Minimum Rank with Hysteresis Objective Function (MRHOF)[13]. The objective function defines rank metric in RPL to select a node's parent.

Rank

Rank is the location of a node in the network [13]. The rank is increased from top to bottom and decreased from bottom to top. A node selects its parent which has lower rank than its rank [12]. In this paper, the hop count is used as the objective function. A node selects its parent based on hop count which has less hops to reach the root node. There is a possibility of changing rank value from low to high and from high to low by the intruder. The illegitimate changes of rank is called rank attack.

Rank Attack

The purpose of increasing and decreasing rank value is to generate traffic and control overhead in the network [9]. Rank attack is classified into two types such as rank increased attack and rank decreased attack [12]. There are many approaches used to detect rank attack such as Energy based technique, PDR based approach and Nodes' behaviour approach. A novel technique is proposed to identify rank attack while objective function is set as hop count. The node having a minimum hop count has good RSSI value for the communication path.

RSSI

Radio Signal Strength Indicator (RSSI) is used to find out the communication range between two nodes. RSSI is measured in decibel (dB). A node which is very near to another node has good RSSI value. A node which is far from another node has a bad RSSI value. The formula for calculating RSSI value is given below [14].

$$RSSI(X) = A – 10n*\log d$$

A – Received Signal Power

n – Path loss Index

d – Distance

The rest of the paper is structured into review of literature which contains related work of the proposed work, methodology that consists of a technique to detect rank attack, result and

discussion which contains mathematical computation to prove the proposed work is better than the other works based on RSSI and finally the conclusion is given.

Review of Literature

In [1], authors presented an overview of RPL topology, structure, security challenges and attacks against RPL in IoT. All the recent techniques which were used to detect and mitigate the RPL based attacks were clearly discussed. These techniques were compared using Frieddman test.

Zahrah et al. [2] reviewed the different techniques and methods to detect RPL attacks. Rank attack and Version number attack were explained in detail. These two attacks were compared by the attack detection accuracy metrics.

Fatima et al. [3] proposed a framework using machine learning for detecting rank attack and wormhole attack in RPL based IoT. The proposed framework consisted of three modules. The first module was choosing attack detection parameters. The second module was used for building and training the model based on machine learning. And the third module was used for activating the model to test the detection of rank and wormhole attacks.

In [4], RSSI based technique to estimate distance using Node MCU ESP 8266 in IoT was proposed. The authors took 300 sample RSSI values for the purpose of testing. The estimated distance based on the RSSI values was compared with the actual distance to find out the error level.

Mirko Ivanic et al. [5] presented RSSI based distance estimation technique for indoor and outdoor IoT environment. Curve fitting model was applied in this technique for finding the distance.

Mohamad Nikravan et al. [6] proposed a lightweight offline/online signature based scheme for mitigating rank and version number attack in IoT. The proposed scheme contained two phases such as offline phase and online phase. The proposed technique was compared with VeRA and TRAIL. And the proposed scheme secured more than the two existing algorithms.

Ahmed Raoof et al. [7] analyzed RPL protocol and attacks against the RPL protocol. Various techniques and methods used for identifying and mitigating RPL attacks were surveyed. The mitigation techniques were classified based on the attacks. The paper provided brief knowledge about mitigation techniques of RPL attacks.

Rashmi Sahay et al. [8] explored the vulnerabilities of rank property in RPL. The attack graph was presented to analyze various possible threads against rank property in RPL. The impact of the attacks which affected rank property were tested in Cooja simulator in Sky mote.

Felisberto Semedo et al. assessed the vulnerabilities in RPL objective functions for IoT. OF0 and Minimum Rank with Hysteresis Objective Function (MRHOF) were examined in the rank attack environment using Contiki Cooja simulator [9].

Usman Shafique et al. [10] proposed intrusion detection system to detect malicious nodes in RPL based IoT. The proposed work had high computation overhead because the detection process was done in sink node. The IDS was simulated with Cooja simulator.

Methodology

RSSI based rank attack detection technique is proposed specifically for hop count based DODAG construction. The nodes which have minimum hops to reach the root have low rank and nodes which have maximum hops to reach the root have high rank in the network. For each node, the RSSI value is calculated from the node to its parent. The total RSSI value from a node to root is computed by adding RSSI values of current node and RSSI values of its intermediate node. The computed values are stored in the root node .If any inconsistent change in the rank is found, the node is compared with its total RSSI value from root (TRRX) with its parent's total RSSI value from the root (TRRP(X)). If the current node has less RSSI value than its parent and higher rank than its parent then the current node is considered as malicious node. And the malicious node is removed from the network and new network will be formed. This technique contains three phases such as **Construction phase** where DODAG is formed, **TRRX computation phase** where the RSSI computation process is held and **Rank attack detection phase** where rank attack is identified using RSSI value.

Terms used in the Technique

TRRX - Total RSSI value from root node to current node.

Rnode - Root node.

IMn - Inter Mediator node.

X - Current node.

Pnode - Parent node

NBnodes – Neighbor nodes

OF – Objective Function

HC – Hop Count

TRRP(X) - RSSI value from root node to parent node of current node

Technique

Phase I – DODAG Construction

Input: RPL Control messages

Output: DODAG

Step 1: Rnode broadcasts the DIO message to start DODAG construction

Step 2: NBnodes receive and accept DIO message ⇔ OF(Rnode) & OF(NBnodes) =HC

Step 3: Compute Rank based on OF (HC) to select Parent Node

Rank (Pnode) < Rank (Child node)

Step 4: Child Node unicasts DAO message to its selected preferred parent node

Step 5: Parent node sends DAO_ACK message to its children then the DODAG is constructed.

Phase II – TRRX computation

Input: RSSI (X)

Output: TRRX

Step 1: If Pnode(X) = Rnode Then

TRRX = RSSI(X)

Step 2: If Pnode(X) ≠ Rnode Then

TRRX = RSSI(X+IMn1+IMn2+……IMnn)

Step 3: TRRX is stored in Rnode

Phase III – Rank Attack Detection

Input: TRRX, TRRP(X)

Output: Rank Attack Detection

Step 1: If Rank(X) > Rank(Pnode(X)) && TRRX < TRRP(X) then

X is legitimate node

Step 2: If Rank(X) < Rank(Pnode(X)) && TRRX < TRRP(X) then

X is affected by Rank Decreased Attack then remove X from the network

Step 3: If Rank(X) > Rank(Pnode(X)) && TRRX > TRRP(X) then

X is affected by Rank increased Attack then remove X from the network

Step 4: Form the new network after eliminating malicious nodes

Result and Discussion

Fourteen nodes have been taken for testing the proposed technique. The RSSI values of the nodes are taken randomly.

Let S be the set of all nodes in the network then

S = {A,B,C,D,E,F,G,H,I,J,K,N,M,N}

The communication path from Rnode to Nnode be

Path(Rnode, Nnode) = (Rnode, IMn1, IMn2, IMn3,…..IMnn, Nnode)

Path(X,Rnode) = (X, IMn1, IMn2, IMn3,…….IMnn, Rnode)

The communication path from Rnode to X be

If Parent(X) ≠ Rnode then, ∃ IMnode ∈ P(Rnode, Nnode) ------ A

If Parent(X) = Rnode then ∄ IMnode ------- B

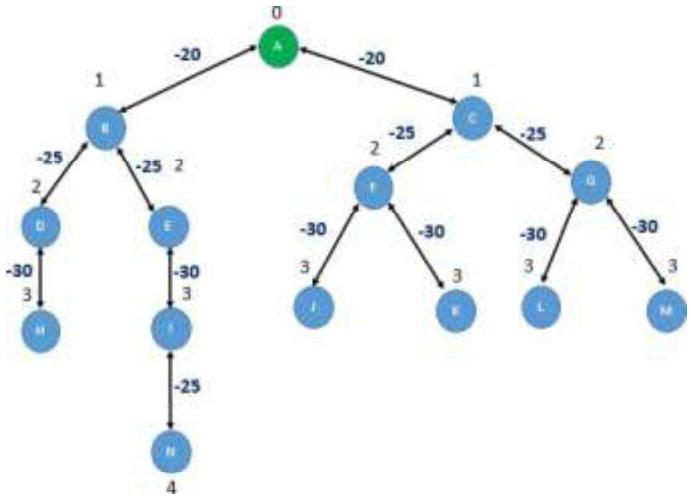


Fig 3.1 Rank and RSSI value of each Node

Fig 3.1 shows the hop count based DODAG construction. The RSSI value of each node concern with their path is given in the fig 3.1. A is the root node of all the nodes in the network. The rank attack detection process is done in the root node by analyzing the total RSSI value of each node (TRRX) in the network.

Table 3.1 Node properties

Node	Parent	Rank	IMN	RSSI(dB)	TRRX(dB)
A	-----	0	-----	---------	--------
B	A	1	-----	-20	-20
C	A	1	------	-20	-20
D	B	2	B	-25	-45
E	B	2	B	-25	-45
F	C	2	C	-25	-45
G	C	2	C	-25	-45
H	D	3	D-B	-30	-75
I	E	3	E-B	-30	-75
J	F	3	F-C	-30	-75
K	F	3	F-C	-30	-75
L	G	3	G-C	-30	-75
M	G	3	G-C	-30	-75
N	k	4	K-F	-25	-100

Table 3.1 shows rank of each node, RSSI values, intermediator nodes for each node and TRRX value from a node to root node. The RSSI value of the each node is taken randomly. Based on the RSSI value, the TRRX is computed.

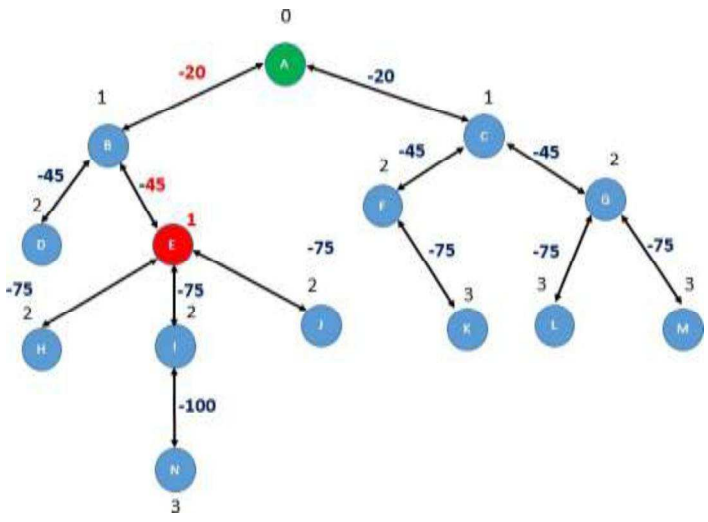


Fig 3.2 Malicious Node Identification

Fig 3.2 depicts the rank attack scenario by considering node E as the malicious node. In this scenario, the malicious node changes its actual value to lower rank in order to attract its nearby nodes in the network. The malicious node E is identified by comparing its TRRX with TRRP(X). From the table 3.1, TRRX(E) < TRRP(E) and Rank(X) < Rank (Parent(X)). So, node E is declared as malicious node.

Here, node H and J select E as their parents without knowing that the node E is affected by rank attack. The decreased rank attack causes several problems in the network such as packet loss, packet dropping and high traffic.

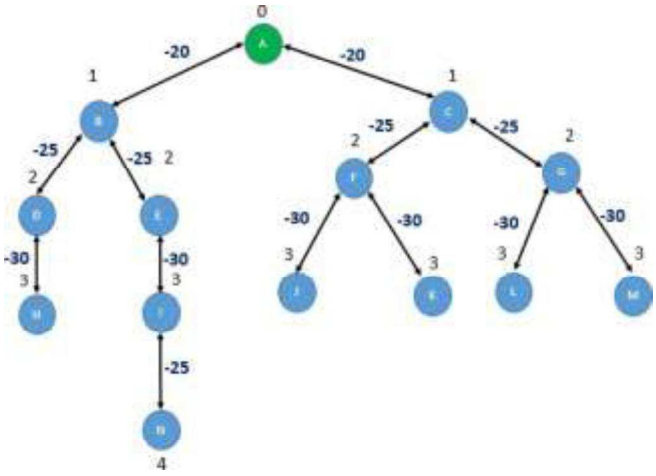


Fig 3.3 Re-construction of DODAG

So, E is declared as malicious node. And the root node informs to all nodes in the network that E is a malicious node and eliminates the node E from the network. After eliminating node E, the network is re-constructed with new DODAG version. The detection process is performed when there is inconsistent changes in the rank in the network.

Conclusion

There is no specific technique proposed to identify rank attack concerned with the selection of specific objective function. This research article focuses specifically on the hop count based DODAG construction rank issues. The article provides the novel technique to detect rank attack based on RSSI value while setting Hop count as an objective function. The proposed technique has been mathematically proved. In future, the proposed work could be implemented in Cooja simulator.

References

[1] Mohammed Amine Boudouaia, Adda Ali-Pacha, Abdelhafid Abouaissa, and Pascal Lorenz, "Security Against Rank Attack in RPL Protocol", IEEE Network, Volume 34, Issue 4, pp. 133-139, 2020.

[2] Zahrah A. Almusaylim, Abdulaziz Alhumam and N.Z. Jhanjhi,. "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review", Ad Hoc Networks, volume 101, Article 102093, pp. 1-7, 2020.

[3] Jhanjhi, N. Z., Sarfraz Nawaz Brohi, and Nazir A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning", DOI: 10.1109/MACS48846.2019.9024821, pp. 1-9, 2019.

[4] Suvankar Barai, Debajyoti Biswas and Buddhadeb Sau, "Estimate distance measurement using NodeMCU ESP8266 based on RSSI technique", IEEE, DOI: 10.1109/CAMA.2017.8273392, pp. 170-173, 2017.

[5] Mirko Ivanic and Ivan Mezei, "Distance estimation based on RSSI improvements of orientation aware nodes", IEEE, DOI: 10.1109/ZINC.2018.8448660, pp. 140-143, 2018.

[6] Mohammad Nikravan1, Ali Movaghar and Mehdi Hosseinzadeh, "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks", Wireless Personal Communications, Issue 99, Volume, pp. 1035-1059, 2018.

[7] Ahmed Raoof, Ashraf Matrawy, and Chung-Horng Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things", IEEE, Volume 21, Issue 2, pp. 1582-1606, 2018.

[8] Rashmi Sahay, G. Geethakumari and Koushik Modugu, "Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT", IEEE, DOI: 10.1109/WF-IoT.2018.8355171, pp. 308-313, 2018.

[9] Felisberto Semedo, Naghmeh Moradpoor and Majid Rafiq, "Vulnerability assessment of objective function of RPL protocol for Internet of Things", https://doi.org/10.1145/3264437.3264438, pp. 1-6. 2018.

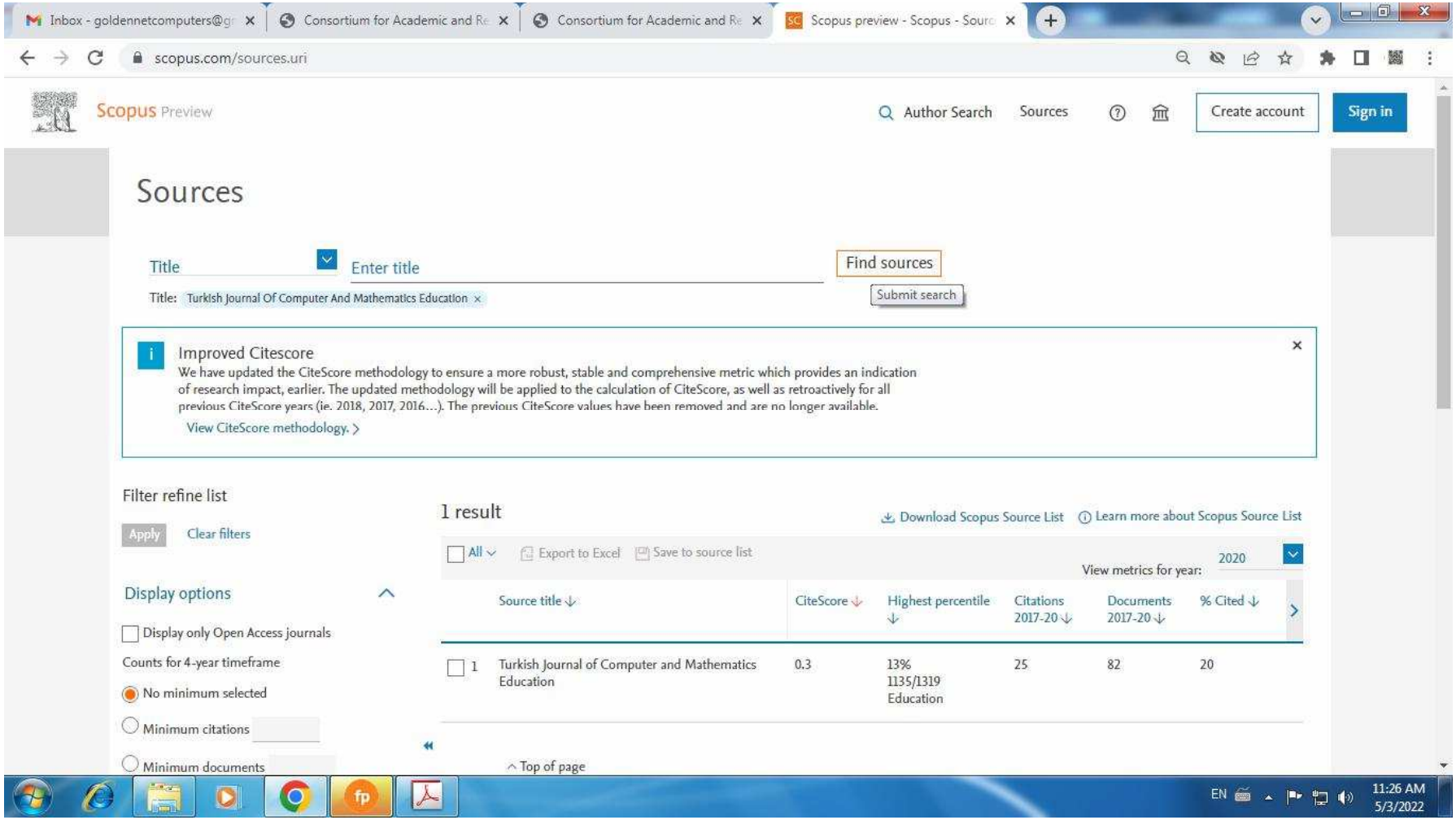
[10] Usman Shafique, Abid Khan, Abdur Rehman, Faisal Bashir and Masoom Alam "Detection of rank attack in routing protocol for Low Power and Lossy Networks", Annals of Telecommunications, Volume 73, Issue 7-8, pp. 429-438, 2018.

[11] C. C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT", https://doi.org/10.1007/s11277-020-07108-5, pp 1-47, 2020.

[12] Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z.Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review", Ad Hoc Networks, https://doi.org/10.1016/j.adhoc.2020.102096, Volume 101, pp 1-17, 2020.

[13] Boualam S.R., Ezzouhairi A, "New Objective Function for RPL Protocol", Embedded Systems and Artificial Intelligence, Springer, vol 1076, https://doi.org/10.1007/978-981-15-0947-6_64, pp. 681-690, 2020.

[14] Jungang Zheng , Chengdong Wu, Hao Chu and Yang Xu, "An improved RSSI measurement in wireless sensor networks", Procedia engineering, pp. 876-880, 2011.


Inbox - goldennetcomputers@g
Consortium for Academic and Re
Consortium for Academic and Re
Scopus preview - Scopus - Sourc
scopus.com/sources.uri
Scopus Preview
Author Search
Sources
Create account
Sign in
Sources
Title
Enter title
Find sources
Submit search
Title: Turkish Journal Of Computer And Mathematics Education
Improved Citescore
We have updated the CiteScore methodology to ensure a more robust, stable and comprehensive metric which provides an indication of research impact, earlier. The updated methodology will be applied to the calculation of CiteScore, as well as retroactively for all previous CiteScore years (ie. 2018, 2017, 2016...). The previous CiteScore values have been removed and are no longer available.
View CiteScore methodology. >
Filter refine list
Apply
Clear filters
Display options
Display only Open Access journals
Counts for 4-year timeframe
No minimum selected
Minimum citations
Minimum documents
1 result
Download Scopus Source List
Learn more about Scopus Source List
All
Export to Excel
Save to source list
View metrics for year:
2020
Source title
CiteScore
Highest percentile
Citations 2017-20
Documents 2017-20
% Cited
1
Turkish Journal of Computer and Mathematics Education
0.3
13% 1135/1319 Education
25
82
20
Top of page
EN
11:26 AM
5/3/2022

Level Based Rank Attack Detection Technique (LEACE)

A.Stephen [a] and Dr. L. Arockiam [b]

[a] *Research Scholar[1], Department of Computer Science, St. Joseph's College (Autonomous),(Affiliated to Bharathidasan University),Tiruchirappalli – 620 002, India*
[b] *Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous),(Affiliated to Bharathidasan University),Tiruchirappalli – 620 002, India*

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: *Internet of Things (IoT) prevails in the technological world among various technologies. The creation of IoT brings about a renaissance in the smart connected world. The security issues in IoT have risen alarmingly in recent years. These security issues are inalienable in IoT network. Particularly, attacks in IoT network layer exploit the entire IoT system. The most common attack which makes a big impacts on RPL based IoT network is rank attack. The impacts of rank attack could be reduced by providing efficient technique to identify and mitigate the rank attack. In this paper, a technique "LEACE" is proposed to identify and mitigate rank attack based on the level of the nodes in the network. Rank and level of the nodes are corresponded in the IoT system. For identifying rank attack, the level and rank of the nodes are checked whether the nodes' rank are corresponded with their level. The proposed technique outperforms the VeRa technique. It provides better results than the VeRa in terms of packet delivery ratio, detection accuracy and throughput.*

Key words: RPL, Rank attack, LEACE, IoT

.

1Introduction

Internet of Things (IoT) is a looming technology in the modern era which connects everything in the world via Internet. The connected things in an IoT system have distinct ID to communicate with each other. These things can be accessed by computers, smartphones and IoT equipped devices through Internet (**V.A. Jane et al., 2021)** IoT provides automated services in all fields such as home automation, agriculture, smart city, smart health care, etc. The sensitive data which are collected by the IoT system from these fields are needed to be secured from the intruders. Network security plays a major role for securing data in IoT. RPL based network security is the most predominant issue. RPL is designed for low power lossy network (LLN). RPL is the most used protocol for routing in Internet of Things. Rank attack is very harmful attack in RPL based IoT network **(A. Stephen et al., 2021)**. Rank attack changes the legitimate rank value into illegitimate. The rank attack reduces packet delivery ratio, throughput and energy. Rank attack is categorized into two types such as rank increased attack which increases the rank of the node illegitimately in the network and rank decreased attack which decreases the rank of the node illegitimately in the network. The proposed LEACE technique identifies and mitigates the rank attack based on the number of hops in the network.

Further, the paper is divided into four sections such as literature review, methodology, results and discussions and conclusion. Literature review section examines the related work of IoT and rank attack. Methodology section expounds the proposed technique. The result and discussions section explicates the experimental work and comparisons of the proposed work with existing technique. Ultimately, the conclusion gives the key idea of the proposed technique.

2. Review of Literature

Dhuha Khalid Alferidah1 et al., (2020)), IoT challenges, security and privacy issues were entailed. The context of the paper was detailed into two aspects such as layer-wise attack and taxonomy of the attacks. It explicated the most predominant issues in IoT. The attack tabulation in the paper gave the better comprehension of various attack in IoT.

Charles Wheelus et al., (2020), analyzed security crises in Internet of Things. The authors explained the securitythreats which provoked a security crises in IoT system. The authors were able to shed some light on the characteristics for securing the IoT environment. The framework for deploying secured IoT was proposed.

Sandeep CH et al., (2020), delved into IoT architecture, elements of IoT and security in IoT. The authors specially expounded the momentous role of security for IoT architecture and its development. The significant roles of security in each layer were explored. The attacks in Internet of Things were mooted by the authors.

Marius Preda et al., (2020), examined the portrayal of RPL attacks by simulating them in Cooja simulator. The impacts of RPL on resources, topology and data traffic in IoT were analyzed. The article was concluded that energy and packet loss ratio were the major parameters to be analyzed for detecting attacks in RPL protocol.

Mohammad Nikravan et al., (2018), explicated the topological vulnerabilities such as version number attack and rank attack. Authors introduced proficient scheme to counter these attacks. The scheme used online and offline signature process to scout out the predominant attacks in RPL. The scheme was compared with existing techniques namely TRAIL and VeRA. It achieved better results than the compared techniques in term of authentication.

Mohammed Amine Boudouaia et al., (2020), diverse techniques and methods were spotlighted which were used to get wind of rank attacks in RPL based Internet of Things. These techniques were looked over their key ideas behind finding and mitigating the rank attack in RPL. Friedman test was conducted to compare the impacts of rank attack, selective forwarding attack and IP spoofed attack on RPL.

Aditya Tandon et al., (2019), recommended enhanced trust based method to secure IoT routing against sybil and rank attacks. The method solved the destructive situation in IoT which was generated by simultaneous occurrence of sybil and rank attacks. It was compared with Sec-Trust protocol in terms of detection accuracy, energy consumption and throughput.

Abd Mlak Said et al., (2020), suggested anomaly based rank attack detection system using support vector machine in IoT network. The system was deployed in healthcare field to secure patients' sensitive data. The system provided better detection accuracy.

Manjula C Belavagi et al., (2020), proposed multiple intrusion detection system to identify detrimental attacks such as rank attack, wormhole attack, selective forwarding attack and denial of service attack in wireless sensor network. The proposed intrusion detection system was simulated using Cooja simulator on Contiki operating system with 10, 40 and 100 nodes. Different parameters like energy consumption, detection accuracy and false positive rate of malicious nodes were considered for evaluating the proposed system.

3. Methodology

In RPL based IoT network, the network is established in different form according to the objective function. The proposed technique "Level based Rank attack detection technique" uses hop count as objective function. In hop count based RPL construction, the node which has less hop count compared with other nodes in the network is selected as parent. The rank of a parent node is required to be less than its child/ children nodes. All the nodes in the network are divided into levels according to the rank of the nodes. The nodes which are having the same rank value are placed in same level. Each node is corresponded with its rank and level in the network. The levels of the nodes are stored in the root node. The levels are updated periodically. Before changing a rank of a node, it has to verify its level for detecting rank attack. If a node is not in the level with its corresponding rank then the node is considered as malicious node which is affected by rank attack. If the level of a node is less than its corresponding rank, it is affected by rank decreased attack. And if the level of a node is higher than its corresponding rank then it is affected by rank increased attack. The malicious node is isolated from the network. After isolating the affected node, the network is reconstructed.

3.1 Theoretical analysis of the proposed LEACE technique

For analyzing the proposed technique, forty nodes are taken and proved that the technique detects the rank attack in RPL based IoT network. Fig 1 shows the legitimate network with nodes' rank and corresponding levels.

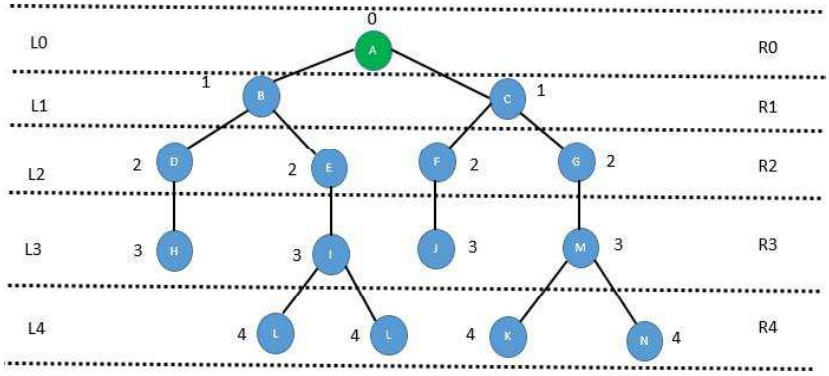


Fig 1 Level of each nodes

In right side of the fig 1, the nodes' rank is given and left side the nodes' level is displayed. R represents the rank of the nodes. L represents the level of the nodes. The correspondence of the rank and level are indicated with double side arrow which is given below.

R0 ⟷ L0

R1 ⟷ L1

R2 ⟷ L2

R3 ⟷ L3

R4 ⟷ L4

Table 1 Nodes' Level and Rank

Level	Rank	Nodes
L0	R0	A
L1	R1	B, C
L2	R2	D, E, F, G
L3	R3	H, I, J, M
L4	R4	L, O, K, N

Table 1 shows the nodes which are stored levelwise in the root table. The levels of the nodes' are checked by using this table. Let the node J be affected by rank attack which changes its rank into one in the given network.

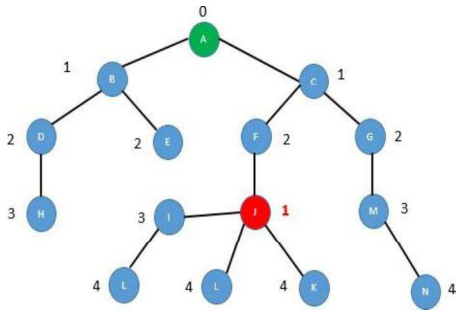


Fig 2 Network with rank attack

Now, the level of the node has to be verified from the table which is stored in the root node. From the table 1, the rank of node J is one but the corresponding level for node J is four. So, the rank of the node J does not correspond with its level. It is declared that there is no corresponding matches with rank and level for node J. So, node J is affected by the rank attack. Node J has to be isolated from the network.

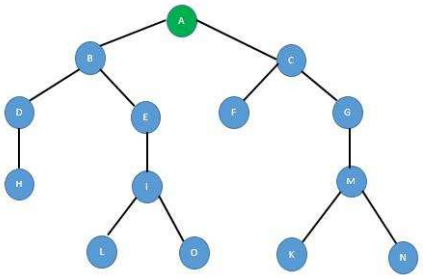


Fig 3 Reconstruction of the network

Fig 3 shows the reconstruction of the network. The node J is isolated from the network and network is reconstructed with the legitimate nodes. After reconstructing the network, the nodes' level table is updated with current rank and level for the available nodes in the network.

Labels used in the Technique

NHC – Number of hop count
L - Level of a node
CU – Current node
RT – Root node
NR – Neighbor nodes
RK –Rank of a node
PA – Parent node
Ch – Children
AN – All nodes in the network

3.2 Proposed "LEACE" technique

Input : *RPL Control messages, L, RK*

Output: *Rank attack detection*

1: RT multicasts the DIO messages

2: NR receives DIO messages and send DAO to RT

3: Compute

$RK(CU) = RK(PA(CU)) + HC(CU, PA)$

4: Children unicast DAO to their selected parents.

5: PA sends DAO_ACK message to CH then the DODAG is constructed.

6: Compute Level of each node from RT to AN based on RK of nodes

for i=0; i++; i<=n-1 // i is Index of Level, n is total number of nodes in the network

{

$L_i = i+0;$

}

7: Do corresponding process of nodes' rank with nodes' level

$L_i \longleftrightarrow RK_j$

8: Rank attack detection process

If L (CU) = RK (CU)

CU is an legitimate node

If L (CU) < RK (CU)

CU is affected by rank increased attack

If L (CU) > RK (CU)

CU is affected by rank decreased attack

10: Isolate the affected nodes

11: Reconstruct the network

4. Experimental Result

For implementing level based rank attack detection technique, Cooja simulator is used over the Contiki operating system. Forty nodes have been taken for the testing process. The sky mote is used to simulate the proposed work.

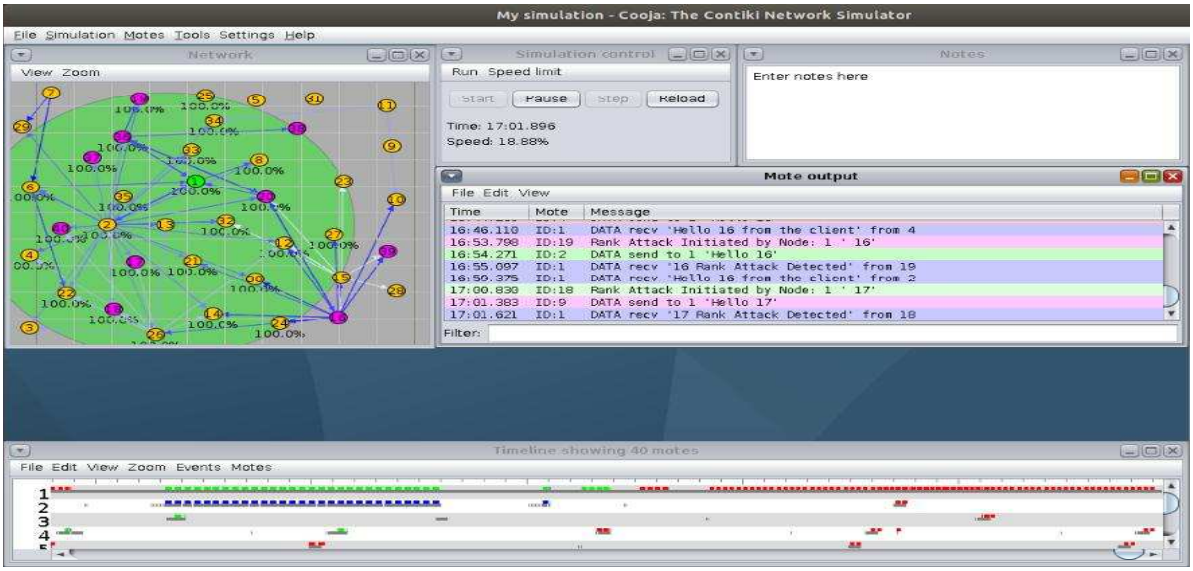


Fig 4 Rank Attack identification

Fig 4 exposes the rank attack detection process. The node which is in green colour is the root node. The yellow colour nodes are legitimate nodes in the network. The pink colour nodes are malicious nodes which are affected by the rank attack. The nodes which are detected as malicious nodes are specified in the mote output.

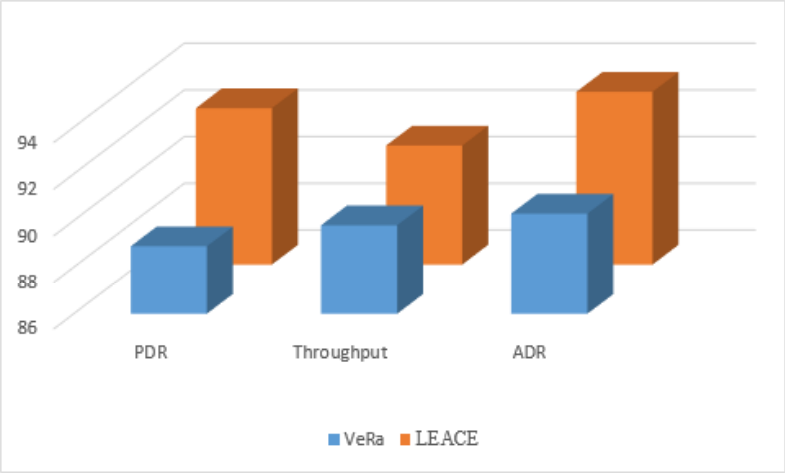


Fig 5 LEACE vs VeRa

Fig 5 depicts the comparison of the proposed work. The proposed work is compared with the existing technique VeRa in terms of packet delivery ratio, throughput and attack detection rate. The values for Packet delivery ratio (PDR), Throughput and Attack Detection Ratio are given in percentage. The proposed LEACE technique has performed better than the VeRa technique.

5. Conclusion

The proposed technique is a proficient technique to detect rank attack in RPL based Internet of Things. It identifies rank attack using the level of the nodes in the network. Each node is corresponded with rank and level in the network. The proposed work outperformed the existing technique VeRa in terms of packet delivery ratio, throughput and attack detection accuracy. In future, the work will be tested for other attacks such as block hole attack, sinkhole attack, version number attack and hello flood attack in Internet of Things environment.

References

[1] Dhuha Khalid Alferidah1 and NZ Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things", International Journal of Computer Science and Network Security, Volume 20, Issue No.4, 2020, pp. 263-285

[2] Charles Wheelus and Xingquan Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework." IoT,Volume 1, Issue 2, 2020, pp. 259-285.

[3] Sandeep CH, Naresh Kumar S, Pramod Kumar P,"Significant Role of Security in IoT Development and Iot Architecture", Journal Of Mechanics Of Continua And Mathematical Sciences, Volume 15, Issue 6, 2020, pp 174-184.

[4] Marius Preda and Victor Valeriu Patriciu, "Simulating RPL Attacks in 6lowpan for Detection Purposes", 13th International Conference on Communications (COMM), Bucharest, Romania, pp. 239-245, 2020, doi: 10.1109/COMM48946.2020.9142026.

[5] Mohammad Nikravan, Ali Movaghar and Mehdi Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Volume 99, Issue 2, 2018, pp. 1035-1059.

[6] Mohammed Amine Boudouaia, Adda Ali-Pacha, Abdelhafid Abouaissa and Pascal Lorenz, "Security against Rank Attack in RPL Protocol", IEEE Network, Volume 34, Issue 4, 2020, 133-139.

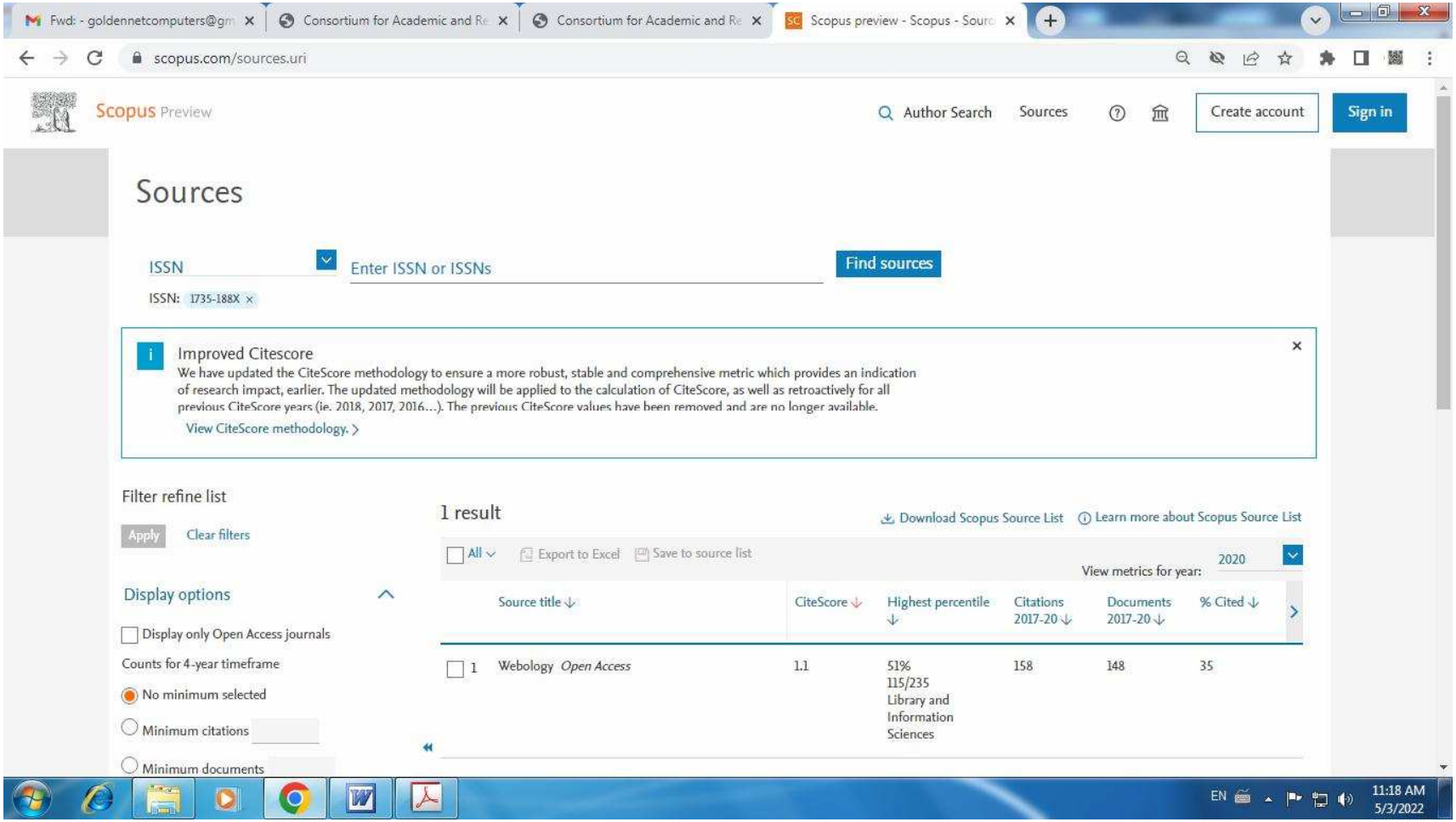
[7] Aditya Tandon and Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-7, doi: 10.1109/IC3.2019.8844935.

[8] Abd Mlak Said, Aymen Yahyaoui, Faicel Yaakoubi, and Takoua Abdellatif, "Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure." In International Conference on Smart Homes and Health Telematics, Springer, Cham, pp. 28-40, 2020, doi: 10.1007/978-3-030-51517-1_3.

[9] Manjula C Belavagi and Balachandra Muniyal, "Multiple intrusion detection in RPL based networks", International Journal of Electrical and Computer Engineering, Volume 10, Issue 1, 2020, pp. 467-476.

[10] V. A. Jane, Dr. L. Arockiam. (2021). DaRoN: A Technique for Detection and Removal of Noise in IoT Data by using Central Tendency. Annals of the Romanian Society for Cell Biology, 25(2), 3197Ranjeeth, S., Latchoumi, T. P., & Paul, P. V. (2020). Role of gender on academic performance based on different parameters: Data from secondary school education. Data in brief, 29, 105257.

[11] A. Stephen and Dr. L. Arockiam, "Attack against RPL in ioT: A Survey", Annals of the Romanian Society for cell Biology, Volume 25, Issue 4, 2021, pp. 9767 – 9786.


Fwd: - goldennetcomputers@gm
Consortium for Academic and Re
Consortium for Academic and Re
Scopus preview - Scopus - Sourc
scopus.com/sources.uri
Scopus Preview
Author Search
Sources
Create account
Sign in
Sources
ISSN
Enter ISSN or ISSNs
Find sources
ISSN: 1735-188X
Improved Citescore
We have updated the CiteScore methodology to ensure a more robust, stable and comprehensive metric which provides an indication of research impact, earlier. The updated methodology will be applied to the calculation of CiteScore, as well as retroactively for all previous CiteScore years (ie. 2018, 2017, 2016...). The previous CiteScore values have been removed and are no longer available.
View CiteScore methodology. >
Filter refine list
Apply
Clear filters
Display options
Display only Open Access journals
Counts for 4-year timeframe
No minimum selected
Minimum citations
Minimum documents
1 result
Download Scopus Source List
Learn more about Scopus Source List
All
Export to Excel
Save to source list
View metrics for year:
2020
Source title
CiteScore
Highest percentile
Citations 2017-20
Documents 2017-20
% Cited
1
Webology Open Access
1.1
51% 115/235 Library and Information Sciences
158
148
35
EN
11:18 AM
5/3/2022

Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

Location Based Rank Attack Detection Technique (LRADT)

A.Stephen[1] , Dr. L. Arockiam[2]

Research Scholar[1] , Associate Professor[2]

Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620 002, India.

Abstract
Internet of Things (IoT) turns up the computerized world with smart automated system through Internet. IoT has lots of issues such as internet outage, light weight, connectivity, big data privacy and security in the connected environment. Network security is the predominant issue in Routing Protocol for Low Power and Lossy Networks (RPL) based IoT. Rank attack is one of the issues in RPL. Rank attack is ruinous to RPL based network in Internet of Things compared with other attacks. In this paper, location based rank attack detection technique is proposed (LRADT). This technique uses distance of each node to find the location of the given nodes to root node in a network. The technique LRADT surpasses the existing technique RDAID by means of packet delivery ratio, attack detection rate and throughput.

Keywords: IoT, Rank Attack, Security, LRADT

1. Introduction

1.1 IoT

In 1999, Kevin Ashton coined the term "Internet of Things (IoT)". According to Kevin Ashton, IoT is a technology which connects physical and virtual things via Internet. Each thing in the connected system has its own identity and attributes. IoT is a resource constrained technology which supports low power, low memory and so on. It only supports light weight process over the connected network. IoT has different layered architecture with regard to the users' requirements or needs. But three layer architecture is the most common and widely used architecture.

1.2 IoT Architecture

The internet |Engineering task force (IETF) explicates three layer architecture in Internet of Things. Taking into account the rapid requirements of the IoT users, the three layer architecture is reformed into four layer architecture, five layer architecture and seven layer architecture. The three layer architecture is the fundamental for all other architectures. It comprises of perception layer, network layer and application layer.

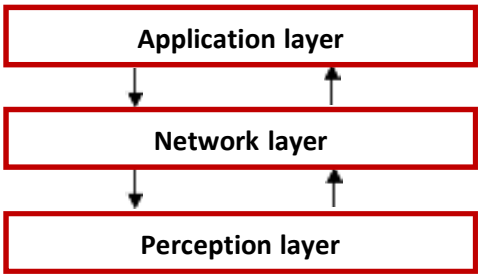


Fig 1.1 IoT Three Layer Architecture

Perception layer monitors the physical properties of the connected things in IoT network. It has the responsibilities of collecting data from the sensors which are embedded in the smart things. Network layer is responsible to connect things, network devices and servers. It is also used to process and transmit the collected data to the application layer. Standard protocols are used to transmit the data. Application layer provides various services to the IoT users according to their needs based on the available data.

1.2 Issues in IoT

Though, IoT is an emerging technology, it is weakened by lots of issues. The various issues in IoT are as follows.

Internet outage:

Internet connection is mandatory for Internet of Things for connecting and communicating smart things. If the Internet connection is unavailable, the entire IoT system is inoperable. And also poor Internet connection leads to worst service.

Light weight:

IoT is a resource constrained technology. It supports only lightweight mechanisms in the IoT system. The heavyweight mechanism cannot be used in IoT. But, for solving critical problems, IoT needs heavy weight mechanisms.

Connectivity:

Due to the rapid growth of IoT technology, numerous devices are connected in a single IoT system. Connecting N number of devices in a single system causes various issues such as device failure, connection problem, poor quality of service, reliability and hard to handle big data.

Big data:

Tremendous devices generate enormous data in IoT. As IoT is resource constrained, the enormous data cannot be stored in the IoT system. So storing and processing big data is not possible in IoT.

Privacy:

IoT accesses anything at any time at anywhere. Everyone or everything which is connectedto IoT can easily be tracked. So the privacy of IoT users is a challenging issue.

Security:

Crucial data of the users are collected by the IoT devices which should not be revealed to anyone except the concerned users. Since, IoT is connected through Internet at all the time, an intruder can easily hack the data and system. Collected data is processed by network layer, the network security is more important. Various protocols are used in network layer. RPL is one of the network protocols in IoT. Different attacks occur in RPL protocol. So there is a need to providea new technique to identify the attacks in RPL.

1.3 RPL

Routing Protocol for Low-Power and Lossy Networks is explicitly designed for Low power LossyNetwork. It is used in IoT for routing. RPL uses Destination Oriented Directed Acyclic Graph (DODAG) to form the network. It utilizes four types of control messages to construct DODAG. The control messages are as follows (i) DODAG information Object (DIO) which is used for providing node basic information. (ii) DODAG Information Solicitation (DIS) is used for probingneighbour nodes in the network. (iii) DODAG Advertisement Object (DAO) is used to propagatereverse route information. (iv) DODAG Information Advertisement Acknowledgement (DAO_ACK) provides acknowledgement for DAO message. For constructing DODAG, the objective function such as Expected Transmission Count (ETX), Hop count and Energy are used.

1.4 Rank Attack

Position of a node towards the root node is specified by the Rank. A node in the network selects its parent which is less than its Rank. The rank of a parent node must be less than its child node. Inconsistent change of rank in the network may form loop. Illegitimate change in the rank of a node over RPL protocol is called as rank attack in the IoT network. The rank attack is classified into two types namely rank increased attack and rank decreased attack. Impacts of rank attacks are less packet delivery ratio, worst parent selection and high packet loss.

The proposed LRADT technique is used to detect both rank increased attack and rank decreased attack. The technique uses location of the nodes to identify attack in the network. It is simulated using Contiki OS and Cooja simulator with fifty nodes in random position environment.

Rest of the paper is formulated into different sections such as review of literature which speaks about the related works of rank attack, methodology which explicates the proposed technique, result and discussion which justifies the proposed technique, experimental result which brings out the fact of the proposed work in virtual IoT environment and finally conclusion.

II Review of literature

Shadab Alam et al..[1] discussed the enabling technologies in Internet of Things. The authors explained requirements of IoT system with concerned application.

Mark Mbock et al.[2] detailed the privacy and security issues in IoT in terms of security requirements, techniques to face IoT threats and counter measuring the privacy issues. The threat taxonomy was figured out relatively to the current IoT applications scenario.

Akanksha Jain et al.[3] surveyed attacks and countermeasures for RPL protocol. The paper was one of the bedrocks to learn and analyze distinct attacks in RPL routing protocol. The authors unfolded the impacts of various attacks such as sinkhole attack, wormhole attack, selective forward attack and rank attack in IoT network. The paper was a panacea to fathom out the countermeasure of the RPL attacks.

Somnath Karmakar et al.[4] analyzed the attacks in RPL based Internet of Things and found that rank attack was the predominant attack among other attacks which caused detrimental impacts on the IoT system. Authors proposed a technique to detect rank attack with low overhead.The technique was used to detect both rank increased attack and rank decreased attack in non- storing mode. The proposed technique made use of DAO control message by incorporating message authentication code in the control message to detect the attack. The technique was energyefficient and provided better detection accuracy. It was implemented by Cooja simulator.

Nabil Djedjig et al.[5] recommended a new RPL version using trust based mechanism. Trusted platform module was used to check the trustworthiness of the proposed RPL. The new RPL version was evaluated by the authentication method in the trusted platform module. The behavior of the available nodes in the network analyzed to confirm trustworthiness of the IoT system.

Eli Kfoury et al.[6] suggested intrusion detection system to detect attacks in the RPL protocol. The self-organization map was trained by the supervised learning method to detect the attacks. The abnormal behavior in the protocol was found using the self-organization map. The required data for the model was generated using Cooja simulator by running the RPL based IoT network system. It performed better in terms of energy consumption and attack detection accuracy

Mina Zaminkar et al.[7] proposed SoS-RPL to secure against sinkhole attack in Internet of Things. It consisted of two sections. The first section was used to rate and rank the nodes using distance. The second section was used to discover the malicious sources in the IoT network by calculating average packet transmission of route request (RREQ). The SoS-RPL was tested using NS-3 simulation. It provided good packet delivery rate and better detection rate.

Mina Zaminkar et al.[8] suggested DSH-RPL for secured IoT ecosystem. It comprised of four phases. Reliable RPL was created in the first phase. In the second phase the sinkhole attack

was detected. The detected malicious nodes were quarantined in the third phase. In the fourth phase, data was transmitted after homomorphic encryption process. It reduced false positive rate and false negative rate. It increased packet delivery rate compared with Sec Trust-RPL and IBOOS-RPL.

Zahrah et al.[9] proposed SRPL-RPL protocol to detect and mitigate rank and version number attacks. The attacks were detected using rank strategy. The mitigation was done using threshold and attack status table. The proposed SRL-RPL was compared with existing system such as sink based intrusion detection systems and RPL+Shield technique. The proposed SRPL-RPL outperformed better than these existing protocols with regard to packet delivery ratio, energy consumption and attack detection accuracy rate.

3. Methodology

Location based rank attack detection technique (LRADT) is proposed to detect rank attack in hopcount based RPL construction. The proposed technique calculates distance of each node to its parent node and to its root node, to identify the node location. The location of each node is identified by calculating the distance of each node and stored in the root node. The distance of a node is compared with its parent's distance to root node, when there is an inconsistent change in the rank of the parent and child. If the distance and rank of the current node are less than its parent then it is affected by rank decreased attack. If the distance is less than its parent and rank is higher than the parent then the node is affected by rank increased attack. The affected node is cleared away from the network. The logic behind the rank and distance is, while constructing RPL network by hop count as the objective function parent node must have less distance than the child node. LRADT is compared with the RDAID technique. The RDAID technique uses packet delivery ratio of each transaction of the nodes in the network. The LRADT performs better than the RDAID technique in terms of packet delivery ratio, throughput and attack detection rate.

3.1 Theoretical Analysis

The location based rank attack detection technique is used to detect rank attack specifically whilesetting hop count as an objective function in RPL network. For examining the proposed technique,the RPL based IoT network with ten nodes (A,B,C,D,E,F,G,H,I,J) has been taken. Node "A" is the root node. The rank of a node is shared by the DIO message in the RPL network. Fig. 3.1 represents the RPL network with rank of each node towards root node before attack.

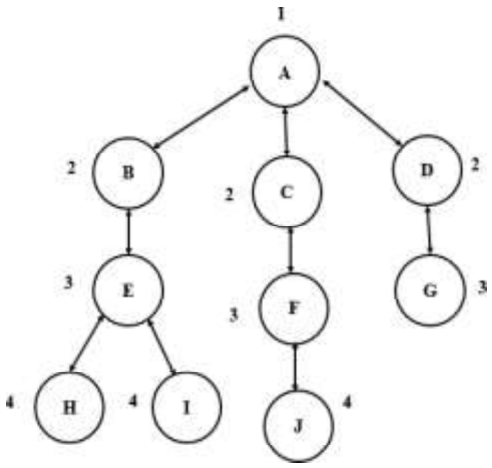


Fig. 3.1 RPL network before attack

Table 3.1 shows the distance of each node from the root node as well as to its parent node. This table is stored in the root node. The distance of the nodes in the given network is calculated periodically. The X and Y values for finding location of the nodes given in the table are taken from Cooja simulator. For identifying the location, first the distance from node to its parent is calculated and then the distance from node to root is calculated.

Table 3.1 Location of the Nodes

Node	Rank	X	Y	Distance to its parent	Distance to the root
A	1	76.42	23.14	--------	---
B	2	46.95	45.17	51.5	51.5
C	2	78.29	47.96	26.69	26.69
D	2	112.7	44.24	57.38	57.38
E	2	45.71	67.19	23.26	74.76
F	3	81.70	72.78	28.23	54.92
G	3	111.4	70.91	25.37	82.75
H	4	126.17	96.66	48.51	123.27
I	4	56.88	94.28	15.92	90.68
J	4	82.94	99.76	28.22	83.14

Before the occurrence of rank attack, the parent nodes have lower rank than their children nodes. Fig 3.2 depicts the rank attack scenario. In Fig 3.2, node E is considered as a malicious node which is affected by rank attack. For identifying whether the node is affected by rank attack, rank of the node E and its parent's rank are compared. The parent node must have low rank than its child / children.

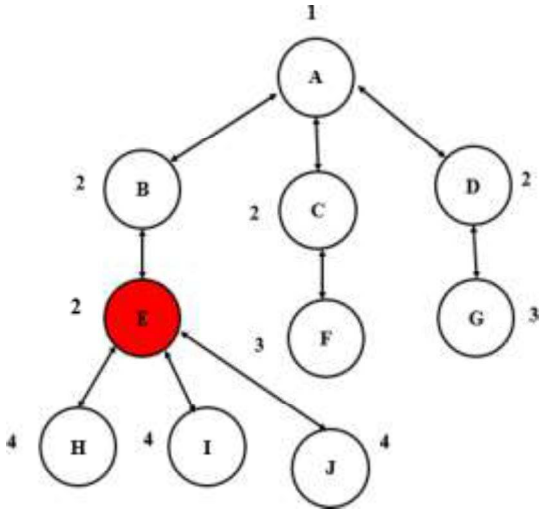


Fig. 3.2 RPL network after attack

Rank of node E is 2 as well as the rank of its parent also 2. Ranks of both nodes are same. So, there is an illegitimate change in the rank. Now, for identifying which node is affected by the rank attack, the location of both nodes are found by calculating distance of both nodes. In the table 3.1 node E is located 74.76 meters from the root node and node B is located 26.69 meters from the root node. So, node E is far away from the root node compared with node B. Now it is found that node E is affected by rank attack. Fig 3.3 depicts re-construction of the network.

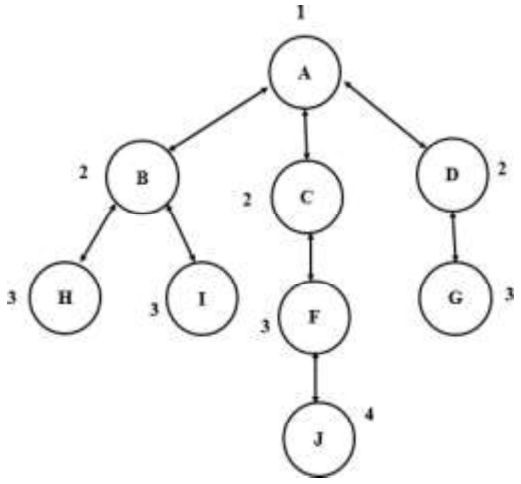


Fig. 3.3 RPL network after reconstruction

The affected node E should be removed from the network. The root node sends the message to all the nodes in the network that node E is affected by rank attack. The nodes connected with node E receive the message from root node and remove node E from the network. After removing the affected node, the nodes will form new network with a new version.

3.2 Labels used in the Technique

X – Root node,
P – Parent node
N – Nodes in the network
Y – Neighbor nodes
K –Current node
R – Rank of a Node
C – Child node

Input : RPL Control messages, LRADT
Output : Rank Attack Detection

1: X multicasts the DIO message and followed by N to start DODAG construction

$$X, N \xrightarrow{DIO} Y$$

2: Yi receive and accept DIO message

3: Compute R

$$R(K) = R(P) + HC(K, P)$$

$$R(P) < R(K)$$

4: Child Node unicasts DAO message to its selected preferred parent node

$$C \xrightarrow{DAO} P$$

5: P sends DAO_ACK message to C then the DODAG is constructed.

6: Identify the node location by Calculating D for all nodes from K to P and K to X

$$D = | x2-x1| + |y2-y1|$$

7: If $R(K) > R(P(K)) \&\& D(P(K)) < D(K)$ then

K is legitimate node

8: If $R(K) < R(P(K)) \&\& D(P(K)) > D(K)$ then

K is affected by Rank Decreased Attack then remove K from the network

9: If R(K) < R(P(K)) && D(P(K)) D(K)then

K is affected by Rank increased Attack then remove K from the network

10: Form the new network after eliminating malicious nodes

The above proposed technique uses traditional process for constructing DODAG in RPL which is given in the technique from step 1 to step 5. The novelty of the proposed work is to identify the rank attack using location of the nodes in the network which is given in the technique from step 6 to step 10.

4. Experimental Evaluation

Contiki operating system and Cooja simulator are used for deploying the proposed technique. It isone of the best network simulation tools for IoT. Simulation is done with the proposed technique for fifty nodes. In Fig 4.1, the green colour node is root node. The yellow colour nodes are legitimate nodes and pink colour nodes are malicious nodes affected by rank attack.

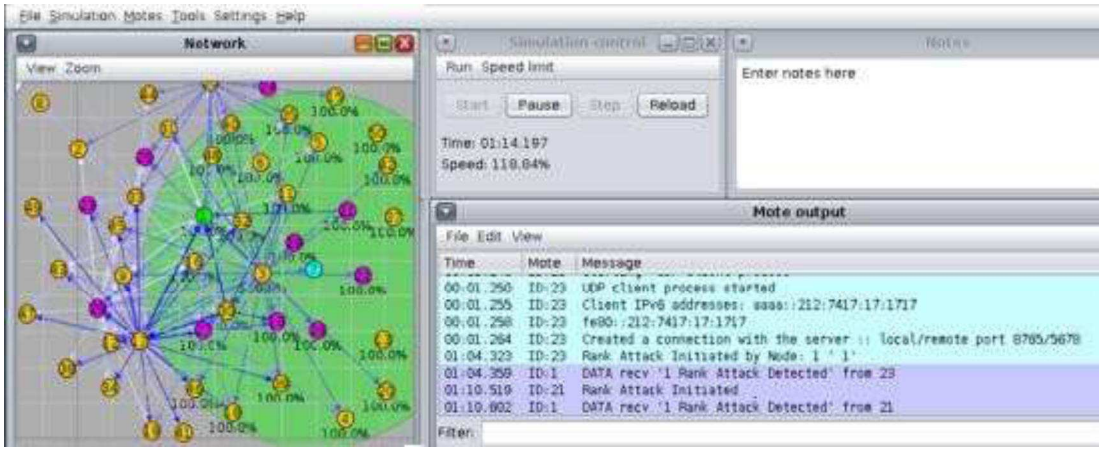


Fig 4.1 Attack simulation

In output window, the affected nodes are listed. The packets are analyzed in 6LOWPAN analyzer mode in Cooja simulator. Fig 4.2 shows the comparison of RDAID and LRADT techniques. It shows the performance metrics evaluation in percentage.

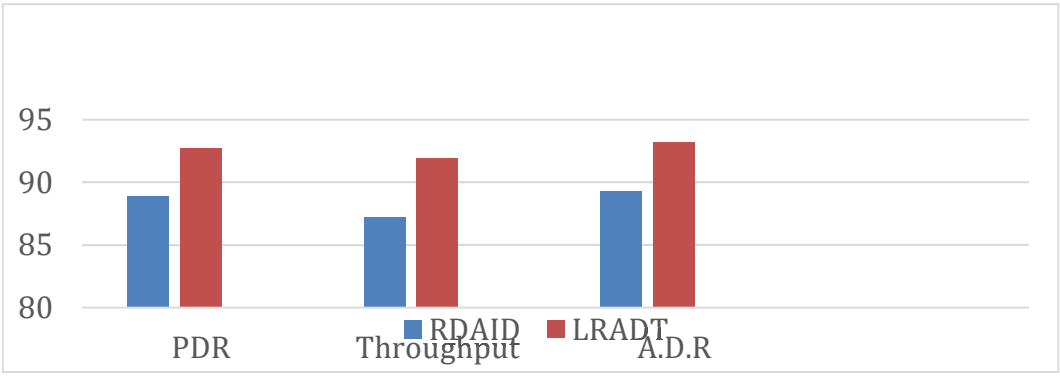


Fig 4.2 Attack simulation comparison

The attack detection rate (A.D.R) is measured using confusion matrix. Proposed technique outperforms the existing technique RDAID in terms of packet delivery ratio, throughput and attack detection rate. The better attack detection rate leads to better packet delivery ratio and the better packet delivery ratio leads to better throughput in the network. These are achieved by the proposed "LRADT" technique.

Conclusion

The technique "LRADT" is the proficient technique to detect and mitigate rank attack in hop countbased RPL network in IoT. It uses location of a node to find out the rank attack. It outperforms theRDAID technique in terms of packet delivery ratio, throughput and attack detection rate. The technique is implemented using Cooja simulator in sky Mote with fifty nodes. In future, the work will be enhanced to detect rank attack in ETX and Energy based RPL network in IoT.

References

[1] Shadab Alam, Shams Tabrez Siddiqui, Ausaf Ahmad, Riaz Ahmad and Mohammed Shuaib, "Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges", Advances in Data and Information Sciences, https://doi.org/10.1007/978-981-15-0694-9_12, pp. 119-126, 2020.

[2] Mark Mbock Ogonji, George Okeyo and Joseph Muliaro Wafula, "A survey on privacy and security of Internet of Things", Computer Science Review, pp. 1-19, 2020.

[3] Akanksha Jain and Sweta Jain, "A Survey on Miscellaneous Attacks and Countermeasures for RPL Routing Protocol in IoT", Emerging Technologies in Data Mining and Information Security, Advances in Intelligent Systems and Computing, https://doi.org/10.1007/978-981-13-1501-5_54, pp. 611 - 620, 2019.

[4] Somnath Karmakar, Jayasree Sengupta and Sipra Das Bit, "LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT", IEEE, International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 429-437, 2021.

[5] Djedjig Nabil, Djamel Tandjaoui and Faiza Medjek, "Trust-based RPL for the Internet of Things", IEEE Symposium on Computers and Communication (ISCC), pp. 962-967, 2015.

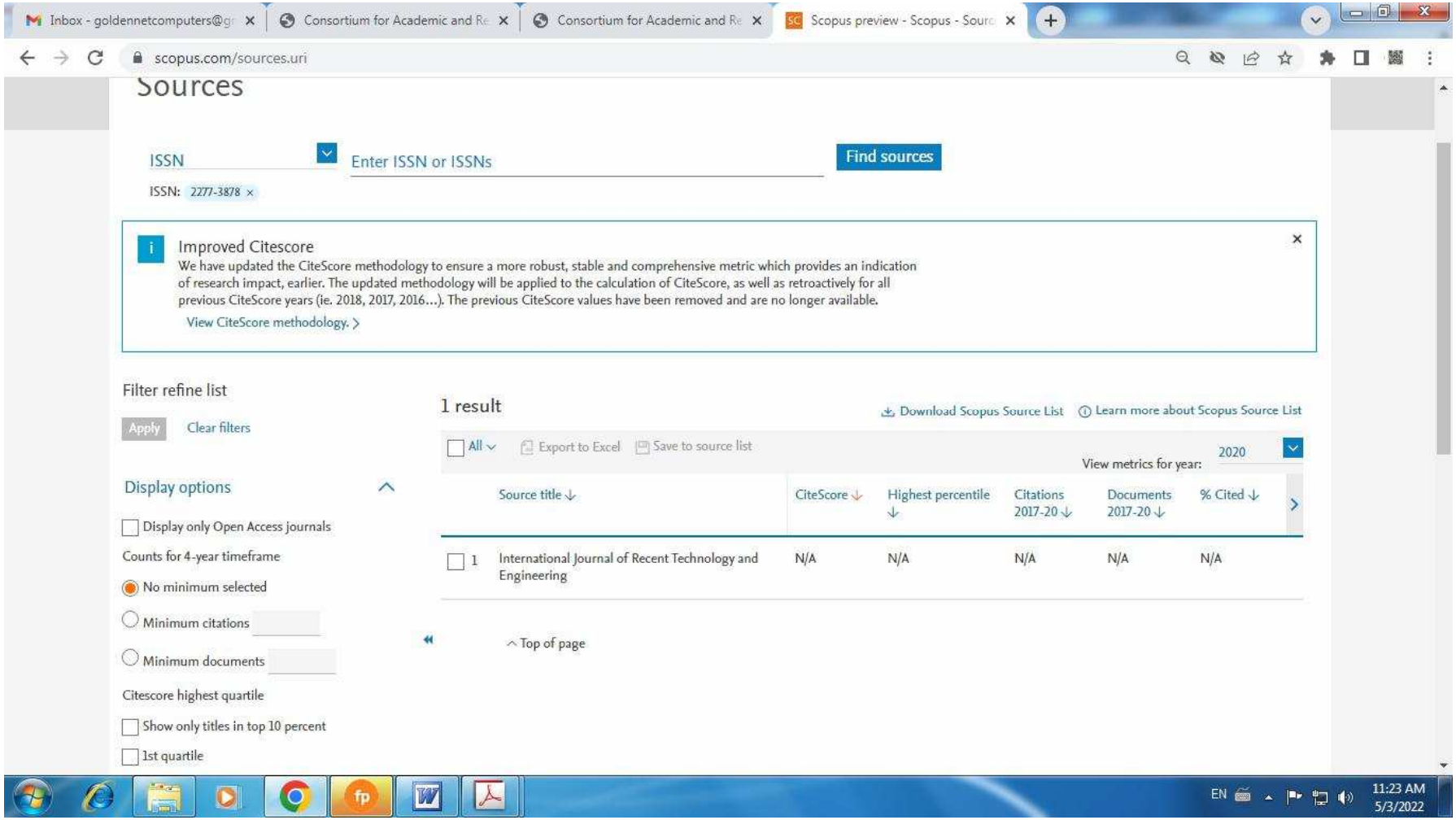
[6] Elie Kfoury, Julien Saab, Paul Younes and Roger Achkar, "A self organizing map intrusion detection system for rpl protocol attacks." International Journal of Interdisciplinary Telecommunications and Networking (IJITN) Volume 11, Issue no. 1, pp. 30-43, 2019

[7] Mina Zaminkar and Reza Fotohi, "SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism." Wireless Personal Communications, pp. 1287-1312, 2020.

[8] Mina Zaminkar, Fateme Sarkohaki and Reza Fotohi, "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem." International Journal of Communication Systems, Volume 34, Issue 3, pp. 1-24, 2021.

[9] Erol Gelenbe, Piotr Frohlich, Mateusz Nowak and Dimitrios Tzovaras "IoT Network Attack Detection and Mitigation", IEEE, Mediterranean Conference on Embedded Computing (MECO), pp. 1-6 , 2020.

[10] Zahrah A. Almusaylim , NZ Jhanjhi and Abdulaziz Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP." Sensors, Volume 20, Issue 21, pp. 1-25, 2020.


Inbox - goldennetcomputers@g
Consortium for Academic and Re
Consortium for Academic and Re
Scopus preview - Scopus - Sourc
scopus.com/sources.uri
Sources
ISSN
Enter ISSN or ISSNs
Find sources
ISSN: 2277-3878
Improved Citescore
We have updated the CiteScore methodology to ensure a more robust, stable and comprehensive metric which provides an indication of research impact, earlier. The updated methodology will be applied to the calculation of CiteScore, as well as retroactively for all previous CiteScore years (ie. 2018, 2017, 2016...). The previous CiteScore values have been removed and are no longer available.
View CiteScore methodology. >
Filter refine list
Apply
Clear filters
Display options
Display only Open Access journals
Counts for 4-year timeframe
No minimum selected
Minimum citations
Minimum documents
Citescore highest quartile
Show only titles in top 10 percent
1st quartile
1 result
Download Scopus Source List
Learn more about Scopus Source List
All
Export to Excel
Save to source list
View metrics for year:
2020
Source title
CiteScore
Highest percentile
Citations 2017-20
Documents 2017-20
% Cited
1
International Journal of Recent Technology and Engineering
N/A
N/A
N/A
N/A
N/A
Top of page
EN
11:23 AM
5/3/2022

International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Hybrid Method for Smart Irrigation System

A. Arul Anitha, A. Stephen, L. Arockiam

Abstract*: Internet of Things (IoT) is a boon to the technological developments during the past decade. Though the adoption of this technology in agriculture has gone up immensely in recent years, the implementation of the smart irrigation system remains its initial stage in this agricultural setup. The sprinkler or dripper irrigation methods are widely used in the smart irrigation environment. In this paper a hybrid method is proposed to select the irrigation method automatically based on the climate changes and soil moisture level. By enhancing this method using the rapid growing technologies and IoT enabled smart irrigation controllers, the agriculture sector will be improved over the foreseeable future.

Keywords*: Smart Irrigation, Sprinkler, Dripper, Hybrid Method.

I. INTRODUCTION

Agriculture plays a vital role in countries like India. As Mahatma Gandhi said, the development of our country depends on the economic status of the villages which are mainly depending upon agriculture. Water is the core element for agriculture [1]. Figure 1 explains the need of water resource for agriculture. In India 80% of water resource is used for agriculture. Nowadays, climate changes reflect in the time and duration of monsoons which are the main water source.

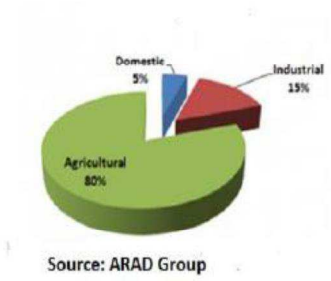


Figure 1: Water usage in India

To overcome this water scarcity issue, the smart irrigation system is deployed in agriculture field. The smart irrigation system monitors the weather, soil type and its moisture level, evaporation and water usage of the plants and automatically adjusts the watering schedule [2]. It helps the farmers to optimize the water usage, enrich the quality of crop growth and quantity of yields in their fields. Smart irrigation systems are easy to implement and it has a straight forward approach [3]. In this paper, the background study related to smart irrigation, the issues and challenges in implementing the smart irrigation and IoT-based smart irrigation methods are discussed. A hybrid irrigation framework is proposed and some research issues in the smart irrigation systems are also highlighted

II. RELATED WORKS

Yuthika et. al [4] proposed an Intelligent IoT based irrigation system. For analysing and predicting KNN (K-Nearest Neighbour) classification machine learning algorithm was used in this approach. Machine to Machine (M2M) technology was implemented for communication among the devices and a prototype model was developed to test the efficiency. The security and water source issues were ignored in their work. Alauddin et al [5] proposed a Cloud based IoT for Smart Garden Watering System using Arduino Uno which was used to monitor and to maintain the soil moisture and light intensity. The monitored data was sent to ThingSpeak IoT cloud. The data gathered in the cloud was analysed and when it reached the threshold value, an action was sent accordingly from the cloud to the irrigation system. It needs further refinement like including temperature sensor and controlling the system using smart phone. Harishankar et al [6] suggested an automatic sprinkler irrigation system using solar power for automating the irrigation process using solar power and to optimize the use of water. When implemented for bore holes, the system was found to be successful. Solar pumps also offered clean solutions with no danger of borehole contamination. Maroufpoor et al [7] recommended three artificial intelligence methods such as Artificial Neural Network (ANN), Adaptive Neuro-fuzzy Inference Systems (ANFIS) and Gene Expression Programming (GEP) for estimating wind drift and evaporation losses from sprinkler irrigation systems. According to the authors, Gene Expression Programming method provided the best result. Fabrizio et al [8] explained a machine learning technique to manage heterogeneous datasets which include physical, biological and sensory values collected from real-time agricultural sector. Weather, humidity, wind speed and soil types were the factors considered in their approach. The supervised machine learning algorithms such as decision tree, K-nearest neighbours, Neural Network and polynomial predictive models were used in this research. According to the authors, effective implementation of their work will increase productivity and will save the environmental resources and will pursue economic profits.

Revised Manuscript Received on September 25, 2019.

A. Arul Anitha*, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli 620002, India. Email: arulanita@gmail.com.

A. Stephen*, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli 620002, Tamilnadu India. Email: stephena003@gmail.com.

Dr. L. Arockiam*, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli 620002, Tamilnadu, India. Email: larockiam@yahoo.co.in

III. ISSUES AND CHALLENGES

To adopt and implement the technologies in agricultural sector, the developing countries like India have to face many issues and challenges.

- Lack of knowledge and fear of implementing and upgrading the technology in higher levels among large number of farmers in the country.
- The solution must have the customization facilities for different languages, so that it could be easy to understand for the ordinary people.
- Interoperability is another issue, due to lot of platforms and vendors for IoT tools and techniques.
- The farms own by the farmers are varying in its size. Hence, the solution related to smart irrigation should be scalable and flexible.
- Security is another big issue. If one of the sensors is hacked it will collapse the entire system. The security tools have to be updated frequently and it leads to additional headache to the poor farmers.

To find out a solution having all these requirement is not easy. These challenges and issues lead to further research and developments in the smart irrigation field.

IV. IoT BASED IRRIGATION METHODS

IoT based smart irrigation system is capable of automating the irrigation process by analyzing the moisture of soil and the climate condition. When the power supply is given to the microcontroller, it will check the soil moisture content [9]. If the moisture content is not up to the threshold then it makes the motor to get on automatically and turns off automatically if it reaches to the threshold level. The need of water for any crop is also reduced drastically. Remote monitoring is also possible in IoT based smart irrigation system.

A. Smart Irrigation System Requirements:

The core components for deploying the smart irrigation system are: Node MCU, Soil moisture sensor, temperature sensor, humidity sensor, 5v Relay, Sprinkler, Dripper, Solenoid valve and Water tank [10]. There are two types of irrigation methods such as dripper and sprinkler can be used according to the season. Dripper irrigation method can be used in the windy season, whereas sprinkler irrigation method can be adopted in the summer season.

B. Sprinkler Irrigation System:

Sprinkler irrigation system allows application of water under high pressure with the help of a pump. Small diameter nozzle is placed in the pipes, it releases rainfall like water through the distributed system of pipes and sprays into air and irrigates [11]. Thus, it is not suitable for the windy season. Figure 4.1 depicts the sprinkler irrigation system with solenoid valve and other required components

In summer, the leaves of the plants easily wither; since this sprinkler irrigation method sprays water like rainfall, it is suitable for the summer season

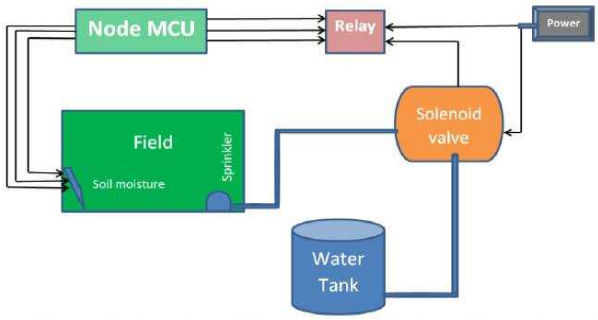


Figure 4.1 Design of Sprinkler Irrigation Method

C. Dripper Irrigation System:

Drip irrigation systems distribute water through a network of valves, pipes, tubing and emitters. Depending on how well designed, installed, maintained, and operated it is, a drip irrigation system can be more efficient than sprinkler irrigation. This system with dripper component is explained in figure 4.2.

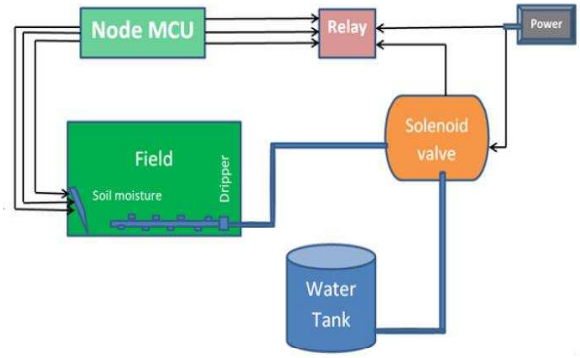


Figure 4.2 Design of Dripper Irrigation Method

This method is useful for all seasons, but sprinkler outperforms this drip system during summer season. There is a need for a better irrigation method which adapts all weather.

V. PROPOSED HYBRID METHOD FOR SMART IRRIGATION

In some situation both sprinkler and dripper irrigation methods can be used when the crop is needed to spray water on leaves of the crop as well as to be fed water to the root of the crop. According to the weather and climate condition either sprinkler or dripper method can be adopted. It is called hybrid irrigation method. This system can be controlled from anywhere through the User Interfaces such as mobile phone or laptop. The sensor data sent by different sensors are stored into the Cloud like ThingSpeak through the border router. The working environment with the combination of sprinkler and dripper is shown in the figure 5.1 and the various functionalities of the smart hybrid irrigation system framework are explained below:

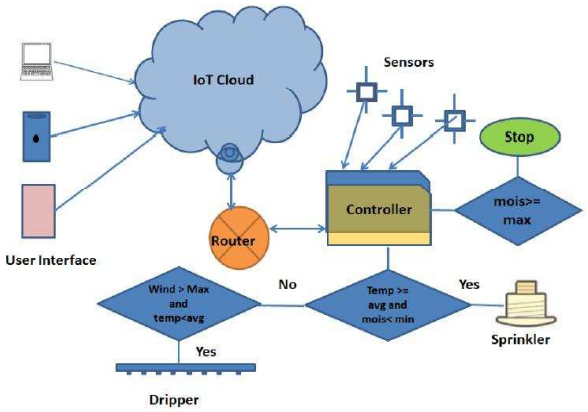


Figure 5.1. Hybrid Smart Irrigation Framework

Step1: The soil moisture sensor and weather sensors will give the details of moisture level of the soil, temperature, rainfall, wind speed and humidity information to node MCU (Microcontroller) whether water is needed to the crop or not.

Step 2: If watering is needed, the Microcontroller will trigger the relay to be switched on the power.

Step 3: Once the relay is switched on then the solenoid valve will be opened which is already connected with water tank and water is poured using sprinkler/dripper to the crop. If the temperature is high and the soil moisture level is very low then the sprinkler system is enabled to water the plants. If the wind speed is very high and also the moisture level of the soil is below the average level then the drip irrigation method is triggered.

Step 4: After irrigation process, the information will be sent to the microcontroller and the relay will be triggered to switch off the power.

Step 5: If water is not needed the irrigation system remains idle.

Mobility of the system helps the farmers to monitor the irrigation process from anywhere. Thus, by using this hybrid smart irrigation strategy, protection of the crops against various climate conditions is very easy.

VI. CONCLUSION

The Smart hybrid irrigation system is recommended to provide a valuable tool for conserving water planning and irrigation scheduling. The dripper or sprinkler method is selected automatically according to the moisture level of the soil, surrounding temperature and climate condition. This system can be used in large agricultural area where human effort needs to be minimized and the farmers can monitor and control the irrigation process from anywhere. Many aspects of the system can be customized and fine-tuned according to the requirement of a particular plant.

REFERENCES

1. K K Namala, Krishna Kanth Prabhu A V, Anushree Math, Ashwini Kumari, Supraja Kulkarni, "Smart Irrigation with Embedded Systems", IEEE Bombay Section Symposium (IBSS), 2016.
2. N. Đuzić and D. Đumić, "Automatic Plant Watering System and its Applications", Coll. Antropol. 41 (2017).
3. L. Selvam and Dr. P. Kavitha, "Smart Agriculture Monitoring System Based On Internet Of Things (IoT)", Vol. 9, issue 6, 2017, pp. 1416-1426.
4. Yuthika Shekhar, Ekta Dagur and Sourabh Mishra, "Intelligent IoT Based Automated Irrigation System", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 12, Number 18, 2017, pp. 7306-7320.
5. Alauddin Al-Omary , Haider M. AlSabbagh , Hussain Al-Rizzo, "Cloud based IoT for Smart Garden Watering System using Arduino Uno", Smart Cities Symposium 2018 (SCS'18), University of Bahrain", April 2018.
6. S. Harishankar, R. Sathish Kumar, Sudharsan K.P, U. Vignesh and T.Viveknath, "Solar Powered Smart Irrigation System", Advance in Electronic and Electric Engineering, ISSN 2231-1297, Volume 4, Number 4 (2014), pp. 341-346
7. E. Maroufpoor, H.Sanikhani, S. Emamgholizadeh and Ö. Kisi, "Estimation of wind drift and evaporation losses from Sprinkler Irrigation Systems by different Data-driven method", Irrigation and Drainage 2017, DOI: 10.1002/ird.2182.
8. Fabrizio Balducci, Donato Impedovo and Giuseppe Pirlo, "Machine learning applications on agricultural datasets for smart farm enhancement", Machines 2018, 6, 38 (Scopus), Doi:10.3390/machines6030038.
9. Aman Bafna, Anish Jain, Nisarg Shah and Rishab Parekh, "IoT Based Irrigation Using Arduino And Android On The Basis Of Weather Prediction", International Research Journal of Engineering and Technology (IRJET), Volume 05 Issue 05, 2018, pp. 433-437.
10. Meraj Ahmed, Md Kamre Alam and Imaad shafi, "A Nobel Report on Smart Irrigation System using IoT", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 11, Nov 2018, e-ISSN: 2395-0056, p-ISSN: 2395-0072.
11. M. Rakibuzzaman, Sk. Rahul, M.R. Jahan, F.B.R. Urme and AFM Jamal Uddin, "Performance of Drip Irrigation System over Conventional Irrigation Technique for Tomato Production on Rooftop", International Journal of Business, Social and Scientific Research, ISSN: 2309-7892 (Online), 2519-5530 (Print), Volume: 7, Issue: 1, Page: 40-43, August-November 2018.

AUTHORS PROFILE

A.Arul Anitha is a Full-time Ph.D Research Scholar in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli which is affiliated to Bharathidasan University, Tiruchirappalli, Tamilnadu, India. She received her Master's degree in Computer Applications (MCA) from Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India and Bachelor of Science in Computer Science from Madurai Kamaraj University, Madurai, Tamilnadu, India. Her Research interest is on Network Security, Intrusion Detection Systems, Internet of Things (IoT) and Machine Learning. She has cleared the National Eligibility Test (NET) conducted by the National Testing Agency (NTA) in December, 2018.

A.Stephen is a Full-time Ph.D Research Scholar in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India. He received his Master of Philosophy (MPhil) in Computer Science from St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India. He received his Master degree in Computer Science (MSc) from Loyola College (Autonomous), Chennai, Tamilnadu, India and Bachelor of Science in Computer Science (BSc) from Loyola College, Tiruvannamalai, Tamilnadu, India. His research interests are Internet of Things (IoT) and Cloud Computing.

Dr. L. Arockiam, working as an Associate Professor in the Department of Computer Science and Dean of Computing Sciences at St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 29 years of experience in Teaching and 21 years of experience in Research. He has Published 345 Research Articles in the International / National Journals and Conferences. He has guided more than 38 M. Phil Research Scholars and 29 Ph. D. Research Scholars and at preset he is guiding 6 Ph. D Research Scholars. His research interests are Internet of Things, Cloud Computing, Big Data, Data Mining, Software Measurement, Cognitive Aspects in Programming, Web Service and Mobile Networks.

Google Scholar

Stephen A

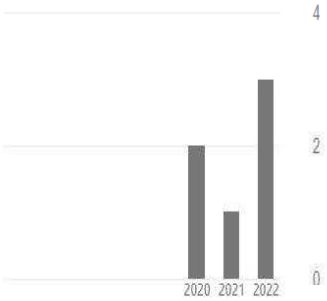
FOLLOWING

Research Scholar
Verified email at mail.sjctni.edu
cloud computing IoT Big Data Data Science

TITLE	CITED BY	YEAR
Attacks against Rplin Iot: A Survey A Stephen, L Arockiam Annals of the Romanian Society for Cell Biology, 9767-9786	4	2021
Enhanced Round Robin Algorithm for Cloud Computing HSBJRD Stephen A International Journal of Scientific Research in Computer Science ...	1	2018
A Hybrid Method for Smart Irrigation System AA Anitha, A Stephen, DL Arockiam International Journal of Recent Technology and Engineering (IJRTE), ISSN ...	1	
Level Based Rank Attack Detection Technique (LEACE) A Stephen Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12 (9), 268-272		2021
Location Based Rank Attack Detection Technique (LRADT) DLA A. Stephen		2021

Cited by

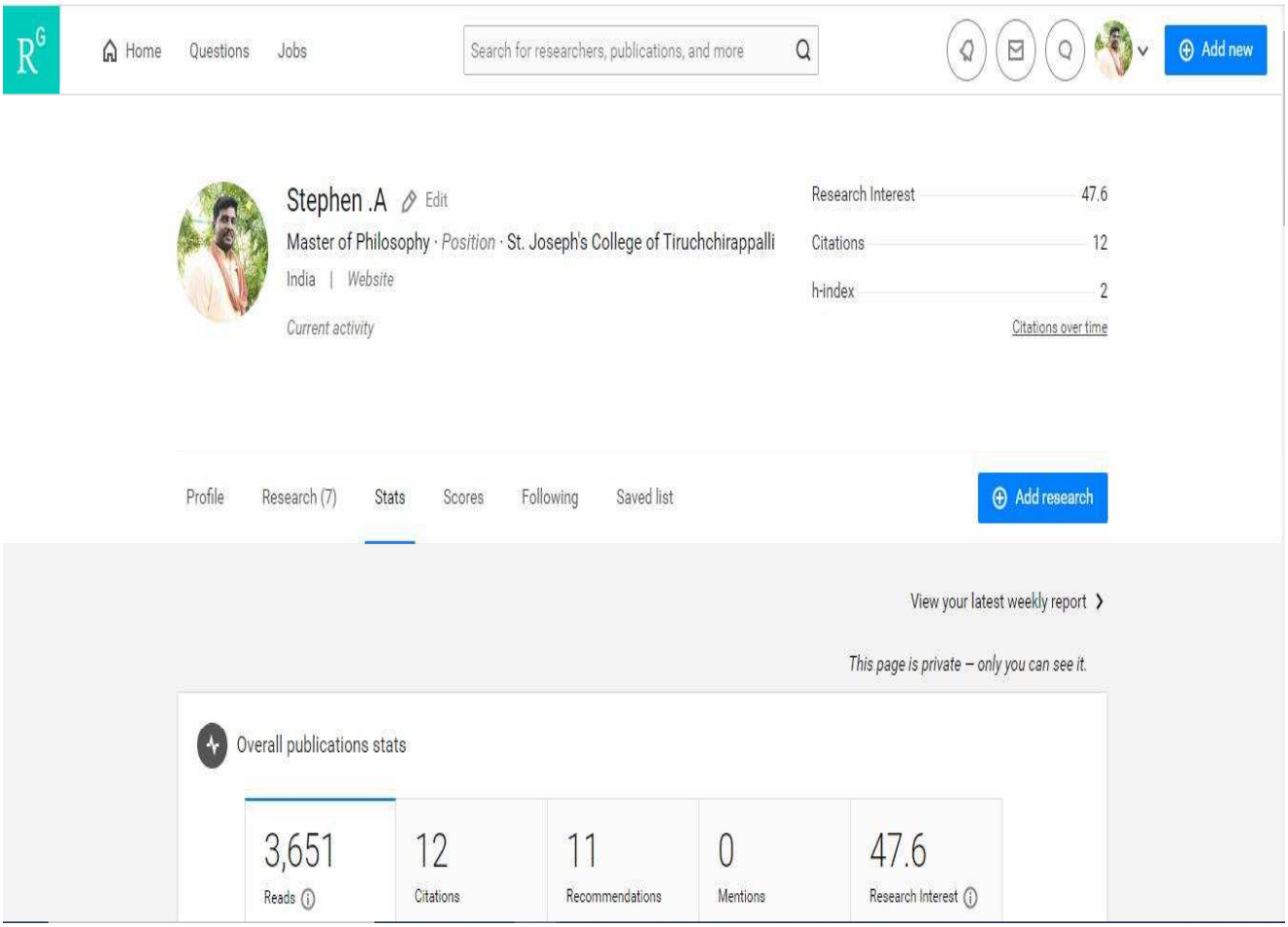
	All	Since 2017
Citations	6	6
h-index	1	1
i10-index	0	0



Co-authors EDIT


Dr. BJ. Hubert Shanthan
Assistant Professor in Comp.Sci...


A. Arul Anitha, MCA, NET, (Ph.D).
Research Scholar, Department o...


Home
Questions
Jobs
Search for researchers, publications, and more
Add new
Stephen .A
Edit
Master of Philosophy · Position · St. Joseph's College of Tiruchchirappalli
India | Website
Current activity
Research Interest 47.6
Citations 12
h-index 2
Citations over time
Profile
Research (7)
Stats
Scores
Following
Saved list
Add research
View your latest weekly report
This page is private – only you can see it.
Overall publications stats
3,651
Reads
12
Citations
11
Recommendations
0
Mentions
47.6
Research Interest