International Journal of Electrical Engineering and Technology (IJEET)
Volume 11, Issue 10, December 2020, pp. 421-430, Article ID: IJEET_11_10_053
Available online at https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10
ISSN Print: 0976-6545 and ISSN Online: 0976-6553
DOI: https://doi.org/10.34218/IJEET.11.10.2020.053

TRUST BASED CLUSTER SELECTION FOR INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

Dr. T. Dheepak
Assistant Professor, Department of Computer Science, Government Arts and Science College, (Affiliated to Bharathidasan University), Perambalur Tamil Nadu, India.

ABSTRACT

A MANET (Mobile Ad hoc Network) is a wireless network which is mobile and is deployed for an immediate or short-term purpose. MANETs operate by sharing information among its neighbors and each node in a MANET takes responsibility for information propagation since central coordination is absent. Hence, each node in a MANET implicitly trusts its neighbors for information sharing. Nodes in a MANET are vulnerable to various security threats which seek to exploit the weaknesses of the network. In this paper, a novel cluster-based traffic analysis is a reactive on-demand method for secured routing. This article explains the method to overcome the traffic in the MANET by using trust-based cluster method.

Key words: Mobile Ad Hoc Network, Traffic Analysis, Clustering, Trust Calculation

Cite this Article: T. Dheepak, Trust Based Cluster Selection for Intrusion Detection in Mobile Ad Hoc Networks, *International Journal of Electrical Engineering and Technology*, 11(10), 2020, pp. 421-430.
https://iaeme.com/Home/issue/IJEET?Volume=11&Issue=10

1. INTRODUCTION

In a MANET, nodes cooperate with each other to share information [1]. A node wanting to send information transmits the information to its neighbor which in turn propagates it to its neighbors until it reaches the required destination. This system places an inherent trust in among the other nodes in the network for information propagation. An attacker can take advantage of this trust relationship among the nodes thereby compromising the network. Also, due to the mobility of the nodes and the dynamically changing network topology, it is hard to determine if a packet is dropped because of the intrinsic network characteristics or the presence of an attacker.

Ad hoc networks operate by establishing an intrinsic trust relationship among its participating nodes. Hence each node in a MANET is able to function as a router. But since the wireless medium is shared and there is a lack of central coordination, ad hoc networks are vulnerable to attacks from other devices within the transmission range. MANETs face vulnerabilities because of shared wireless medium, lack of physical protection for the mobile nodes, and complete trust among nodes because of lack of centralized decision-making entity

[2] [3]. MANETs are susceptible to DoS attacks as they do not have a clear line of defence [4][5]. Ad hoc networks operate by establishing an intrinsic trust relationship among its participating nodes. Hence each node in a MANET is able to function as a router. Each node in a MANET completely trusts its neighbors to carry out network activities such as packet forwarding and packet delivery until each packet reaches the intended destination. Often, attackers try to take advantage of this particular trait present in the nodes in a MANET. Thus, managing trust also becomes an important issue [6][7].

2. RELATED WORKS

Qi, Huamei, et al [8] proposed clustering algorithm takes the residual energy and group mobility into consideration by restricting minimum iteration times. In addition, a distributed fault detection algorithm and cluster head backup mechanism are presented to achieve the periodic and real-time topology maintenance to enhance the robustness of the network.

Sugumar, Rajendran, et al [9] a trust-based authentication scheme for cluster-based VANETs is proposed. The vehicles are clustered, and the trust degree of each node is estimated. The trust degree is a combination of direct trust degree and indirect trust degree.

Oubabas, Sarah, et al [10] proposed a new approach that elects trustworthy cluster head based on hybrid approach combining stability and trust factors. The authors introduced a timer that reduces the control traffic during a clustering process by eliminating the competition of nodes to become the cluster head.

Bala, K, et al [11] proposes a novel system network information-based moderation model to identify and alleviate routing attacks. The proposed system uses time variant snapshots to detect routing attacks. Each node learns network details using the network information theory (NIT) to get the knowledge about the nodes of network, the neighbor locations, energy details, displacement speed from the route discovery packets and reply packets.

Zhang, Wei, et al [12] to solve the problem of quantification and uncertainty of trust, a novel trust management scheme based on Dempster-Shafer evidence theory for malicious node detection has proposed in this paper. Firstly, by taking into account spatiotemporal correlation of the data collected in sensor nodes in adjacent area, the trust degree can be estimated. Secondly, according to the D-S theory, the trust model is established to count the number of interactive behaviors of trust, distrust or uncertainty, further to evaluate the direct trust value and indirect trust value.

3. PROPOSED CLUSTER BASED TRAFFIC ANALYSIS FOR MOBILE AD HOC NETWORK

In this proposed method, a novel cluster-based traffic analysis is an on-demand and reactive method for secured routing. It establishes the system into 1-hop disjoint clusters, whereby each node selects its cluster head (CH), which should be 1-hop neighbors, most trustworthy and qualified node. Cluster members in Cluster-based traffic analysis method forward packet only within the trusted CHs. The following steps are involved in the finding of the traffic and malicious node in the network.

Step 1: Cluster Formation: In this method, the formation of the cluster has done by using Cosine Similarity method. This method usually elect cluster-heads (CH) taking into consideration like Speed of the node, Power of a node, Degree Difference and Sum of distances. Using the above metrics, the weight of individual nodes can be a calculation for electing the CH.

Pn_i = Total battery life of n_i

Cur-Pn_i = Current battery life of n_i

Tn_i = Expected Trust value of n_i (1)

Cur- Tn_i = Current Trust value of n_i

Dn_i = expected 1-hop distance of n_i from the neighboring nodes

Cur-Dn_i = current distance of n_i from the neighboring nodes

Req-IHn_i = Required interaction history of n_i with the interaction nodes

Cur-IHn_i = Current interaction history of n_i with the interaction nodes

Algorithm 1: Cluster Formation Step by Step Procedure

Input: Set of nodes

Output: Set of clusters

Step 1: Begin cluster = 1/* represent cluster number 1*/

Total number of nodes = N

Step 2: For (Number of nodes n_i = 1; number of nodes n_i< N; number of nodes n++)

Step 3: if ((Cur-Pn_i >=Pn_i) (Tn_i >=Cur- Tn_i) (Cur-Dn_i >=Dn_i) (Req-IHn_i >=Cur-IHn_i)

Node n_i cannot be a part of the cluster formation

Step 4: Else Node n_i can be a part of the cluster formation

Step 5: Repeat

Step 6: Repeat

Step 7: Select a node n_i which is 1 hop distance apart from other nodes where

Step 8: Do

Step 9: N = n_i ; d=d1; N=$\bigcup_{n_i \in N, n_i \neq n_j} \{n_j | \ distance\ (n_i, n_j) \leq TRANS\ n_i\}$

Step 10: Draw a circle with n_i as center and d as radius

Step 11: Compute new radius (d1) = d+ $|n_i - n_j|$

Step 12: while $n_i \neq n_j$

Step 13: Cluster – 1 is formed with cooperating nodes lying within the circle;

Step 14: End

Step 2: Node Trust Calculation: In this method, the trust value computation depends on the data that every node can associate with another node. Relevant information about other nodes has associated by examining the forwarded packets, overhead packets and received packets, given that proper reinforcements have utilized at various protocol layers. The trust between the two nodes has represented in a 3-dimensional opinion metrics (Acceptance, Rejection and Doubtful).

$T_j^i = (a_j^i, r_j^i, d_j^i)$ such that $a_j^i + r_j^i + d_j^i = 1$ (1)

T_j^i denotes the node i's opinion about any node i's trustworthiness

a_j^i denotes the acceptance that i holds for j (i.e., the probability that a node j can be trusted by a node i)

r_j^i denotes the rejection that i holds for j (i.e., the probability that a node j cannot be trusted by i).

d_j^i denotes the doubtful that i holds for j (i.e., doubtful fills the void in the absence of both acceptance and rejection).

In the proposed method, a node monitors other nodes' behavior to collect and record all positive (p) and negative (n) events about their trustworthiness. As such, the opinion metrics of T_j^i can be expressed as a function of p and n as follows:

$$a_j^i = \frac{p}{p+n+2}$$

$$r_j^i = \frac{n}{p+n+2}$$

$$d_j^i = \frac{2}{p+n+2}$$

Algorithm 2: Cluster Head Selection Step by Step Procedure

Step 1: $CH_{cur} \leftarrow 0$

Step 2: $CH_{prev} \leftarrow 0$

Step 3: $Time_{prev} \leftarrow 0$

Step 4: now () $\leftarrow 0$

Step 5: Time - $Out_{loop} \leftarrow 3 * COUNTR$

Step 6: The trust value can be further evaluated by the above equation (1)

Step 7: Interaction history (IH) ≥ 0

Step 8: while ($Time_{prev} \leq now$ () or TRUST_VALUE (CH_{prev}) $\leq 1 = true$)

Step 9: do CH_{prev} remains as cluster head

Step 10: end while

Step 11: if TRUST_VALUE (CH_{prev}) = TRUST_VALUE (CH_{cur}) and IH (CH_{prev}) = IH (CH_{cur})

Step 12: then both CH_{cur} and CH_{prev} remain as Cluster Heads

Step 13: Else

Step 14: select new CH

Step 15: end if

Step 3: Local Cluster Formation: If the elected CH is the malicious node, then it threatens the network connectivity. In this proposed method, a node should change its CH when it becomes Malicious node (which can be identified by the above step) to evade the overhead causing by revoking the first step of cluster formation.

Step 4: Handling of Route Request by CH: A CH receives the Route Request from any node in the network, and then it will check for the trust value of the node and compare with the acceptance, rejection and doubtful value. If the rejection value of a node is higher than the given rejection threshold, then the node can be discarded as the Malicious node.

Step 5: Handling of Malicious Nodes: In this method, if any node determines that the next hop in the source route packet be Malicious, then it attempts to attain another trustfulness intermediary nodes to the next jump in the same route by searching its cache or routing table for the route to the destination.

4. RESULT AND DISCUSSION

4.1. Simulation Setup

The proposed Cluster based Traffic Analysis method has been simulated in Network Simulator 2 (NS-2) environment. The total number of nodes considered is 100 nodes, the simulation area is 250m X 250m, each node initial energy is 20000 joules, total time for simulation is 300

seconds, packet size is 512 bytes, each node operating power is 10mW, percentage of malicious node is 10% and 20%.

4.2. Performance Analysis of the Proposed Method with 10% Malicious Nodes

Table 1 represents the number of clusters formed by existing clustering method and proposed cluster-based traffic analysis method at 10% malicious nodes. Figure 1 depicts the graphical representation of the number of cluster formation in the existing method and the proposed method. From the table 1 and figure 1, the proposed method gives the increased number of clusters than the existing method. The increased number of clusters reduces the packet loss and end to end delay.

Table 1 Number of Clusters formed by Existing clustering method and proposed Cluster based Traffic analysis method at 10% malicious nodes

Number of Nodes	Number of Clusters formed	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	8	9
100	11	12
150	18	20
200	21	22
250	22	23
300	26	27

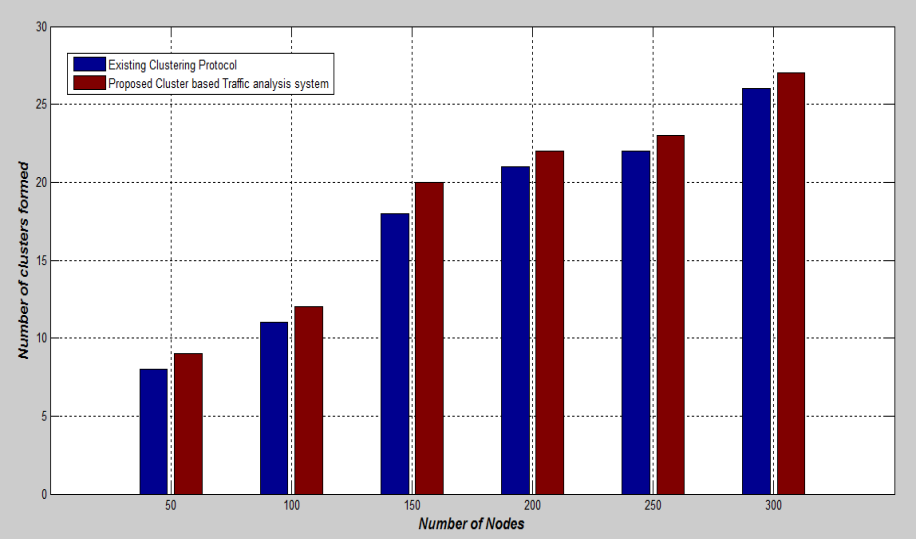

Figure 1 Graphical representation of the number of clusters formed Proposed Cluster based Traffic analysis method and existing clustering method by number of clusters formed at 10 % malicious nodes

Table 2 represents the average packet delivery ratio of the existing clustering method and proposed cluster-based traffic analysis method at 10% malicious nodes. Figure 2 depicts the graphical representation of the average packet delivery ratio in the existing method and the proposed method. From the table 2 and figure 2, the proposed method gives the increased average packet delivery ratio than the existing method.

Table 2 Average Packet Delivery Ratio of the Existing clustering method and proposed Cluster based Traffic analysis method at 10% malicious nodes

Number of Nodes	Average Packet Delivery Ratio	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	0.9221	0.9396
100	0.8782	0.9842
150	0.8725	0.8862
200	0.8219	0.8457
250	0.7579	0.7863
300	0.6601	0.6883

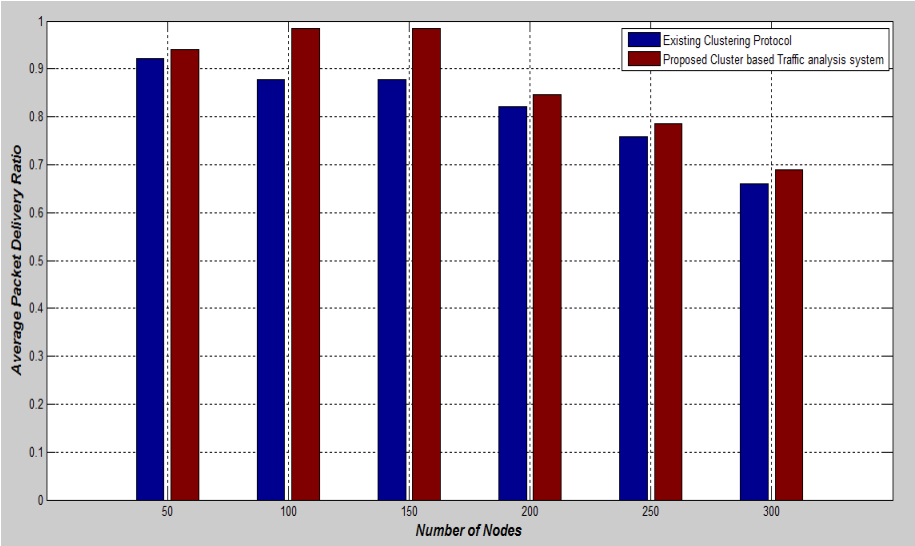

Figure 2 Graphical representation of the average packet delivery ratio of the existing clustering method and proposed Cluster based Traffic analysis method at 10% malicious nodes

Table 3 represents the remaining energy consumption in joules of the existing clustering method and proposed cluster-based traffic analysis method at 10% malicious nodes. Figure 3 depicts the graphical representation of the remaining energy consumption in joules in the existing method and the proposed method. From the table 3 and figure 3, the proposed method gives the increased remaining energy consumption (in joules) than the existing method.

Table 3 Remaining Energy consumption in Joules of the Existing clustering method and proposed Cluster based Traffic analysis method at 10% malicious nodes

Number of Rounds	Remaining Energy Computation in Joules	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
0	0.5	0.5
100	0.41	0.45
200	0.24	0.34
300	0.2	0.29
400	0.18	0.27
500	0.12	0.18
600	0	0.10
700	0	0.8
800	0	0

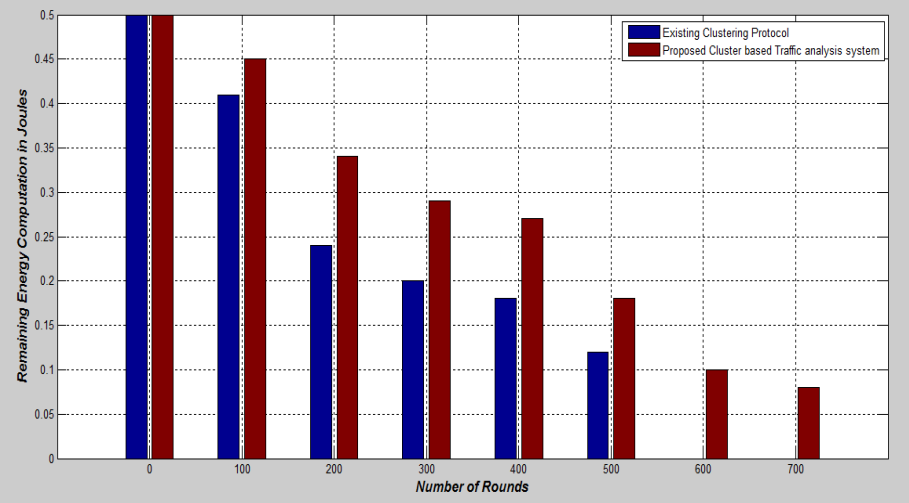

Figure 3 Graphical representation of the remaining energy consumption (in jouls) of the existing clustering method and proposed Cluster based Traffic analysis method at 10% malicious nodes

4.3. Performance Analysis of the Proposed method with 20% Malicious Nodes

Table 4 represents the number of clusters formed by existing clustering method and proposed cluster-based traffic analysis method at 20% malicious nodes. Figure 4 depicts the graphical representation of the number of cluster formation in the existing method and the proposed method. From the table 4 and figure 4, the proposed method gives the increased number of clusters than the existing method. The increased number of clusters reduces the packet loss and end to end delay.

Table 4 Number of Clusters formed by Existing clustering method and proposed Cluster based Traffic analysis method at 20% malicious nodes

Number of Nodes	Number of Clusters formed	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	8	8
100	11	10
150	16	19
200	22	23
250	21	20
300	26	27

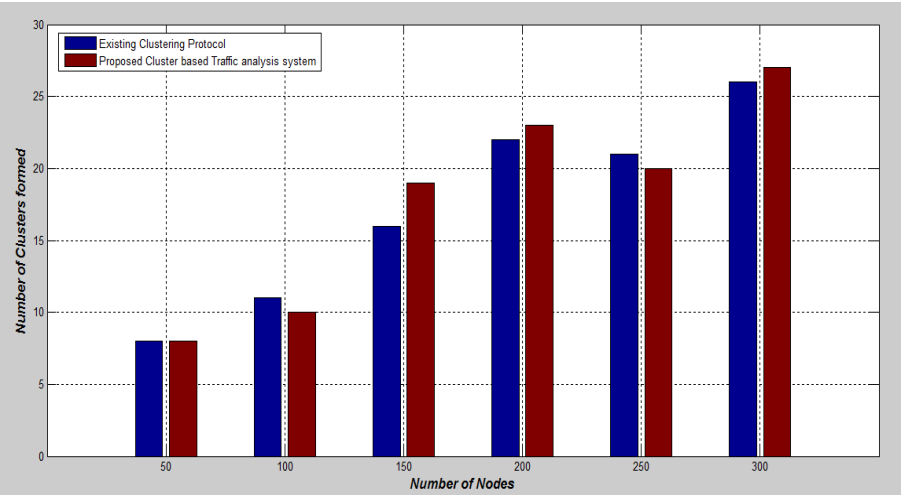

Figure 4 Graphical representation of the number of clusters formed Proposed Cluster based Traffic analysis method and existing clustering method by number of clusters formed at 20 % malicious nodes

Table 5 represents the average packet delivery ratio of the existing clustering method and proposed cluster-based traffic analysis method at 20% malicious nodes. Figure 5 depicts the graphical representation of the average packet delivery ratio in the existing method and the proposed method. From the table 5 and figure 5, the proposed method gives the increased average packet delivery ratio than the existing method.

Table 5 Average Packet Delivery Ratio of the Existing clustering method and proposed Cluster based Traffic analysis method at 20% malicious nodes

Number of Nodes	Average Packet Delivery Ratio	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	0.8427	0.8592
100	0.8165	0.8235
150	0.7858	0.8181
200	0.7406	0.7757
250	0.6776	0.6943
300	0.6113	0.6362

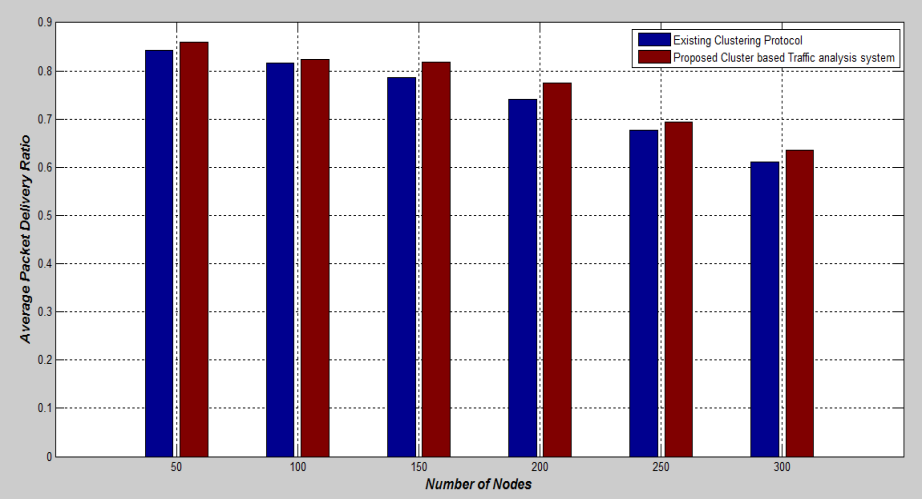

Figure 5 Graphical representation of the average packet delivery ratio of the existing clustering method and proposed Cluster based Traffic analysis method at 20% malicious nodes

Table 6 represents the remaining energy consumption in joules of the existing clustering method and proposed cluster-based traffic analysis method at 20% malicious nodes. Figure 6 depicts the graphical representation of the remaining energy consumption in joules in the existing method and the proposed method. From the table 6 and figure 6, the proposed method gives the increased remaining energy consumption (in joules) than the existing method.

Table 6 Remaining Energy consumption in Joules of the Existing clustering method and proposed Cluster based Traffic analysis method at 20% malicious nodes

Number of Rounds	Remaining Energy Computation in Joules	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
0	0.5	0.5
100	0.35	0.38
200	0.2	0.29
300	0.17	0.24
400	0.15	0.23
500	0.1	0.16
600	0	0.08
700	0	0
800	0	0

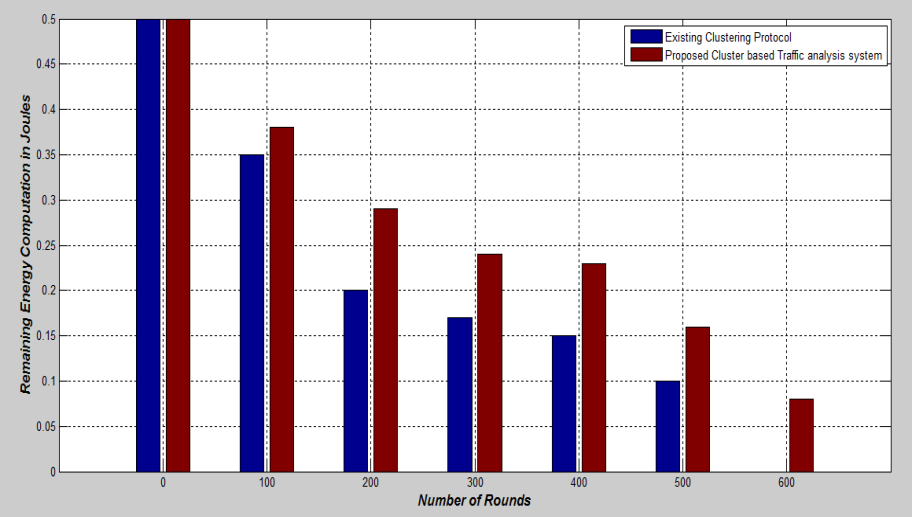

Figure 6 Graphical representation of the remaining energy consumption in Joules of the existing clustering method and proposed Cluster based Traffic analysis method at 20% malicious nodes

5. CONCLUSION

In the research work, a novel cluster-based traffic analysis method has proposed to transmit the packet in the expansive network and the detection of the malicious node. The trust value calculation method has performed in this methodology, to know the trust of the neighboring nodes in the network. The malicious node has discarded from the network. The packet delivery ratio, remaining energy consumption in joules are increased when the number of nodes as well as the number of malicious nodes presented in the network. It increases the life time of the network by this method.

REFERENCES

[1] Usman, Muhammad, et al. "QASEC: A secured data communication scheme for mobile Ad-hoc networks." *Future Generation Computer Systems* (2018).

[2] Sen, Biswaraj, et al. "A Trust-Based Intrusion Detection System for Mitigating Blackhole Attacks in MANET." *Advanced Computational and Communication Paradigms*. Springer, Singapore, 2018. 765-775.

[3] Liu, Gao, Zheng Yan, and Witold Pedrycz. "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey." *Journal of Network and Computer Applications* (2018).

[4] Vanamala, C. K., and G. Raghvendra Rao. "SC-MANET: Threats, Risk and Solution Strategies for Security Concerns in Mobile Ad-Hoc Network." *Computer Science On-line Conference*. Springer, Cham, 2018.

[5] Mehra, Ankush. "To Enhance the Security and Improve the Performance of Aodv Protocol in Manet Using Delay Per Hop Technique." *Global Journal of Computers & Technology* 6.2 (2018): 354-365.

[6] Srinivasan, A., and Shaik Naseera. "Trust and location-based service in mobile social networks–A survey." *Multiagent and Grid Systems* 14.3 (2018): 263-282.

[7] Borkar, Gautam M., and A. R. Mahajan. "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks." *Wireless Networks* 23.8 (2017): 2455-2472.

[8] Qi, Huamei, et al. "A Robust and Energy-Efficient Weighted Clustering Algorithm on Mobile Ad Hoc Sensor Networks." *Algorithms* 11.8 (2018): 116.

[9] Sugumar, Rajendran, Alwar Rengarajan, and Chinnappan Jayakumar. "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)." *Wireless Networks* 24.2 (2018): 373-382.

[10] Oubabas, Sarah, et al. "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme." *Vehicular Communications* 13 (2018): 128-138.

[11] Bala, K., S. Jothi, and A. Chandrasekar. "An enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis." *Cluster Computing* (2018): 1-8.

[12] Zhang, Wei, et al. "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks." *The Journal of Supercomputing* 74.4 (2018): 1779-1801.

[13] Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[14] Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical Engineering and Technology, 11(5), 217-226 (2020).

[15] Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255-1262 (2020).

[16] Subhashini, M., & Gopinath, R., Employee Attrition Prediction in Industry using Machine Learning Techniques, International Journal of Advanced Research in Engineering and Technology, 11(12), 3329-3341 (2020).

[17] Rethinavalli, S., & Gopinath, R., Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology, 11(12), 3348-3356 (2020).

[18] Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).