International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 12, December 2020, pp. 3398-3405, Article ID: IJARET_11_12_320
Available online at https://iaeme.com/Home/issue/IJARET?Volume=11&Issue=12
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: https://doi.org/10.34218/IJARET.11.12.2020.320

TRUST AWARE ENERGY EFFICIENT ROUTING PROTOCOL IN AD HOC NETWORKS

Dr. D. Shanmugasundaram
Department of Computer Science, H.H. The Rajah's College (Affiliated to Bharathidasan University, Tiruchirappalli), Pudukkottai, Tamil Nadu, India

ABSTRACT

A Mobile Ad hoc Network (MANET) is a system which organizes itself in the temporary network topologies which are primarily arbitrary by nature. Since the MANET is a system of wireless nodes, each node moves independently to any direction but with communicative links within the cluster. The wireless network topology shares the information with other nodes, besides which the manner of exchanging the information is rapid and efficient. The mobile Ad hoc network is a particular variety of ad hoc network which can alter its position and configuration itself. MANET is one of the mobile devices which connect various networks. In this research paper, an intelligent dynamic trust model (IDT) for providing security in wireless networks. This model is the combination of dynamic trust and beta reputation trust for secure routing in ad hoc networks.

Key words: Wireless Network, Secure Routing, Dynamic Trust Model, Intelligent Dynamic Trust, Mobile Ad Hoc Network, Routing protocol, Ad Hoc On-Demand Vector, Dynamic State Routing.

Cite this Article: D. Shanmugasundaram, Trust Aware Energy Efficient Routing Protocol in AD HOC Networks, *International Journal of Advanced Research in Engineering and Technology,* 11(12), 2020, pp. 3398-3405.
https://iaeme.com/Home/issue/IJARET?Volume=11&Issue=12

1. INTRODUCTION

MANET is a mobile router self-configuring device connected by wireless connections that consequently combine to form an arbitrary topology. Thus, the wireless topology of the network can change quickly and unpredictably [1]. However, it is difficult to exploit the existing routing methods for network services due to the lack of any fixed infrastructure, and this poses some immense difficulties in providing communication security, which is not achieved seamlessly, as the number of network security specifications clash with the demands of mobile networks, primarily due to the existence of mobile devices, for example.

In MANETs, network nodes are free to randomly switch. The network topology of a MANET can therefore alter quickly and unpredictably[2]. All network operations, such as exploring the topology and delivering data packets, must be conducted either individually or

collectively by the nodes themselves. The structure of a MANET can vary from a small, static network that is highly power-restricted to a large-scale, mobile, highly dynamic network depending on its application. It is a community of autonomous mobile nodes or devices linked without the assistance of a communications system via wireless links. As the nodes transfer and reorganise themselves, the topology of the network dynamically shifts to allow communication with the nodes outside their immediate wireless communications range by relaying messages to each other, i.e. multi-hop [3].

MANET depends on the cooperation of all the nodes involved. The more nodes to pass traffic cooperate, the more efficient a MANET becomes. But it is a cost-intensive operation for a mobile node to support a MANET [14][15][16]. Network bandwidth, local CPU power, memory and resources are consumed by detecting routes and forwarding packets. Therefore, a node is strongly encouraged to refuse packet forwarding to others when using its services to deliver its own data at the same time [17][18][19].

1.1. Characteristic of Mobile Ad Hoc Networks

The following represents the characteristic of the MANET

Dynamic Topology: Hosts are mobile and can, in any arbitrary way, be connected dynamically. Network connections differ and are based on the proximity of one host to another host.

Autonomous: To manage the operation of the various mobile hosts, no centralised administration agency is needed.

Bandwidth Constraint: Wireless connections have a slightly lower capacity than wired connections; they are affected by many sources of error that cause the signal received to be degraded.

Energy Constraint: Mobile hosts rely on battery power, which is a scarce resource; energy conservation may be the most significant device design criterion for optimization.

Limited Security: Since portable devices can be stolen or their traffic can cross unsecured wireless links, mobility means higher security risks than static operations.

2. RELATED WORKS

Zhang, Tong, Lisha Yan, and Yuan Yang [4] The cloud-based confidence assessment approach for clustered wireless sensor networks is proposed and assessed, which implements the conversion between qualitative and quantitative confidence metrics of sensor nodes to achieve better confidence assessment. First, the approach takes several factors into account, including contact factor, message factor, and energy factor, and generates a mathematical model for each confidence factor to get the trust cloud factor. Second, by assigning adjustive weights for each trust cloud factor and combining them, the immediate trust cloud is determined. Thirdly, the trust cloud recommendation and the instant trust cloud are synthesised according to the time-sensitive factor in order to get the final trust cloud. In addition, through trust cloud decision-making, the final trust cloud of sensor nodes is transformed to trust grade.

Li, Jilong, et al [5] proposed a clustering-based routing algorithm considering an interference and load balancing routing metric that focuses on minimizing the existing issues of networks. In this study, we propose a scheme that reduces the end-to-end delay but also gives full consideration to both the quality on the entire route to the destination and to the expected lifetime of nodes with bottlenecks from heaped traffic in IoT.

Gupta, Govind P., and Sonu Jha [6] This paper suggested an improved energy balanced node clustering protocol based on cuckoo search that uses a novel objective function for uniform distribution of cluster heads. In addition, an improved routing protocol based on

harmony search is proposed for routing the data packet between the heads of the cluster and the sink.

Meng, Weizhi, et al [7] in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, the authors focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure.

Gaber, Tarek, et al [8] in the Intelligent Transportation Systems (ITS) clustering would help in addressing the high communication overhead problem. In this paper, we introduce a bio-inspired and trust-based cluster head selection approach for WSN adopted in ITS applications. A trust model is designed and used to compute a trust level for each node and the Bat Optimization Algorithm (BOA) is used to select the cluster heads based on three parameters: residual energy, trust value and the number of neighbors.

3. ROUTING PROTOCOLS IN AD HOC NETWORKS

3.1. Ad Hoc On-Demand Distance Vector (AODV)

AODV is considered as a combination of both DSR and DSDV [12]. This is because AODV borrow the basic mechanism for requesting Route Discovery and Route Maintenance of DSR. In addition, this protocol performs Route Discovery using control messages Route Request (RREQ) and Route Reply (RREP) [13]. When the source node S wants to send data packets to the destination node D but could not find a route in the routing table, the node spreads the message of Route Request (RREQ) to neighboring nodes, including the last known sequence number for the destination. Neighbors and spread the message RREQ to its neighbors if they do not have a good route to the destination node. This process continues until the message RREQ reaches the destination node or an intermediate node that has a good track.

3.2. Dynamic Source Routing (DSR)

The Dynamic Source Routing protocol composes of two main mechanisms to allow the discovery and maintenance of source routes in the ad hoc networks [9]. Source routing does not need to maintain a middle node to update the routing information to route packets as all routing decisions are continuously updated inside the mobile nodes. DSR contains two mechanisms, namely the Route Discovery and Route Maintenance. In route discovery, DSR floods Route Request Packet to the network [10]. Route Discovery is a mechanism whereby node S sends packets to the destination D and have access to the source D. For Route maintenance, DSR provides three successive steps [11]. Route Maintenance is the mechanism whereby the packet forwarding S detect if the network topology has change, the route to the destination D cannot be used because the two nodes that are listed in the route have been out of range of each other. Hence, when Route Maintenance indicates source routing damaged, S notified the route error packet. Sender S can try to use any other route to D for requesting Route Maintenance to seek new password again.

4. TRUST AWARE EFFICIENT ROUTING METHOD

In this work, an intelligent trust model called intelligent dynamic trust (IDT) is proposed for effective secure communication. A widely used way to map the observed information from the evidence space to the trust space is the beta distribution. Let s and f represent the total amount of positive and negative feedbacks in the evidence space about target entity, then the trust worthiness t of a subject node is then computed as,

$$t = s + 1/f + s \qquad \text{Eq. (1)}$$

DyT = Dynamic Trust (t, <t1,t2>)

IDT is the combination of Dynamic Trust (DyT). Intelligent Dynamic Trust model is used for calculating the beta direct trust value using intelligent agents. Here, the intelligent agents are used for monitoring the node trust during particular time duration dynamically. The proposed intelligent system demonstrates the behaviors of each individual node as a binary event. This binary event is modeled by the distribution which is commonly used to represent the posterior probability of a binary event using intelligent agents. Dynamic trust model of each node is evaluated by the features provided by the beta distribution that acts as a basis. The family of probability density functions (PDFs) is a set of continuous function indexed by two parameters α and β. In beta reputation system, α is assigned as the number Np of positive ratings plus 1 and β is assigned as the number Nn of negative ratings plus 1. Initially, dynamic trust is the expectation of positive behavior from a node. In future interactions, the trust worthiness value is calculated as,

$$\frac{\alpha}{\alpha+\beta} \equiv \frac{N_P+1}{N_P+N_n} + DyT \qquad \text{Eq. (2)}$$

P represents the decay factor or forgetting can be applied to assign more weight to new ratings and gradually the older ratings are decreased. Intelligent beta reputation and dynamic trust value is calculated as follows:

$$IDT = \frac{S+1}{F+S+2} + \frac{dS+1}{dF+dS} + DyT \qquad \text{Eq.(3)}$$

IDT is the combination of dynamic trust. The proposed intelligent beta reputation model is used for calculating the trust value dynamically. The proposed work consists of a trust-based secure routing algorithm that works in three phases namely trust score evaluation, threshold setting, and routing based on the trust values. This proposed work focuses on important aspect namely dynamic trust based secure routing. The trust-based secure routing algorithm is the main focus of this work. The steps of the proposed secured routing algorithm are as follow:

Dynamic Trust based Secure Routing Algorithm

Step 1: Let T_v (n_1, n_2…n_m) = 0. // T_v indicate trust value, n_1, n_2, …n_m are nodes.

Step 2: Every node (n_1, n_2…n_m) are considered as source node in different time duration (t_1, t_2).

Step 3: Send messages to the neighbour nodes.

Step 4: HC = HC + 1

Step 5: Start the Scheduler Class to execute the simulation.

Step 6: If it received the request from neighbour nodes then ensure that the node is destination node

Else If it is destination then

It sends the acknowledgement to its neighbouring nodes.

Step 7: Compute the trust score for all the nodes using Eq. 1.

Step 8: Compute the dynamic trust score for all the nodes using Eq. 2.

Step 9: Compute the overall trust score for all the nodes using Eq. 3.

Step 10: If Minimum value (Tkc) < Threshold then

Detect the malicious node

Else

Update the routing table with new node.

Step 11: Perform routing performance

The proposed secure routing algorithm calculates the trust value dynamically. The trust values are calculated during different time intervals for all the participant nodes of the network scenario. The participant nodes ensured the proper destination node by receiving the acknowledgement for their messages. Similarly, the trust score and dynamic trust score have been calculated for the individual nodes using the Eqs. (2) and (3). Threshold values are fixed by the intelligent agents and checked with the dynamic trust scores of all nodes in the network scenario. If the dynamic score of the particular node is less than the threshold value, then the particular node must be considered as malicious node and it is also avoided for performing routing. Finally, the routing process is performed with all other nodes which are having the dynamic scores above the threshold.

5. RESULT AND DISCUSSION

The proposed routing approach is implemented using NS2 by using existing AODV routing protocol. The topology of the wireless network depends on the pause time and mobility speed and also it changes its topology frequently when pause time is less and mobility speed is more. The performance of AODV protocol in presence of malicious node is compared with the performance of proposed technique in this work. Figure 1 describes the trust score variation between the existing and proposed system. From Fig. 1, it can be seen that the proposed system performs well than the existing system. This is due to the use of intelligent reputation mechanism and dynamic trust value calculation.

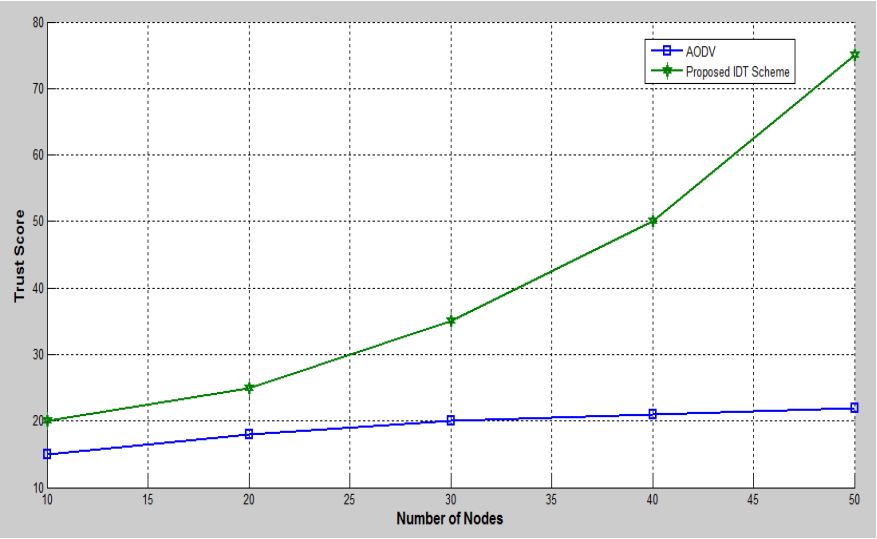

Figure 1 Graphical representation of the Average Trust Score analysis in percentage

Figure 2 shows the delay analysis of the proposed system and the existing AODV protocol. From Fig. 2, it can be observed that the performance of the proposed system is better than the existing protocol in terms of delay. Figure 3 shows the packet drop ratio analysis of the proposed routing algorithm and the existing AODV.

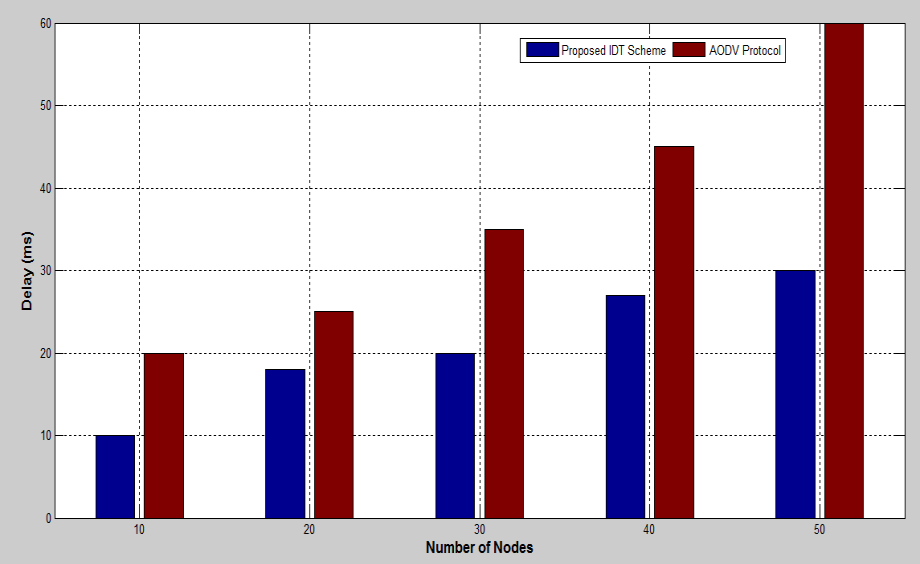

Figure 2 Graphical representation Delay Analysis of Proposed IDT Scheme with existing AODV Routing protocol

From Fig. 3, it can be observed that the packet drop ratio gradually decreases in this proposed IDT when it is compared with AODV with the minimum number of malicious nodes are present in the network. This is due to the use of intelligent agent, dynamic trust and the beta reputation system.

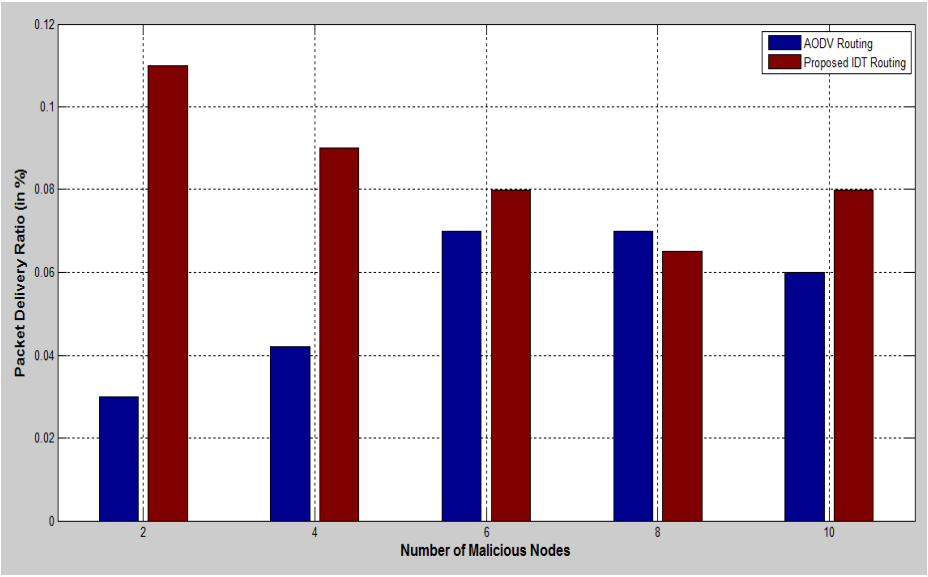

Figure 3 Graphical representation of the Analysis of the Packet Delivery ratio based on Number of malicious node using Proposed IDT scheme and AODV protocol

6. CONCLUSION

An intelligent beta reputation and dynamic trust model is proposed and implemented for effective secure communication. Moreover, an intelligent secure routing algorithm has been proposed, discussed and implemented in this research work. From the experiments conducted using this secure routing algorithm, it has been shown that the trust and reputation calculation and management for secure communication in wireless networks.

REFERENCES

[1] R. Akbani, Korkmaz, T., Raju, G. V. S: Mobile ad hoc network security. In: Lecture Notes in Electrical Engineering, Springer, vol. 127 (2012).

[2] T. Anantvalee and Wu, J.: A survey on intrusion detection in mobile ad hoc networks. In: Wireless/Mobile Security. New York: Springer (2008).

[3] Elhadi, M., Shakshuki, EAACK.: A secure intrusion-detection system for MANETs. In: IEEE Transactions on Industrial Electronics, vol. 60(3) (2013).

[4] Zhang, Tong, Lisha Yan, and Yuan Yang. "Trust evaluation method for clustered wireless sensor networks based on cloud model." *Wireless Networks* 24.3 (2018): 777-797.

[5] Li, Jilong, et al. "A clustering-based routing algorithm in IoT aware Wireless Mesh Networks." *Sustainable cities and society* 40 (2018): 657-666.

[6] Gupta, Govind P., and Sonu Jha. "Integrated clustering and routing protocol for wireless sensor networks using Cuckoo and Harmony Search based metaheuristic techniques." *Engineering Applications of Artificial Intelligence* 68 (2018): 101-109.

[7] Meng, Weizhi, et al. "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data." *Ieee Access* 6 (2018): 7234-7243.

[8] Gaber, Tarek, et al. "Trust-based secure clustering in WSN-based intelligent transportation systems." *Computer Networks*146 (2018): 151-158.

[9] Prasath, N., and J. Sreemathy. "Optimized dynamic source routing protocol for MANETs." *Cluster Computing* 22.5 (2019): 12397-12409.

[10] Guaya-Delgado, Lenin, et al. "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks." *EURASIP Journal on Wireless Communications and Networking* 2019.1 (2019): 77.

[11] Sahu, Prabhat Kumar, and Biswa Mohan Acharya. "Performance Analysis of Unicasting Routing Protocols for Mobile Ad-Hoc Network." *2019 International Conference on Applied Machine Learning (ICAML)*. IEEE, 2019.

[12] Ali, Sara. "An Enhanced Virtual Private Network Authenticated Ad Hoc On-Demand Distance Vector Routing." *International Conference on E-Business and Telecommunications*. Springer, Cham, 2019.

[13] Robinson, Y. Harold, et al. "FD-AOMDV: fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks." *Journal of Ambient Intelligence and Humanized Computing* 10.11 (2019): 4455-4472.

[14] 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).

[15] 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).

[16] 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).

[17] 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).

[18] 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).

[19] 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).