TRUSTWORTHY MANET ROUTING ESTAODV IMPLEMENTATION USING DEEP REINFORCEMENT LEARNING

*Abstract* ***-* Mobile ad hoc networks (MANETs) are a collection of mobile nodes which can move randomly and communicate with each other wirelessly with a dynamic topology. Frequent topological changes are happened in the network because of this dynamic nature. Providing security in Mobile Ad Hoc Network has become a crucial problem due to the unpredictable motions and behaviors of the network nodes. Traditionally routing protocols follow routing operations and they can be affected by the misbehaving nodes. Therefore, a security mechanism is required to distinguish between trustworthy and malicious nodes. Routing has become the most active research area in the MANET field due to these challenges and the significance of the routing protocols.**

**In this article, we have proposed a Trust-based MANET routing model to detect the misbehaving nodes over Ad Hoc On Demand Distance-Vector (AODV) routing protocol. Trust is calculated based on the previous individual experiences and the recommendations of other neighbor nodes. Trust Recommendation Routing Protocol (TRR) which allows nodes to exchange recommendations regarding their neighbors within one-hop is introduced in this proposed model. In order to identify malicious nodes, nodes are categorized into a number of trust levels. After detecting malicious nodes, they will be isolated from the network and broadcasted to the neighbor nodes. Reinforcement Learning (RL) Model is trained to achieve a particular goal through the optimal path. It will assign a positive reward for correct action and negative reward for incorrect action. RL model is used to predict more accurate result without utilizing more historical data of the relevant scenario.**

***Keywords - Mobile Ad hoc Network (MANET), Routing, Ad Hoc On Demand Distance-Vector (AODV), Trust, Malicious, Trust Recommendation Routing (TRR)***

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) performs basic networking functions such as packet forwarding, service discovery and routing. Nodes are depended on each other in forwarding a packet from source to its destination in an ad hoc network. Therefore, every node performs two roles, a host which performs ordinary network operations and a router which forwards packets. Ad hoc networks have the mobility feature. Nodes can be deployed easily and they move randomly as they want, without the support of any centralized structure and irrespective of time, hence due to this self-configuration, self-healing and self-

optimization characteristics, they are also called as self-organized networks (SON) [1]. Because of the dynamic topology in ad hoc networks, nodes can leave or join the network at any time. The topology can be changed randomly at unpredictable moments in the network. Providing security in MANET is a crucial problem because of this dynamic nature and the open shared wireless medium.

Although routing protocols are traditionally designed to cooperate with routing operations, in practice they might be affected by the misbehaving nodes. As a result, they try to disturb the normal routing operations by launching different types of attacks with the intention to minimize or collapse the overall network performance [2]. Nodes are depending on each other for forwarding packets and each node expects cooperation from their neighbor nodes. But providing cooperation can be difficult due to the dynamic behavior of the network. Even though the cooperation is achieved, it is difficult to ensure the well behavior of nodes. The existence of misbehaving nodes might cause the packets to be dropped in an unexpected manner so that the regular transmission process of the network can be interrupted. Therefore, detecting misbehaving nodes guarantees the authentication and the security of routing. Authentication is one of the most important security requirements in MANET and it is defined as “the ability of a node to ensure the identity of the receiver [3]”. Existing cryptographic techniques like public or private key encryption and other security mechanisms such as packet filters, firewalls cannot always identify the trustworthy nodes for the communication purposes. In public/private key encryption, anyone can encrypt a message using the public key of the receiver. Packet filtering or static filtering is a firewall technique which can monitor incoming and outgoing packets. As diverse to all the above-mentioned methods, defining a trust-based schema on top of ad hoc networks to detect each one-hop (directly connected) neighbor nodes will solve this issue up to a considerable level.

Trust is related to the concept of human-based trust which is a connection between the trustor and the trustee. The trustor confides on the trustee. The estimation of the trust is either a quantitative or a subjective measure which is utilized to check whether the trust relationship exists to analyze the trust for various decisions. According to ad hoc networks, the trust could be defined as “the reliability, timeliness, and integrity of message delivery to a node’s intended next hop [4]”. To provide security with limited computational capabilities trust comes into existence because it offers less memory overhead, less transmission overhead and less bandwidth consumption [5]. Trust is basically evaluated on direct trust and indirect trust. Direct trust is the trust which builds based on the experience among directly connected nodes. Indirect trust means the recommendations gathered from the neighbor nodes. Both direct trust and indirect trust depend on the historical interactions among the nodes.

In the proposed trust-based model, we are detecting the misbehaving nodes over Ad Hoc On-Demand Distance Vector (AODV) routing protocol. Here we avoid the misbehaving nodes based on the previous individual experiences of the node (Direct trust) and the recommendations of the neighbor nodes (Indirect trust). The recommendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link outages [2] After calculating the trust, nodes are categorized to several trust levels. By identifying the trust levels of the nodes, a node can easily detect and isolate malicious nodes and avoid relaying packets to malicious neighbors. Also, cooperation can be stimulated by selecting the nodes with higher trust levels. It is important to communicate only with trustworthy neighbors since communicating with misbehaving nodes can compromise the autonomy of ad hoc networks. [2] In the proposed model, nodes interact only with one-hop neighbors. Therefore, no need to keep information about each node in the network. It also ﬁts well to ad hoc networks, which are usually composed of portable devices with power, processing, and memory restrictions. [6]

In this model, Trust Recommendation request Protocol (TRR) is proposed. TRR enables nodes to receive trust recommendations from neighbor nodes. The concept of relationship maturity which improves the efficiency of the trust evaluation is used here. Nodes evaluate the maturity based on the number of interactions occurred among nodes. Penalty phase is carried out for the nodes which are recommending malicious nodes. Their trust value is deducted using a reduction factor. After identifying malicious nodes, the details are broadcasted to neighbor nodes and the malicious nodes will be isolated from the network.

Simulation is performed to assess the viability of the proposed model in ad hoc networks. Performance analysis is done in order to compare the Trust-based routing protocol with the AODV routing protocol. In this paper, we present a detailed description of our proposed trust-based model. Trust Recommendation request Protocol (TRR) is evaluated and analyzed. The paper structure is as follows. Section 2 discuss the related work and section 3 describes the Trust-based routing protocol. In section 4, performance is analyzed using simulation results and section 5 concludes the paper.

1. RELATED WORK

Because of the challenges and the significance of the routing protocols, mobile ad hoc networks have become one of the most active research areas. There has been a number of research papers that have shown keen interest in this field.

S.Sivagurunathan, K.Prathapchandran and A.Thirumavalava have proposed a Trust and Q-learning based Security (TQS) model to detect the misbehaving nodes over Ad Hoc On Demand Distance-Vector (AODV) routing protocol.[1].In this model, nodes are categorized into different trust levels based on the direct trust. Q-learning mechanism has used to avoid malicious nodes by calculating an aggregated reward. “Trust Management in Mobile Ad Hoc Networks Using Scalable Maturity Based Model” [2] article has proposed a human-based model which builds trust relationships between nodes in an ad-hoc network. Trust is evaluated based on the recommendations and individual experience. A protocol called recommendation exchange protocol is used to exchange recommendations among neighbor nodes. Relationship maturity concept is introduced which allows nodes to improve the efficiency of the proposed model for mobile scenarios. [2] “Information theoretic framework of trust modeling and evaluation for ad hoc networks” article has proposed an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. [7] In this paper trust is considered as a measure of uncertainty. They have introduced four Axioms which address the basic understanding of trust and the rules for trust propagation.

In order to increase Quality of Service (QoS) in ad hoc networks, Sridhar Subramanian and Baskaran Ramachandran have proposed a trusted AODV called “ST-AODV”. In ST-AODV protocol a trust value is assigned for each node. Nodes are given permission to participate in routing operations based on the trust values. A threshold value is assigned and if the nodes trust value is greater than this value its marked as a trustworthy node and allowed to participate in routing else the node is marked untrustworthy.[8] “QoS of MANET Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack” paper has proposed a mechanism to evaluate trust values for nodes in the ad hoc networks based upon two criteria, which are their ability to forward data packets and the ability to forward RREQ for a given network node. The trust value is calculated as a multiplication of forwarded data packets ratio and forwarded RREQ packets ratio. The trust value is recorded in the routing table to make routing decisions. [9]

“Different ways to achieve trust in MANET” paper has proposed a cluster-based model to maintain trust relationships dynamically and efficiently in MANET. In this model, the ad-hoc network is divided into clusters. Any two nodes in a cluster calculate trust value between them according to recent transaction records and it is considered as direct trust. [10] In this model router packets are not involved in direct trust calculation and totally depended on the transaction count. “Self-adaptive trust-based ABR protocol for MANETs using Q-learning” [11] article proposed a trust based ABR protocol for MANET using Q-learning mechanism. This protocol focuses on computing a score using Q-learning to weigh the trust of a particular node over associativity-based routing (ABR) protocol. [11] Trust evaluation is based on direct trust, indirect trust and q-learning algorithm. Nodes can adjust their route request forwarding rate according to the calculated trust value. Tao Jiang and J. S. Baras proposed a scheme for the distribution of trust certificates, which is completely distributed and adaptive to mobility. [12] This scheme is based on the swarm intelligence paradigm, which has been used for routing both in wired and wireless networks.

In a mobile ad-hoc network, there are so many attacks. [13] Compromised network nodes and selfish network nodes could cause for ‘internal attacks’. Santhosh J and Malini V K have proposed an Evidence of Behavior Information Exchange (EBoX) scheme as a collaborative approach based on the diffusion of local selfish nodes awareness when a node is compromised by external attackers.[14] “Prevention of black hole attack in AODV routing algorithm of MANET using trust-based computing” article has discussed blackhole attacks and TAODV routing protocol approach is taken to focus on analyzing and improving the security of Blackhole in AODV routing protocol.[13] Furthermore, [15]–[20] research articles have also addressed the blackhole attacks in AODV routing protocol.

1. TRUST BASED MODEL

Over the period of time, nodes want to send packets to a particular destination. According to the trust-based model, initially, all the nodes broadcast the RREQ packets to initiate routes. Afterwards, HELLO packets are sent before transferring packets to identify the alive neighbors so that each node ultimately ensures its one hop neighbor nodes. Only one hop neighbors respond to the hello packets because they are in same communication range. From that, each node can conclude how many nodes are staying as one-hop neighbors.

1. Trust Computation Phase
2. Direct trust Calculation

In AODV the following control packets are used. In route discovery phase, route request (RREQ), route reply (RPLY) packets are used. Route Error (RERR) and HELLO packets are used in route maintenance phase. While evaluating trust, these packets are also considered because they provide a significant contribution towards the routing operations. Though misbehaving nodes can also utilize such packets, the probability of utilization is relatively low compared to well-behaving nodes.

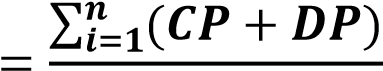
NDF denotes the number of data packets actually forwarded and NDR denotes the number of packets actually received over a period of time with n number of interactions. Likewise, every node could calculate the trust value of all its one-hop neighbors and update its trust table. Each node can monitor its neighboring nodes’ forwarding behavior by using passive acknowledgment.

For the direct trust calculation, Control packets and Data packets are taken periodically for a given time period with the number of interactions happened during that time period.

After calculating the Control Packet (CP) and the Data Packet (DP), Direct Trust (DT) is calculated.

Direct Trust (DT) is calculated using following equations.

Consider two directly connected nodes A and B,

𝑫𝑻AB 

𝟐𝒏

n - number of interactions

Control packet (CP) is calculated by,

CPAB=(RREQAB +RPLYAB + HELLOAB + ERRAB)/4

Data packet (DP) is calculated by,

DPAB = NDFAB / NDRAB

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Neighbor node | Direct Trust  (DT) | Indirect Trust  (IDT) | Global Trust  (GT) | Interactions  (In) | Blacklist  (BL) |
|  |  |  |  |  |  |

Table 3.1: Trust Table

1. Indirect trust Calculation

Indirect trust (IDT) is calculated based on the recommendations given by the neighbor nodes. Trust Recommendation request Protocol (TRR) is used to get the recommendations from the neighbors. After sending the TRR, the node takes replies for a period of 15 seconds. The trust recommendations which are being received during that time are considered as valid replies. The concept of maturity level (ML) is considered similar to the human-related maturity where we give priority to a node which is having a long-term relationship or a higher number of interactions with the evaluating node. Based on this maturity level of each node, a weight factor (W) is calculated to weight the recommendation trust values given by the neighbors.

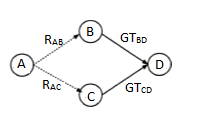


Figure 3.1: Sample Network Diagram with 4 nodes

In Figure 3.1., four nodes are defined as ‘A’, ‘B’, ‘C’ and ‘D’.

When calculating indirect trust (*IDTAD*) between node ‘A’ and node ‘D’, node ‘A’ is taking recommendations for node ‘D’ from node ‘B’ and node ‘C’.

IDTAD = WB [R’AB \* GTBD] + WC [R’AC \* GTCD]

*GTBD*   -  Global trust value between B and D

*GTCD*   -  Global trust value between C and D

Maturity levels for node ‘B’ and ‘C’ is calculated using number of interactions happened between two nodes (In),

MLB = InB  / (InB + InC)

MLC = InC  / (InB + InC)

RA Bdenotes the recommend trust value of node ‘D’ which is given by node ‘B’ to node ‘A’. RAC denotes the recommend trust value of ‘D’ which is given by node ‘C’ to node ‘A’. RAB is equivalent to DTBD which is Direct Trust between nodes ‘B’ and ‘D’ and RAC is equivalent to DTCD which is Direct Trust between nodes ‘C’ and ‘D’. New Recommendation values (R’AB and R’AC ) are calculated using the maturity level and the actual recommended value.

R’AB = MLB\*RAB

R’AC = MLC\*RAC

Weight factors for node ‘B’(WB) and node ‘C’ (WC) is calculated by,

WB = R’AB / R’AB+R’AC

WC = R’AC / R’AB+R’AC

1. Calculate Global Trust

Global trust value (GT) is the summation of Direct Trust (DT) and Indirect trust (IDT).

GT = DT + IDT

Procedure:

1. Get trust table entries as node\_entry\_list
2. for every node in node\_entry\_list do
3. calculate indirect trust value for node
4. update the indirect trust value in the trust table
5. update Global Trust for the node
6. end for
7. Function calculateIndirectTrust
8. consider the node
9. get trust table entries for the given node
10. for each nei\_node in node\_entry\_list do
11. calculate weight for a given node
12. calculate final recommendation trust for a given node
13. get Direct Trust and Global Trust for a given source to destination node
14. Calculate weight term and get the summation of weight
15. end for
16. Return summation of weight
17. End function
18. Function calculating maturity level for a given node
19. get number of interactions for the given node
20. get trust table entries for the given node
21. for each nei\_node in node\_entry\_list do
22. get number of interactions for each node
23. end for
24. calculate maturity level
25. End Function
26. Function calculating final recommendation trust for a given node
27. calculate maturity level for a given node
28. get Direct Trust and Global Trust for a given source to destination node
29. final recommendation trust = maturity level \* DT
30. Return final recommendation trust
31. End function
32. Function calculate weight for a given node
33. calculate new recommendation trust for a given node
34. get trust table entries for the given node
35. for each node in node\_entry\_list do
36. Calculate new recommendation trust for a given node
37. Get the summation of new recommendation trust
38. end for
39. Return the ratio of new recommendation trust from the summation of new recommendation trust
40. End Function
41. Function get DT and GT for a given source to destination node
42. send TRR to the neighbor node and get DT and GT for the destination node
43. End function
44. get trust table entries
45. for each node in node\_entry\_list do
46. calculate indirect trust value for node
47. update the indirect trust value in the trust table
48. Update Global Trust
49. end for
50. End

1. Define Trust Levels

Based on the calculated global trust value, five trust levels are defined. Need to identify the trust levels of the neighbor nodes to make correct routing decision. According to the trust value, five trust levels are listed down in below table (Table 3.2). Threshold value is considered when dividing the trust levels.

|  |  |  |
| --- | --- | --- |
| Trust Level | Threshold | Type |
| 1 | >= TH1 | Trustworthy node |
| 2 | < TH1 and >= TH2 | Partially Trusted node |
| 3 | < TH2 and >= TH3 | Selfish node |
| 4 | < TH3 and >= TH4 | Pure Malicious node |
| 5 | < TH4 | Collaborative Malicious node |

Table 3.2: Threshold Table

* Trustworthy nodes - Trustworthy nodes are participated in normal routing operation and data processing (actual data forwarding and receiving).
* Partially Trusted nodes - Partially Trusted nodes are allowed in normal routing operation and data processing as same as the trustworthy nodes.
* Selfish nodes – Selfish nodes can be identified by their selfish behavior. Unless forwarding of a packet benefits the node, it drops the packet without forwarding. Although these nodes are allowed to take part in the normal routing operations, the nodes will not be involved in actual data processing.
* Pure malicious nodes - Pure malicious nodes only drop packets and once discovered, they are blacklisted and isolated from the network. Then they are deleted from all the trust tables, recommendation tables and backup tables to ensure that that, such nodes will not participate in route discovery process.
* Collaborative malicious nodes - Collaborative malicious nodes collaborate with other nodes to bring harm to bring harm to the network. Same as pure malicious nodes, these are blacklisted. Additionally, the node is broadcasted to other neighbors indicating that it has been detected as a collaborative malicious node.

Structure of the recommendation table and backup table are as follows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Neighbor node | Recommending nodes | Reputation Value/  Maturity level | Blacklist | Recommendation value |
|  |  |  |  |  |

Table 3.3: Recommendation Table

|  |  |  |  |
| --- | --- | --- | --- |
| Neighbor node | Trust Value | Time duration/ Backup time | Analyzed results |
|  |  |  |  |

Table 3.4: Backup Table

Spiral model is used to distinguish if a malicious node is pure malicious or collaborative malicious. Each node can execute the spiral model. Once detected, trust values of all malicious nodes are reduced by calculating a penalty. In addition, if a particular node happens to be identified as a collaborative malicious, it is blacklisted. Since collaborative malicious nodes are hard to detect, only blacklisting is done at first, without also removing the node from tables. When receiving trust recommendation values from other nodes, this blacklist status is checked. If two or more neighbor nodes have blacklisted a particular node, it is confirmed that the node is indeed collaborative malicious and removing it from tables is done.

1. Spiral Model

In spiral model mainly, there are three different phases.

1. Collaborative malicious node discovery process

In this phase collaborative malicious nodes are identified by analyzing the dynamic behavior of nodes. Historical records or trust records are used to predict the collaborative malicious behavior. For this purpose, a backup table is maintained where the recent records of the trust table are stored and each entry on the backup table is associated with a timeout. Initially, predetermined range is defined for the trust with high trust value (HT) and low trust value (LT). Backup table records and current trust records can be compared against the time.

The trust values are analyzed for a given time and after getting the analyzed report or plot, outliers are identified within the given range HT – LT. If it contains any outliers or there are any sudden dynamic changes of the trust values, it is suspected as a

collaborative malicious node. Otherwise, it can be a pure malicious node without any dynamic changing behavior. The range can be changed according to the user specification.

1. Penalty Phase

In the penalty phase the trust value of the particular recommending node which has recommended the malicious node, is reduced using the reduction factor. Reduction factor (RF) is calculated based on the direct trust (DT) and the global trust (GT) of the node.

RF = DT / GT

Reduction factor value is reduced from the indirect trust and then the global trust value is recalculated using the new indirect trust value. Afterwards the trust table is updated and the particular neighbor nodes are redirected to the trust level identification phase in order to re-categorize their trust levels.

Procedure:

1: Get highest trust value and lowest trust value for the node for a given time range and marked them as value boundary for outliers

2: Then compare current trust value is in between the range or not.

3: If current trust value is in between the range, it's categorized as a pure malicious node.

4: Then it (the node who execute this) can delete that record from all of its tables and can broadcast message to aware others.

5: So that will terminate the pure malicious identified process.

6: If current trust value is not in between outliers it's categorized as collaborative malicious (CM) node.

7: Then it (the node who execute this) can edit its trust table blackList flag to true.

8: Identify all the neighbors of identified CM node and reduce their trust value since they have given the incorrect recommendations.

9: Broadcast to the other nodes

10: Go to the Identifying\_trust\_levels algorithm again.

1. After transmission phase

In this phase, nodes receive the collaborative node details through the broadcast. First, node has to check its own neighbors to ensure if the collaborative malicious node is a neighbor or not. If the malicious node is indeed a neighbor, the node checks if that neighbor node has already been blacklisted or not. If not, the node is marked as blacklisted and the penalty process is followed for the nodes which have recommended the malicious node. If the malicious node is already blacklisted, that node will be deleted from all the tables. Finally, the malicious node details are broadcasted to the neighbor nodes and eventually the node will be isolated from the network.

Procedure:

1: read the received broadcast message and identify the p\_CM

2: for every element Bi ∈ BlackListed nodes do

3: if Bi equals p\_CM then

4: delete p\_CM in trust table

5: delete p\_CM in recommendation table

6: break

7: end if

8: end for

9: for each neighbour node do

10: if p\_CM found then

11. Mark as blacklist in trust table

12. Mark as blacklist in recommendation table

13. End if

14. End for

15. Send broadcast message about p\_CM

16. For each node which recommended p\_CM do

17. Calculate the reduction factor

18. Update the indirect trust in the trust table

19. End for

20. End

IV. PERFORMANCE ANALYSIS

The main method of evaluating the performance of MANET is the simulation. Performance analysis is implemented in order to compare the Trust-based routing protocol with the AODV routing protocol. The following performance metrics are evaluated.

Performance is measured on the basis of parameters which are described as follows:

* Packet Delivery Ratio - Packet delivery ratio is measured by the number of packets actually received, divided by the number of packets actually sent. PDR is used in most of the transmissions as a constant rate. The packet delivery ratio is taken as a measure of the throughput of the network.

Packet Delivery Ratio = (Number of packets received / Number of packets sent) \* 100%

* End to End delay – End to end delay is measured by the average time taken by a packet to transfer from the source to its destination. Hence it is calculated by the difference between the arrival times and the sending time of the packets, results will be divided by the total number of connections between the source to the destination. This metric is useful to understand the delay caused while discovering the path from the source to the destination.

End to End delay = (Arrival time – Sending time) / Number of interactions

* Packet Dropped Ratio – Packet drop ratio is calculated by the difference between the total number of packets actually sent and the total number of packets actually received during the simulation.

Packet Drop Ratio = (Number of packets sent - Number of packets received/Number of packets sent) \* 100%

Performance analysis is implemented in Network Simulator 3(NS3). **20** nodes are placed for the simulation with random waypoint mobility model.

|  |  |
| --- | --- |
| **System Parameters** | **Values Utilized** |
| Number of Mobile Nodes | 20 |
| Number of malicious nodes | 2, 4, 6, 8, 10 |
| Mobility Model | Random Waypoint Mobility |
| Simulation Duration | 100 Sec |

A. Vary the number of malicious nodes

Since identifying and isolating malicious nodes is the main aim of the simulation, malicious nodes are included in the network to validate the performance. The number of malicious nodes is increased step by step and analyzed the results in AODV routing protocol and Trust-based routing protocol.

1) Packet Delivery Ratio

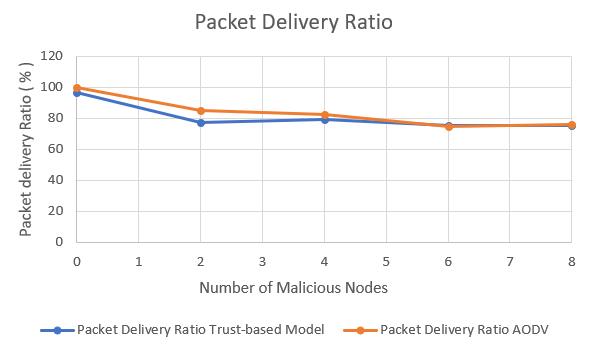


Fig.1. Packet Delivery Ratio

Packet delivery ratio of the Trust-based model is varying with AODV routing protocol.

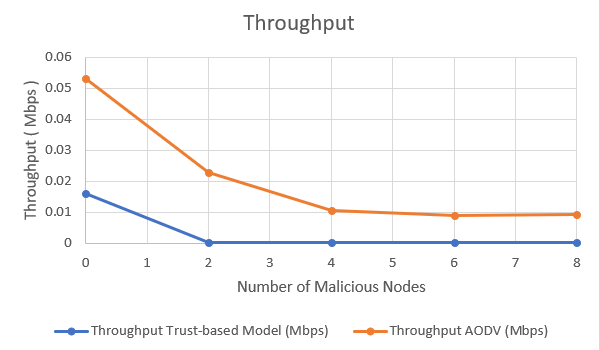


Fig.2. Throughput

2) End to End Delay

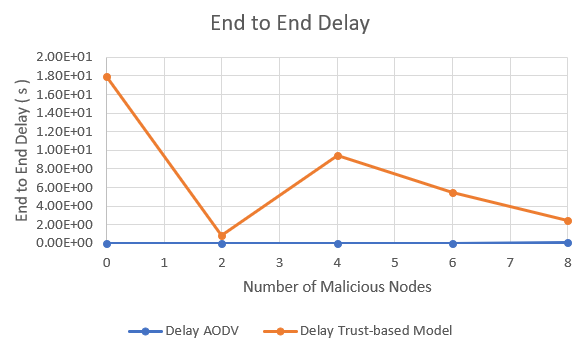


Fig.3. End to End Delay

End to end delay of Trust-based routing protocol is high compared to AODV. But the average latency of both AODV and trust-based model increases when the number of malicious nodes increase. In the trust-based routing protocol, packets are delivered through the most secure route in order to the shortest path which slightly increases the average latency.

3) Packet Drop Ratio

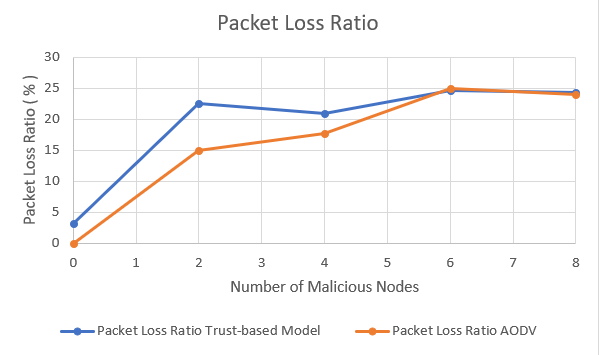


Fig.4.Packet Drop Ratio

Packet dropping ratio of Trust-based routing protocol is relatively low compared with AODV routing protocol. During the simulation, the misbehaving nodes are isolated in the trust-based model so that trust-based routing protocol shows better results over AODV.

B. Malicious node detection accuracy

Results are recorded to analyze the detection accuracy of malicious nodes in the trust-based routing protocol. Pure malicious and collaborative malicious nodes are considered in the ‘Malicious’ category.

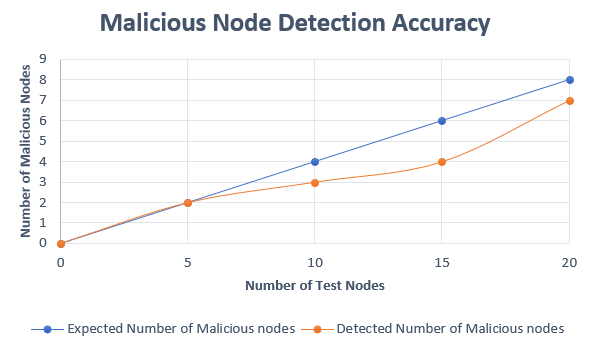


Fig.4.Malicious Node Detection Accuracy

Malicious node detection rate has increased when the number of test node in the network increase.

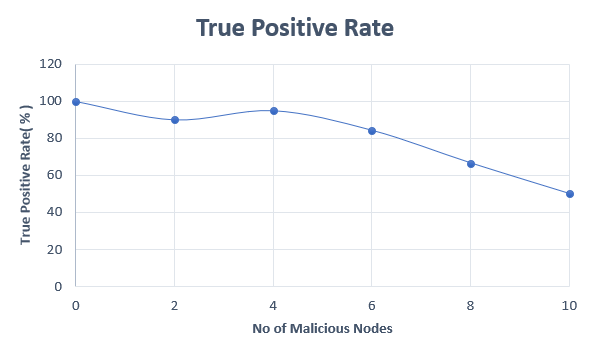


Fig.5.True Positive Rate

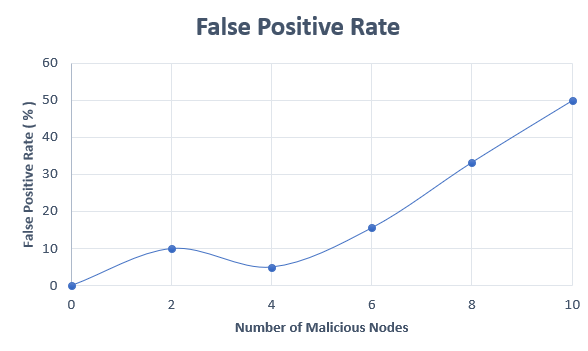


Fig.6.False Positive Rate

Trust-based routing protocol shows the results for identifying malicious nodes with high true positive rate and a low false positive rate.

Above figures ensure that the trust-based routing protocol detects malicious nodes in the MANET with higher accuracy and shows better results than the AODV routing protocol.

V. CONCLUTION

In this paper, we develop a trust-based framework and theory to investigate the dynamic behavior of network nodes and to find the most secured route for packet transmission instead of the shortest path in traditional AODV. Since the first version of traditional AODV had security vulnerabilities which posed serious threats to data packets transmission via MANETs, we have considered different approaches to secure AODV such as considering both direct and indirect trust for nodes and dividing malicious nodes in to two categories; pure malicious and collaborative malicious. A trust recommendation model is introduced to take recommendations from neighbor nodes regarding a particular node as well.

We introduce the concept of relationship maturity based on the interaction count between two nodes and also a trust recommendation model is introduced to take recommendations from neighbor nodes regarding a particular node. Based on direct trust and indirect trust, a global trust value is calculated to evaluate the trustworthiness of nodes and to categorize them in to five trust levels. A performance analysis is implemented to compare the trust-based framework with traditional AODV routing protocol as well. Although this framework is to select the most trustworthy path, one could ideally work to do further research in the above-mentioned domain and come up with a different solution.

REFERENCES

[1] S. S, P. K, and T. A, “Authentication Using Trust to Detect Misbehaving Nodes in Mobile Ad hoc Networks Using Q-Learning,” *Int. J. Netw. Secur. Its Appl.*, vol. 8, no. 3, pp. 47–64, 2016.

[2] P. B. Velloso, R. P. Laufer, D. D. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, “Trust management in mobile Ad Hoc networks using a scalable maturity-based model,” *IEEE Trans. Netw. Serv. Manag.*, vol. 7, no. 3, pp. 172–185, 2010.

[3] W. Stallings, *Cryptography and Network Security: Principles and Practices*. 2005.

[4] Zhaoyu Liu, A. W. Joy, and R. A. Thompson, “A dynamic trust model for mobile ad hoc networks,” in *Proceedings. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004. FTDCS 2004.*, pp. 80–85.

[5] X. Li, F. Zhou, and J. Du, “LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[6] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, “An Efficient Filter-based Addressing Protocol for Autoconfiguration of Mobile Ad Hoc Networks,” in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, 2009, pp. 2464–2472.

[7] Yan Lindsay Sun, Wei Yu, Zhu Han, and K. J. R. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.

[8] S. Subramanian and B. Ramachandran, “QOS Assestion in MANET Routing based on Trusted AODV,” *Int. J. Ad hoc, Sens. Ubiquitous Comput.*, vol. 3, no. 3, pp. 135–143, 2012.

[9] R. K. Bar, J. K. Mandal, and M. M. Singh, “QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack,” *Procedia Technol.*, vol. 10, pp. 530–537, 2013.

[10] R. Dalal, “Different Ways to Achieve Trust in MANET,” *Int. J. AdHoc Netw. Syst.*, vol. 2, no. 2, pp. 53–64, 2012.

[11] A. Vijaya Kumar and A. Jeyapal, “Self-Adaptive Trust Based ABR Protocol for MANETs Using Q-Learning,” *Sci. World J.*, vol. 2014, 2014.

[12] T. Jiang and J. S. Baras, “Ant-based adaptive trust evidence distribution in MANET,” in *24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.*, 2004, pp. 588–593.

[13] A. Sharma, D. Bhuriya, U. Singh, and S. Singh, “Prevention of black hole attack in AODV routing algorithm of MANET using trust based computing,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 4, pp. 5201–5205, 2014.

[14] J. S. S.Uma, “Human Interaction Pattern Mining Using Enhanced Artificial Bee Colony Algorithm S.,” *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 10, pp. 10131–10138, 2015.

[15] Y. Dave, “Er Er,” vol. 1, no. 9, pp. 1–4, 2012.

[16] B. Patel and K. Trivedi, “A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET,” vol. 5, no. 3, pp. 2816–2818, 2014.

[17] T. Farid and A. Prahladachar, “Secure Routing with AODV Protocol for Mobile Ad Hoc Networks.”

[18] R. B. F. Ameza, N. Assam, “Defending AODV Routing Protocol Against the Black Hole Attack,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 8, no. 2, pp. 112–117, 2010.

[19] P. Velloso, R. Laufer, D. De O. Cunha, O. C. Duarte, and G. Pujolle, “Trust management in mobile ad hoc networks using a scalable maturity-based model,” *IEEE Trans. Netw. Serv. Manag.*, vol. 7, no. 3, pp. 172–185, Sep. 2010.

[20] M. Mohanapriya and I. Krishnamurthi, “Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks,” *Arab. J. Sci. Eng.*, vol. 39, no. 3, pp. 1825–1833, Mar. 2014.