International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

A Trust Based Secured Routing Protocol for Mobile Adhoc Network

E. Edwin Lawrence, R. Latha

Abstract: ***Mobile Ad hoc Network (MANET) is a group of wireless mobile nodes that dynamically creates a network without the support of central management. The mobile hosts of MANET network are not restricted to move freely in any direction and thus linking with any other mobile host can be easily done. Without giving any notification to other hosts in the network, they can be switched on or off. Each mobile host must forward traffic, unrelated to its own use and therefore acts as a router. Because of the mobility of wireless nodes, each node must have the capability of managing an autonomous system, or a routing function without requiring any centralized administration. This mobility and autonomy of the wireless nodes along with the transient nature of the end hosts and intermediate host in a communication path creates a dynamic topology of the network. These mobile hosts are connected in an arbitrary manner and as they are highly mobile, the topology changes take place frequently. The rate of change is based on the velocity of the nodes and the challenge is these devices are small and the available transmission power is limited. In this Trust Based Secured Routing Protocol for MANET (TSRPM), certain changes have been made in the design of secure ad hoc routing protocols. First, a modified Diffie Hellman algorithm is implemented; secondly a trust based model has been developed.***

Index Terms: ***Adhoc, Key Exchange, Routing, Secured Transmission.***

I. INTRODUCTION

Early works on ad hoc routing considers only the problem of designing well-organized mechanisms for identifying paths in dynamic networks, without considering security. Meanwhile a number of attacks that manipulates the routing in ad hoc network have emerged. MANET securing protocols faces unique challenges because of their characteristics such as lack of pre deployed infrastructure, centralized policy and control.

Secure ad hoc routing protocols must satisfy the following requirements to make sure that the path discovered from source to destination functions properly even in the presence of malicious nodes.

1. Route signaling can't be spoofed.
2. Injection of fabricated routing messages cannot occur.
3. Routing messages cannot be altered during transmission, except by the functionality of routing protocol.
4. Misbehavior of malicious nodes cannot create routing loops.
5. Redirection of routes from the shortest path by malicious action cannot happen.
6. Unauthorized nodes must be excluded from the path.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
E. Edwin Lawrence*, Research Scholar, Bharathiar University, Coimbatore, India.
Dr. R. Latha, Professor & Head, Dept. of Computer Applications, St. Peter's University, Avadi, Chennai, India

II. RELATED WORK

Dhurandher and Mehra, 2009, suggested a trust based solution to the multipath routing situation. In this method every node in the network is given a zero trust value at the initial stage which indicates unknown trust level. Depending on their behavior, each node is assigned a trust value that can be incremented or decremented. The trust values can be positive, negative or zero for indicating known, malicious, or unknown behavior respectively.

Trivedi et al., 2006, presented an Intrusion Detection System that defines a status assigned to every node in the network. Each node of the network monitors the behavior of its neighbor (next hop) through promiscuous mode. The reports of these nodes are submitted to the reputation manager and it further updates the reputation value. If a node goes beyond a predefined threshold value it is considered as malicious and a alarm message is sent to its neighbor nodes. Each node has a list named avoid list which has a record of malicious nodes and these nodes are avoided for communication.

Mangrulkar and Atique, 2010, presented a method to enhance the AODV protocol by the addition of trust value field in the route request packet. The source node assigns the initial trust value when a RREQ packet is broadcasted. The trust value is incremented for all the nodes of the path if an RREP packet is received. In this method the route with higher trust value is given preference than shortest route thus avoiding the disruption of the network.

Abraham et al., 2004, suggested an Intrusion Detection System that compares the performance of the fuzzy rule based classifiers created by them with similar performance received from the decision tree, support vector mechanisms. Soft Computing based Intrusion Detection System is used to develop IDS that are light weight and more accurate.

Sonja Buchegger et al., 2013, presented CONFIDANT protocol that is used to identify the nodes which are not cooperating. It consists of the following components:

Monitor component: It is responsible for monitoring the passive acknowledgements for each packet that is forwarded by the nodes.

Trust manager component: It is responsible for the sending and receiving of alarm messages. When a node is found to be misbehaving, an alarm message is exchanged between nodes that are already defined as friends.

Alarms from other than friend nodes are treated of less importance.

Reputation system component: This component maintains a table of nodes and their associated ratings. These ratings are modified based on the rate function that uses weightage (smaller weight for a misbehaving node and greater weights for direct observations)

Path manager component: It manages the path information about addition, deletion, and updating of paths depending on the feedback it has received from the reputation system. In case the rating of a path falls under a threshold value, the path is considered to have a malicious node, and path will be removed by the path manager component.

Pengwei and Zhenqiang, 2010, presented a method which focused on security enhancements in AODV protocol. When a data packet is forwarded by a node, a copy of the data packet is created and stored in its buffer. When the node receives another packet and if it is same as the one stored in its buffer, the credit value (which is initially assigned to 1) of the neighboring node is incremented otherwise decremented.

III. METHODOLOGY

The methodology for TSRPM is a combination of modified Diffie-Hellman key exchange algorithm and a trust management mechanism based on Eigenvector centrality.

A. Network Model and Assumptions

In this model, a wireless MANET which consists of an unrestrained number of nodes is considered. All nodes of the network have similar range of communication, and each of these nodes can roam freely within the network or remain static in a place for a period of time. Within its transmission range, a node can communicate with other nodes in the network and these nodes are called its neighbor nodes.

Each node can connect with or quit from the network at any time. These nodes create a peer-to-peer communication through a shared, multihop, bandwidth-constrained wireless channel. For nodes that are outside of one's transmission range, the communication will be through a multi-hop path. It is considered that this network is a group of nodes with every node has at least one neighbor. the communication between two nodes within the wireless transmission range is bidirectional. It is also considered that every node's ongoing communications can be overheard within its wireless transmission range by other nodes.

B. Diffie Hellman Key Exchange Algorithm

The pair wise shared key establishment is designed with a modified Diffie-Hellman (DH) key exchange algorithm which can efficiently avoid replay attacks and also session key disclosure attack. Diffie-Hellman is a mathematics based algorithm which permits two systems to generate an identical shared key on both the systems. The shared key can be used to exchange an encryption key securely. The shared secret is also called Key Encryption Key or KEK which is used to encrypt the symmetric key for secure data transmission. This symmetric key is also called "Data Encryption Key" (DEK).

Diffie- Hellman algorithm has a Certificate Authority (CA) to make sure that the public key is initiating from the source. This accreditation helps to avoid man-in-the middle (MITM) attacks. This attack intercepts public keys and forwards fake public keys to both beneficiaries. The "MITM" attack can intercept encrypted traffic, decrypt it, alter it, re-encrypt it with a fake key, and forward it to its destination.

Diffie Hellman has been applied in various services and is proved efficient. Mostly it is applied in interactive transactions between a sender and receiver. The key exchange algorithm provides better security when the data is encrypted using Secure Socket Layers or Transport Layer Security and in Virtual Private Network.

C. Modified Diffie Hellman Key Exchange Algorithm

A modified Diffie Hellman Key Exchange Algorithm is given below. In this algorithm in addition to prime numbers, a pair of random numbers is also generated to provide a secured environment.

Let P be the prime number and G be the generator of P.

X and Y are the two parties, they both agree upon the parameters P and G.

X thinks of a private number Pr1 and a random number Rn1.

Y thinks of a private number Pr2 and a random number Rn2.

Calculate:

$R1 = (Rn1 + P) \bmod (P + 1)$

$R2 = (Rn2 + P) \bmod (P + 1)$

$P1 = Pr1 + R1$

$P2 = Pr2 + R2$

Compute:

$PU1 = (G \wedge P1) \bmod P$ and

$PU2 = (G \wedge P2) \bmod P$

Now X and Y exchange their intermediate keys PU1 and PU2. The attacker can see only PU1 and PU2, so it will be hard to calculate the private number

Now, X has the intermediate key PU2 and Y has the intermediate key PU1

The common secret key is established as

$S1 = (PU2 \wedge P1) \bmod P$

$S1 = (PU1 \wedge P2) \bmod P$

Finally, X and Y share the common secret key to establish a secure connection

D. Route Discovery

Route discovery is the process of discovering a route from source node to destination node. This can be done by either directly reaching within wireless transmission range or by passing through one or more intermediate hops. The source node broadcasts a Route Request Packet (RREQ) and all other nodes which are present within its transmission range receive the packet. It is transmitted to the first hop discovered in the source route.

When a packet is received by the host and if it is not the destination, then the packet is transmitted to the next hop. In addition to the address of the source and the destination, each route request packet contains the keys generated by the modified Diffie Hellman algorithm.

A RREQ packet has the following fields:

<BroadcastID, SourceAddress, SourceSequenceNo, DestAddress, DestSequenceNo, HopCounter, key>

The RREQ packet originates through the network and finds the destination which is marked as the target to which an optimal route is requested.

After successful identification of route the host receives a route reply packet which contains a list of hops following which the target may be reached. But for returning back to the source node, the RREP packet must discover a route.

E. Eigenvector Centrality

Eigenvector centrality (EC) is a technique that is used to compute the influence of a node in a network. In this technique the total number of adjacent nodes and the influence of this adjacent node are considered. EC is computed by identifying how well an individual node is connected to other parts of the network. A high Eigenvector score refers that a node is connected to many other nodes who themselves have higher scores.

Consider a graph G:=(V,E) where V represents the number of vertices and E represents the number of edges. Let Adj = ($a_{i,j}$) be the adjacency matrix, then

$$a_{i,j} = \begin{cases} 1, \ if \ vertex \ i \ is \ linked \ to \ j \\ 0, \ otherwise \end{cases} \qquad (1)$$

F. Trust Management Mechanism

Every node of the network has a pair of public or private keys generated by the modified Diffie-Hellman algorithm during its deployment. The trust management technique helps in validating the nodes in the network. The trust value (T_{ij}) is calculated with the help of Eigen Vector Reputation Centrality Mechanism.

The Eigen vector centrality (EVC_i) of each node is calculated for finding the reputation on their neighbor. Let n_i and n_j be two adjacent nodes then the centrality for the ith node is proportional to the total score of all nodes connected to it.

$$EVC_i = \frac{1}{\lambda} \sum_{j \in S(i)} EV_j = \frac{1}{\lambda} \sum_{j=1}^{n} Adj_{ij} EV_j \qquad (2)$$

Where Adj_{ij} refers to the adjacency matrix,

S(i) are the group of nodes connected to the ith node,

n refers to the total number of nodes

λ is the constant.

Adj_{ij} is defined using the following condition:

If

ith node is adjacent to the jth node

Then

Adj_{ij} =1 (In EVC_i)

Else

Adj_{ij} =0

End if

The Satisfaction Index (SI) is calculated periodically by each node using

$$SI_{ij} = PI(i,j) - PE(i,j) \qquad (3)$$

Where PI (i, j) is the percentage of packets initiated from n_i and transmitted by n_j. PE (i, j) is the percentage of packets that were expired.

The trust value (T_{ij}) is calculated using the equation

$$T_{ij} = T^*_{ij-pr} + SI^*_{ij} \qquad (4)$$

Where T_{ij} -pr is the trust value of the node j calculated by node i before the inclusion of SI_{ij},

Finally T_{ij} is normalized by analyzing it over time t.

$$T_{ij} = EVC^*_i \frac{T_{ij}}{f(t)_{max}(T_{ij})} \qquad (5)$$

$f(t)_{max}$ refers to the function which is used to calculate the maximum value of T_{ij} in time t. T_{min} is the trust's minimum threshold level. The trust value is calculated based on the Eigen vector centrality score (EVC) and the Satisfaction Index (SI). A regular node must have T_{ij} value greater than the threshold minimum T_{min}.

IV. SUMMARY OF ROUTING ALGORITHM

The algorithm can be summarized as follows.

1. During route discovery process, the source node broadcasts the RREQ packets. These packets contain the regular routing information and their keys which are calculated using the modified Diffie-Hellman algorithm to set up a secured environment. The RREQ also contains the nodes observation on the neighboring nodes (trustworthiness).
2. When a Route request packet (RREQ) is received by the intermediate node, it validates the source, its previous hop gets acknowledged and a pair wise shared key is established between the source node and its previous hop. The RREQ is then forwarded to its next hop. This process is continued till the destination is reached.
3. The destination node after receiving the packet verifies it and retrieves all key information. A pair wise shared key with the source node is then established and the routing decision is not made until the destination receives some of the valid copies of the same message through various routes. The destination node then sends back an RREP packet to the source node through the chosen route.
4. The source node after receiving the RREP packet validates it. The key information is retrieved and a security association is established. The data transmission is initiated on the selected route and the intermediate nodes frequently check the link status and also monitor the neighbor node's behavior.
5. A route error (RERR) message is triggered as soon as a security violation is detected and notified to other nodes of the network. Every other node of the network updates their trustworthiness of the particular erroneous node.
6. If the trustworthiness of a node (calculated using Equation.5) gets below the threshold, the RERR message specifies that the particular node is misbehaving and must be avoided.
7. A new route bypassing the misbehaving node is selected for further transmission. If there is no such route available, then the route discovery process is initiated again.

V. RESULTS AND DISCUSSIONS

Simulations are carried out to analyze the performance of routing protocols after adding security features. Here, Trust Based Secured Routing Protocol for MANET (TSRPM) is compared with Ad hoc On-Demand Distance Vector (AODV) and Trust based Multipath Routing (TMR).
Table 1 shows the NS2 simulation parameters used in this research.

Table 1: NS2 Simulation Parameter

Parameters	Values
Area size	1000 X 1000
Number Of Nodes	100
Radio Range	250m
Mac	802.11
Packet size	512 Bytes/Packet
Traffic source	CBR
No. of attackers	10 -50
Node Pause Times	30s
Source Traffic (Each)	4 Packets/Second
Routing Protocols	TMR and TSRPM

Packet Drop Comparison in the Presence of Malicious Nodes

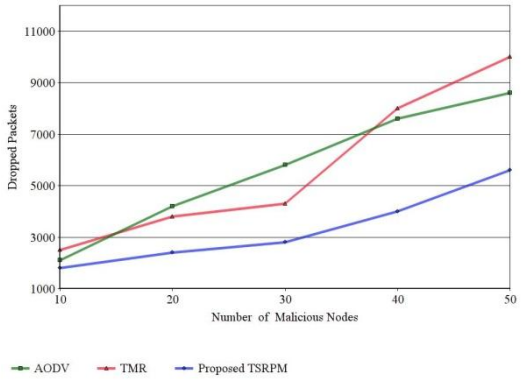

Figure 1: Packet Drop Comparison Graph

Figure 1, shows the number of packets discarded corresponding to the number of malicious nodes. With the increase of malicious nodes, AODV and TMR reflect high packet loss due to high denial by the malicious nodes. The TSRPM method allows the node to restore the trust and manage high packet forwarding and fewer packet dropping. The values attained are tabulated in Table 2

Table 2: Packet Drop Comparison

Number of Malicious Nodes	AODV	TMR	TSRPM
10	2100	2500	1800
20	4200	3800	2400
30	5800	4300	2800
40	7600	8000	4000
50	8600	10000	5600

Control Overhead Comparison in the Presence of Malicious Nodes

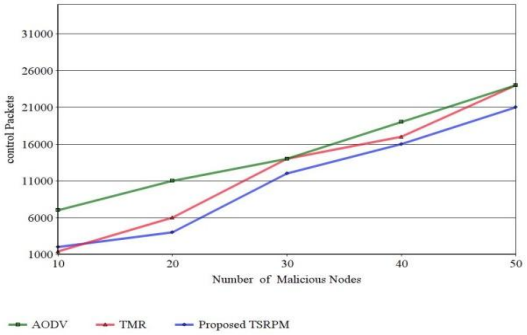

Figure 2: Control Overhead Comparison Graph

Figure 2 shows control overhead comparison of the protocols. All the protocols taken in to consideration have reached a significant level of overhead growth as the number of malicious nodes gets increased. The TMR protocol shows high overhead if there is more number of malicious nodes because of the large number of data packets loss, whereas the TSRPM shows the difference in control overhead because of its reliable node based behavior prediction. The values attained are tabulated in Table 3.

Table 3: Control Overhead Comparison

Number of Malicious Nodes	AODV	TMR	TSRPM
10	7000	1400	2000
20	11000	6000	4000
30	14000	14000	12000
40	19000	17000	16000
50	24000	24000	21000

Packet Delivery Ratio Comparison

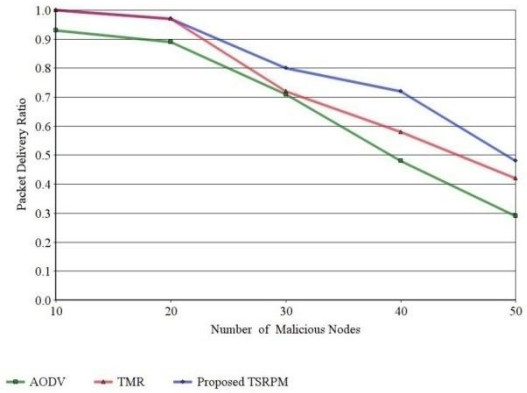

Figure 3: Packet Delivery Comparison Graph

In Figure 3 Packet delivery ratio is analyzed. As the number of malicious nodes increase, packet drop occurs thus affecting the network throughput. In case of packet loss, the existing methods take action on every node present in the network although certain nodes are legitimate. TSRPM instead predicts the behavior of each node and their past collective trust to make a decision, thus helping in retaining the path and improving packet delivery.
The values attained are tabulated in Table 4.

Table 4: Packet Delivery Comparison

Number of Malicious Nodes	AODV	TMR	TSRPM
10	0.93	1	1
20	0.89	0.97	0.97
30	0.71	0.72	0.8
40	0.48	0.58	0.72
50	0.29	0.42	0.48

Latency at Different Speed

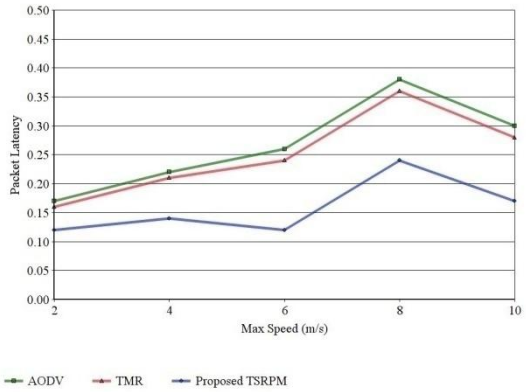

Figure 4: Latency Comparison Graph at Different Speed

Figure 4 depicts the packet latency of TSRPM at various speeds in comparison with AODV and TMR. All of the three protocols take much time to set up routes. However, TSRPM has lower packet latency than others as the performance of packets and reliability of the routes is considered in routing metrics. The values attained are tabulated in Table 5.

Table 5: Latency Comparison at Different Speed

Maximum speed (m/s)	AODV	TMR	TSRPM
2	0.17	0.16	0.12
4	0.22	0.21	0.14
6	0.26	0.24	0.12
8	0.38	0.36	0.24
10	0.3	0.28	0.17

VI. CONCLUSION

Security, reliability, and availability are three essential aspects of ad hoc networks, especially when it comes to security sensitive applications. As MANET's are dependent on wireless medium for communication, it is vital to use a security protocol for protecting the privacy of transmissions. This paper discussed a Trust Based Secured Routing Protocol for MANET (TSRPM) which ensures secured communication in Mobile Ad hoc Networks. The combination of modified Diffie Hellman algorithm and Trust based mechanism makes the protocol more effective and secured against attackers.

REFERENCES

1. Anand, Anjali, Himanshu Aggarwal, and Rinkle Rani. "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks." Journal of Communications and Networks 18.6 (2016): 938-947.
2. Yu, Ming, and Kin K. Leung. "A trustworthiness-based QoS routing protocol for wireless ad hoc networks." IEEE Transactions on wireless Communications 8.4 (2009): 1888-1898
3. Neelakandan, S., and J. Gokul Anand. "Trust based optimal routing in MANET's." 2011 International Conference on Emerging Trends in Electrical and Computer Technology. IEEE, 2011.
4. Sridevi, Kotari, and Mandapati Sridhar. "A Reliable Trustworthy Approach Based on Node Behavior Prediction for Secure Routing in MANET." *International Journal of Intelligent Engineering and Systems, Vol.10, No.6, 2017*
5. John, Saju P., and Philip Samuel. "Self-organized key management with trusted certificate exchange in MANET." Ain Shams Engineering Journal 6.1 (2015): 161-170.
6. Bihari, Anand, and Manoj Kumar Pandia. "Eigenvector centrality and its application in research professionals' relationship network." 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). IEEE, 2015.

AUTHORS PROFILE

Mr. E. Edwin Lawrence is pursuing Ph.D. in the Department of Computer Science, Bharathiar University, Coimbatore, India. His main research focus is on Computer Networks and Swarm Intelligence. He has 9 years of teaching experience.

Dr. R. Latha received her Doctorate Degree in Computer Applications for her research on Parallel and Distributed Simulation from Dr.MGR University. She is having 29 years of teaching and research experience as Faculty, Professor and Head of the Department in various Institutions.