ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Enhanced Trust Based Routing In MANETs

S.Sri Tulasi[1], P.Sree Sudha[2]

M.Tech., Wireless and Mobile Communications, Department of ETM, G.Narayanamma Institute of Technology and Science(GNITS), Ambedkar Nagar, Shaikpet, Hyderabad, Telangana, India

Assistant Professor, Department of ETM, G.Narayanamma Institute of Technology and Science (GNITS), Ambedkar Nagar, Shaikpet, Hyderabad, Telangana, India.

ABSTRACT: Mobile Ad-Hoc Networks (MANET), a fast growing network scheme and it provides lot of features to communication strategies and routing protocols. Trust Management and Energy efficiency are the challenging task to resolve in Wireless Sensor Networks because of dynamic route establishment and route maintenance schemes. The attacks in the network scenarios are: DOS, Wormhole attack and Blackhole attacks. In this system, a new routing protocol strategy is defined by means of Route Request and Route Response Strategies with the help of routing protocols. As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology. In this system, a modified Routing methodology is implemented to define the routing environment with set of nodes and provide the enhanced trust based routing scheme. This proposed approach provides powerful trustworthy data transmission between source and destination, which can perform efficiently. For all, the main motto of the proposed system is to identify the malicious nodes efficiently and send the data between source and destination by choosing a trust worthy path.

KEYWORDS: MANET, Mobile AdHoc Networks, Energy Efficiency, Trust Worthy, Attack Identification.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET), a name defines the network strategy, which contains a set of nodes with mobility enabled features. Due to the openness in network topology and the absence of centralized administration in management of the network, MANET is vulnerable to attacks from malicious nodes or selfish nodes. The nodes in MANET can change their position quite frequently, which mean the mobility of the network. Node misbehaviors such as packet dropping, selective forwarding, flooding are serious attacks for routing protocols in MANET. Secure routing is the milestone in mobile Ad-hoc networks (MANETs). In existing system, we assume that there are malicious nodes in the network which drops the packets. The query issuing node floods a query to the entire network.

Based on the information present in the reply messages, the query issuing node detects the attack and identifies the malicious nodes through message exchanges with other nodes. After identification of malicious node in the network, the path with minimum distance is chosen for forwarding the packets from source to destination via intermediate nodes. The proposed trust management scheme is based on trust. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. After the identification of malicious node, the path with the highest trust value is chosen for forwarding the packets thus by increasing the performance of the network. In the next generation of wireless communication systems, MANET is a collection of mobile users which communicate over bandwidth constrained wireless links. Since the nodes are mobile in nature, the network topology may change rapidly and cannot be predicted over time.

Trust Management System

Ad hoc networks are distributive in nature. Due to this behavior, they are prone to many types of security attacks. The security of ad hoc networks can be enhanced by developing strategies of which one among is: node to use a trust worthy components and improve the network performance by including nodes which are honest and not

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

including the nodes which are dishonest. This strategy also helps in malicious node identification that is identification of the selfish nodes present in the network.

The basic trust management system is shown in following figure.

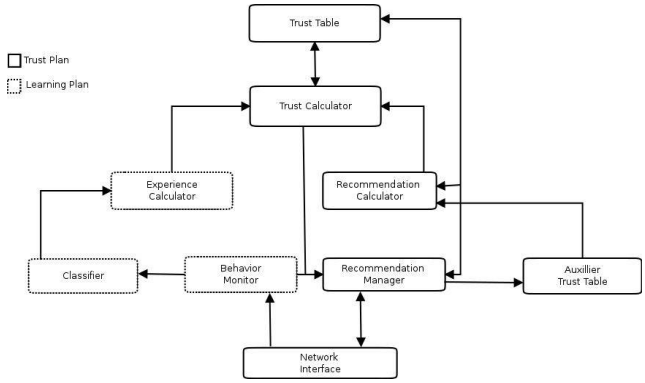

Fig.1 Trust Management Systems

It contains 5 components they are trust table, trust calculator, recommendation calculator, recommendation manager and network interface. The model is basically divided into two parts namely trust plan and learning plan. The function of learning plan is collecting and transforming information and it depends upon three components. Classifier is used for determining the quality of information received. The issue of characterizing trust calculations and trust relationship is studied in many papers. Before we can think about trust models, trust calculations and trust techniques, a basic question must be answered first. What is the actual meaning of trust? Trust is the basic link between perceptions or observations and the metrics that are used for the evaluation of trustworthiness. There are two ways in which the trust relationship can be built. The first way is by observing the behavior of the nodes directly, such as the number of packets dropped, the number of packets delivered etc. The second way is by using the suggestions of the neighboring nodes. For evaluation of trustworthiness, first the initial trust relationship must be maintained. In general, the word trust can be used as the measure of uncertainty. As trust is uncertain in nature, the values of trust can be calculated by using entropy given below.

$$T\{subject : agent, action\} = \begin{cases} 1 - H(p), & \text{for } 0.5 \leq p \leq 1; \\ H(p) - 1, & \text{for } 0 \leq p < 0.5, \end{cases}$$

Where H (p) = entropy function = −p log2 (p) − (1 − p) log2 (1 − p)

p= P {subject: operator, action}

There are axioms that explain the basic rules for building up trust by using suggestions from many nodes. By using below listed axioms, many techniques can be developed. The main goal of this trust models is to enhance the performance of the network and improve security of routing protocols.

Basic Axioms

For building up trust relationship between the entities, understanding basic meaning and the basic axioms is very important.

A. Trust is a relationship set up for a particular activity or action between two entities. Specifically, for performing an action or to play out an activity one entity depends upon the trust values of other entity. The main entity is called subject that is the first entity. Agent or the operator is referred to as the secondary entity. The trust relationship can be denoted by using notation as {subject : operator/agent, action/activity}

B. The uncertainty is taken as measure of trust. The three cases are a) When the subject trusts that the operator will play out the activity without any doubt then the subject completely believes the operator. There is no vulnerability in this

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

case. b) When the subject trusts that the operator will not play out the activity undoubtedly then the subject completely does not trust the operator. c) There is a greater measure of uncertainty, when the subject has no clue about the operator at all. Furthermore, the subject will not have any belief in the operator.

Without a doubt, trust is based on how certain the entity trusts another one and whether few activities will be performed or not. Hence, the level of vulnerability or uncertainty in maintaining trust relationship must be described.

C. Trust is not symmetric in nature. Let us consider two entities A and B. If entity A trusts entity B, it does not mean that the entity B also trusts entity A. Hence a question is raised as how to measure the vulnerability or uncertainty between two entities.

II. LITERATURE SURVEY

In the year of 2010, the authors "X. Liu, J. Xu, and W. C. Lee" proposed a paper titled "A cross pruning framework for top-k data collection in wireless sensor networks", in that they described such as: Energy conservation is a key issue for algorithm designs in wireless sensor networks. In this paper, we explore in-network aggregation techniques for answering top-k queries in wireless sensor networks. A top-k query retrieves the k data objects with the highest scores evaluated by a scoring function on interested features of sensor readings. Our study shows that existing techniques for processing top-k query, e.g., Tiny Aggregation Service (TAG), are not energy efficient due to deficiencies in their routing structures and data aggregation mechanisms.

To address these deficiencies, we propose to develop a new cross pruning (XP) aggregation framework for top-k data collection in wireless sensor networks. The XP framework incorporates several novel ideas to facilitate efficient in-network aggregation and filtering, including 1) building a cluster-tree routing structure to aggregate more objects locally; 2) adopting a broadcast-then-filter approach for efficiently suppressing redundant data transmissions; and 3) providing a cross pruning technique to enhance in-network filtering effectiveness. An extensive set of experiments based on simulation has been conducted to evaluate the performance of TAG and the proposed XP framework. The experimental results validate our proposals and show that XP significantly outperforms TAG in energy cost.

In the year of 2011, the authors "Z. Li and H. Shen" proposed a paper titled "A hierarchical account-aided reputation management system for large-scale MANETs", in that they described such as: Encouraging cooperative and deterring selfish behaviors are important for proper operations of MANETs. For this purpose, most previous efforts either rely on reputation systems or price systems. However, both systems are neither sufficiently effective in providing cooperation incentives nor efficient in resource consumption. Nodes in both systems can be uncooperative while still being considered trustworthy.

Also, information exchange between mobile nodes in reputation systems and credit circulation in price systems consume significant resources. This paper presents a hierarchical Account-aided Reputation Management system (ARM) to efficiently and effectively provide cooperation incentives. ARM builds a hierarchical locality-aware DHT infrastructure for efficient and integrated operations of both reputation and price systems. The infrastructure helps to globally collect all reputation information in the system, which helps to calculate more accurate reputation and detect abnormal reputation information. Also, ARM coordinately integrates resource and price systems by enabling higher-reputed nodes to pay less for their received services. Theoretical analysis demonstrates the properties of ARM. Simulation results show that ARM outperforms both a reputation system and price system in terms of effectiveness and efficiency.

In the year of 2014, the authors "T. Tsuda, Y. Komai, Y. Sasaki, T. Hara, and S. Nishio" proposed a paper titled "Top-k query processing and malicious node identi cation against data replacement attack in MANETs", in that they described such as: mobile ad hoc networks (MANETs), it is effective for mobile nodes to retrieve data items using top-k queries, in which data items are ordered according to a particular attribute score, and the query-issuing node acquires the data items with the k highest scores.

However, accurate results may not be acquired in environments where malicious nodes are present. In top-k queries, it is important to neutralize attacks in which malicious nodes attempt to replace necessary data items with unnecessary ones (we call these, data replacement attacks). In this paper, we propose methods for top-k query processing and malicious node identification against data replacement attack in MANETs. In the top-k query

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

processing method, in order to maintain accuracy of the query result, nodes reply with data items with the k highest scores, along multiple routes. Moreover, to enable detection of data replacement attacks, reply messages include information on the route along which reply messages are forwarded, and thus the query-issuing node can know the data items that properly belong to the message. In the malicious node identification method, the query-issuing node first narrows down the malicious node candidates, using the received message information, and then requests information on the data items sent by these candidates. In this way, the query-issuing node can identify the malicious node. Finally, we verify, through simulation experiments, that the proposed top-k query processing method achieves high accuracy of the query result, and that the malicious node identification method effectively identifies a malicious node.

III. PROPOSED WORK

A Mobile Ad-hoc Network (MANET) is a self-organized network which is comprised of multiple mobile wireless nodes. Due to the openness in network topology and the absence of centralized administration in management of the network, MANET is vulnerable to attacks from malicious nodes or selfish nodes. The nodes in MANET can change their position quite frequently, which mean the mobility of the network. Node misbehaviors such as packet dropping, selective forwarding, flooding are serious attacks for routing protocols in MANET.

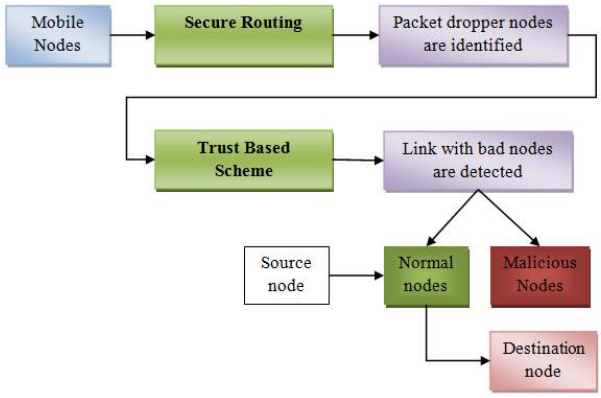

Fig.2 Proposed System Architecture

Secure routing is the milestone in mobile Ad-hoc networks (MANETs). In existing system, we assume that there are malicious nodes in the network which drops the packets. The query issuing node floods a query to the entire network. Based on the information present in the reply messages, the query issuing node detects the attack and identifies the malicious nodes through message exchanges with other nodes. After identification of malicious node in the network, the path with minimum distance is chosen for forwarding the packets from source to destination via intermediate nodes. The proposed trust management scheme is based on trust. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. After the identification of malicious node, the path with the highest trust value is chosen for forwarding the packets thus by increasing the performance of the network.

The main objective of the proposed system is to provide high level of security in ad hoc networks by using trust based routing and prevent data from malicious attackers as well as to differentiate malicious and trustworthy nodes in the network and to improve packet delivery ratio and minimize end to end delay.

The overview of the project is as follows:

A. Forwarding a query
B. Reply forwarding
C. Malicious node identification and Trust based routing

A. Forwarding query

The query is flooded over the entire network by the query issuing node. The query consists of the node identifier of the node which has issued the query (Query-issuing nodeID), the query identifier of the query (Query ID),

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

the query condition, and a list of the node identifiers of nodes on the path along the message has to be forwarded (Query path). In Fig 3, a query issuing node A transmits a query message whose Query path includes its identifier, A, to its neighbor nodes. The node B, receives the query, transmits it to its neighbors. Hop count denotes the number of hops to the node which issues the query, based on the nodes which are included in the Query route. Then, waiting time for reply (RD) is set by B according to the following equation:

$$RD = (hop_{max} - hop_{cnt}) \cdot T_{wait}$$

Where hop count is the number of hops to the query-issuing node, hopmax indicates the maximum number of hops which is calculated based on the size of the network and the range of nodes, and T_{wait} is a positive constant. In this equation, as hop_{cnt} increases, RD decreases. If B receives the query again after sometime, it saves the ID of the sender node as its neighbor node, Query path and the number of hops.

B. Reply Forwarding

After RD has elapsed, each node sends a message in reply (reply message), which contains its own nodeID (Sender node ID), the ID of the next node along the reply path (Dest node ID). A node which has received the query sends a reply message and acknowledgement to the sender. If there is no acknowledgment received by the sender, then the reply message is sent again. If the numbers of transmissions are greater than maximum/threshold value, then the reply message is discarded.

C. Malicious Node Identification and Trust Based Routing

The direct and indirect/recommended trust values are considered for evaluation of trust. The direct calculation of value of trust between two adjacent or neighboring nodes is referred to as direct trust. The node may get suggestion about another node which is adjacent to it from different path as shown in Fig 3. Here node A can get the trust value of node C either directly or indirectly from another path A-BC / A-DC.

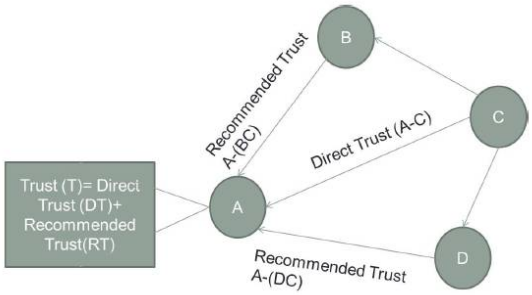

Fig.3 Trust Evaluation

The main aim of the work is to find the malicious nodes present in the networks and to route the packets securely. This mechanism is based on observing the packets and nodal activities. The value of trust is incremented or decremented based on observation of how packets are being transferred and behavior of the node. A node is said to have good behavior if it has successfully sent a packet and bad behavior if it does not perform the above mentioned activity. The trust value of the node is incremented if the number of times the packets transferred successfully is high. The trust value of the node is decremented if the number of times the packets transferred successfully is low. In the proposed strategy, malicious nodes are termed to drop the packets in the network. Based upon the value of trust the good nodes and the malicious nodes can be identified easily.

The value of trust for node x is calculated as follows:

$$T_x = W_d * T_d + W_i * T_i$$

Where W_d and W_i are weights assigned to the direct and indirect trust respectively.

The value of direct trust can be given as follows:

If rate of successful transmission of packets is high then: $T_d = T_d + b*T_p$

If rate of successful transmission of packets is low then: $T_d = T_d - b*T_l$

Where T_p and T_l are sum of success transfer times and failure transfer times respectively and b is arbitrary constant.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

When a packet is sent successfully then the packet success transfer time (T_p) is increased by 1 and if packet failed then packet failure transfer time (T_l) is incremented by 1 and T_p is reset to 0. A HELLO packet is utilised to decide the trust values in the trust table at each and every node.
The indirect trust value is calculated by

$$T_i = \Sigma^{n}_{X=0}\, 0.1 * T_{D\,AX} * T_{D\,XB} \;/\; n$$

Where X is the intermediate node between A and B and n is number of hops. The indirect trust value is determined whenever a node wants to send a packet to another node, or else it is renewed whenever it receives a HELLO message from another node.

The algorithm to find trust worthy path considering direct and indirect trust values is as follows:
1) The trust values of the nodes present in the network and network characteristics are initialised.
2) Whenever a HELLO packet is sent, the malicious node drops the packets and good node forwards the packets. Based upon this network statistics the trust value is updated.
3) To build a path between source and destination a broadcast message should be forwarded.
4) When the route request is received by target node, the route reply is sent along with the trust of the path.
5) The intervening nodes which receive route reply evaluate their trust value based on the behaviour and add their trust values to the trust path.
6) When source receives the reply message for first time, it chooses the best trust value path.
The system can be explained as follows:

- In general, in the route discovery phase, a node which acts as source sends RREQ message to all the nodes present in the network to discover the destination node. When RREQ message is received by the intervening node it will check its routing table and number of hops required to reach the source from itself. RREQ messages can be received by nodes multiple times. So when an intervening node receives the RREQ message for the first time, the hop count is stored as the small number and reverse path is set up to the source. When it receives another RREQ message again after sometime, then it checks if the hop count received is less or more. If the received hop count is less then it is saves as shortest number and the reverse path is reset.
- When RREQ message has reached the destination, it forwards RREP message. The intervening nodes compare the trust value in RREP message in the trust table to get the correct trust value to be utilised to send the RREP message. The node trust values and path trust values are calculated.
- For a node if obtained trust value is less than the threshold value, then it is considered as malicious node or else a normal trust worthy node. When RREP message and path trust values are received by the source node, the paths are sorted in accordance with the trust values obtained. The path with the highest trust value is chosen for transferring the data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

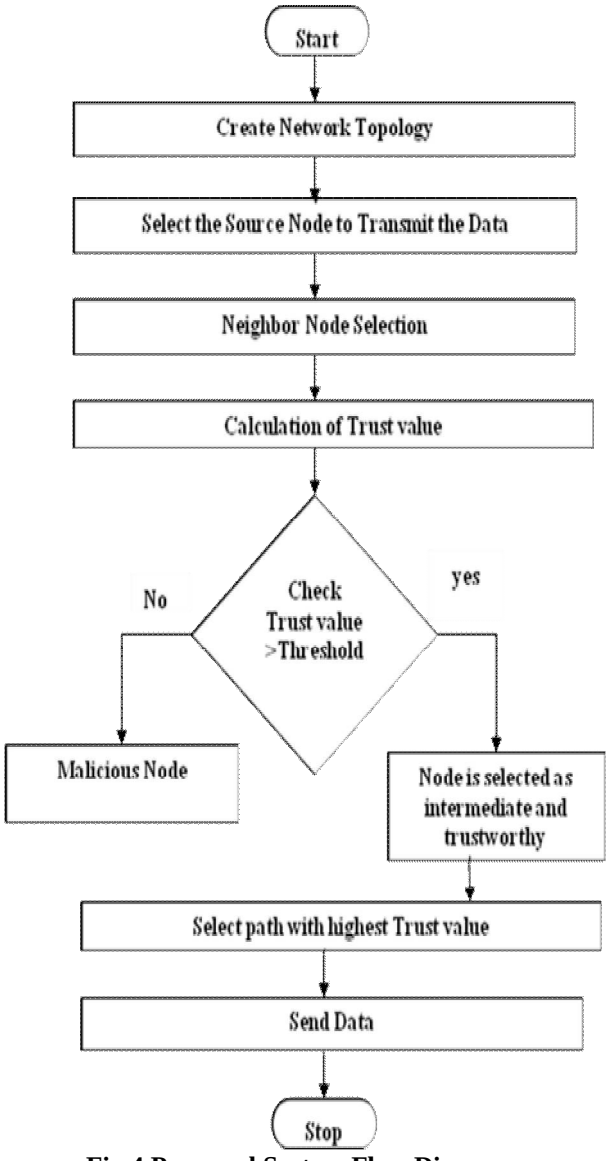

Fig.4 Proposed System Flow Diagram

IV. EXPERIMENTAL RESULTS

The following figure illustrates the simulation parameters of the proposed system. Here, the performance of our proposed trust model is compared with the existing model. Number of nodes which are mobile in the network are 20. NS2 is used for simulation process. The topography of the network is 850 * 850 meters and the movement of the nodes is according to the random waypoint model. The simulation time considered is 2,400 seconds and number of packets is taken as 100. The mobility of the nodes is varied between 0 m/sec to 25 m/sec. The performance metrics considered are Packet delivery ratio, End to End delay.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Simulation run time	2,400 Seconds
Simulation coverage area	850m x 850m
Number of nodes	20
Node assignment	Random
Propagation model	Two way ray model
Wireless transmission range	250 metres
Mobility model	Random Way Point
Network protocol	IP based
Routing protocols	AODV
Maximum Speed	25 m/sec

Table 1. Simulation Parameters

The following figure illustrates the Packet delivery ratio of the proposed system, which is defined as the ratio between amounts of packets received to the amount of packets generated by the source.

Packer Delivery Ratio = number of packets received / number of packets generated.

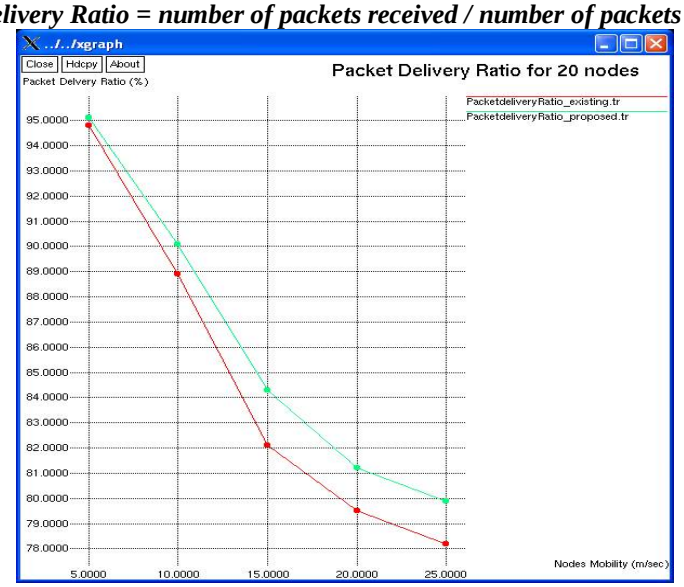

Fig.5 PDR Vs. Mobility

The following figure illustrates the end-to-end delay analysis of the proposed system, which shows the average delay of all the packets transmitted from source to destination is referred to as End to End delay. In Figure 6, the mobility of the nodes in the network increases, the End to End delay also increases. This is due to the time taken for calculation of trust values. As the mobility increases link failures also increases and time is consumed for establishment of new trustworthy path within the network

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

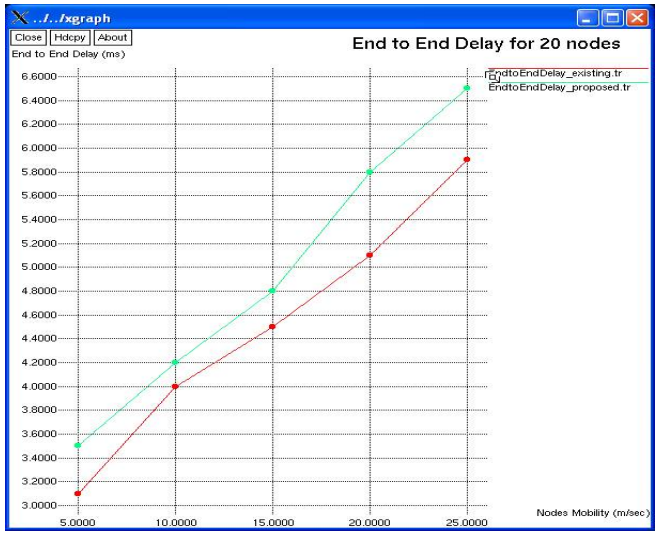

Fig.6 End-to-End Delay Vs. Mobility

V. CONCLUSION

The proposed method, enhanced trust-based routing protocol offers improved packet delivery ratios and enables secure routing of network traffic in MANETs. It isolates malicious nodes from the network using trust levels. Simulation studies, in the presence and absence of trust based routing, have shown better performance results in comparison with metrics, packet delivery ratio, End-to-End delay. Future work on this research will further explore the potential of Enhanced Trust based routing in detecting and isolating additional routing attacks such as: worm whole, modification and rushing attacks.

REFERENCES

[1] D. Amagata, Y. Sasaki, T. Hara, and S. Nishio, "A Cluster-Based Trust Model for Mobile Ad hoc Networks," in Proc. MDM, Jun. 2013, pp. 251_256.
[2] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ``A self-organized mechanism for thwarting malicious access in ad hoc networks," in *Proc. INFOCOM*, 2010, pp. 266_270.
[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs,' pp. 536-550, May 2007, TMC.2007.1036
[4] Balakrishnan, Venkatesan and et al. "Team: Trust enhanced security architecture for mobile ad-hoc networks." Networks, 2007. ICON 2007, IEEE International Conference on IEEE, 2007.
[5] Takuji Tsuda, Yuka Komal, Taka Hiro Hara, "Top-k Query Processing and Malicious Node Identification Based on Node Groping in MANETs ," in Proc. INFOCOM, 2016.
[6] D. Amagata, Y. Sasaki, T. Hara, and S. Nishio, "A robust routing method for top-k queries in mobile ad hoc networks," in Proc. MDM, Jun. 2013, pp. 251,256.
[7] T. Zia, "Reputation-based trust management in wireless sensor networks," in *Proc. International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, 2008, pp. 163-166.
[8] A. Pirzada, A. Datta, and C. McDonald, "Trust-based routing for ad-hoc wireless networks," in *Proc. International Conference on Networks*, 2004, pp. 326-330.
[9] X. Li, M. Lyu, and J. Liu, "A trust model based routing protocol for secure ad-hoc networks," in *Proc. Aerospace Conference*, March 2004, vol. 2, pp. 1286-1295.
[10] W. Lou, W. Liu, and Fang, ``SPREAD: Enhancing data confidentiality in mobile ad hoc networks," in Proc. INFOCOM, vol. 4. Mar. 2004, pp. 2404 2413.
[11] R. Shaikh, H. Jameel, S. Lee, and S. Rajput, "Trust management problem in distributed wireless sensor networks," in *Pro International Conference on Embedded and Real-Time Computing Systems and Applications*, 2006, pp. 411-414.
[12] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in 1*997 New Security Paradigms Workshop, ACM Press*, 1998, pp. 48–60.