Evaluating the Trustworthiness of nodes in AODV by Assigning Reliable Testimonials using NS-2

K. Gowri Raghavendra Narayan, Dr. M. V. Rama Krishna

***Abstract*— An autonomous system of mobile hosts connected by wireless links, often called Mobile Ad-hoc Networks (MANETs) got outstanding success as well as tremendous attention due to its self-maintenance and self-configuration properties or behaviour. Security is a basic and paramount requirement for an ad-hoc network because of its intrinsic vulnerabilities in order for users to perform protected peer-to-peer communication over multi-hop wireless channel. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of nodes. Depending on the application context, a user may desire various security services such as authentication, integrity, non-repudiation, Confidentiality, Key and Trust Management and access control. To improve the security of the MANET, it is essential to evaluate the trustworthiness of nodes by identifying the selfish nodes and malicious nodes in the network. We have used the concept of Reliable Testimonials (RT) in Ad-hoc on demand distance vector routing protocol and assigning it to all the nodes in the network and also we apply a key distribution algorithm. Now this routing protocol deals with attack made by malicious nodes and as well as the presence of malicious nodes during the routing process by omitting them in the communication path based on the threshold value, so that we can assure a highly secured network.**

***Index Terms*— MANETS, Ad-hoc Routing, Selfish and Malicious Nodes, Security, NS-2.**

I. INTRODUCTION

MANET is dynamically self-organized mobile network without infrastructure and central support. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes, not in the direct communication range use intermediate node(s) as routers to communicate with each other. [1] Nodes have to depend on other nodes for forwarding the packets. Due to dynamic topology, open network, energy constraints and limited bandwidth makes MANET vulnerable to many network attacks [2]. Many secure routing protocols have been designed so far like Securing Ad hoc Routing Protocols SAODV, SEAD, etc. which exercises many authentication schemes like hash-chains, digital signature, watchdog and path-rater. [3] [4].

All these secure routing protocols deals with attack made by malicious nodes but does not deal with the presence of these malicious nodes, to maintain the security and integrity of data while forwarding messages we need end-to-end trustworthy communication path. Owing to open medium and intrinsic trust among the nodes it is very difficult to distinguish among normal and malicious node. Recently, many trust based solutions have been proposed that evade the malicious nodes from communication path by assigning some metric to the node which decides the trust level of those particular nodes. But these protocols face the problems of spoof ID, falsified trust, generation of unwanted trust values etc. Also, either the source or destination node is deeply engage in authenticating trust levels of intermediate nodes in the communication path.

In this paper we proposed a concept of Reliable Testimonials (RT) on the basis of a threshold value to the Ad-hoc on demand distance vector routing protocol and applied a key distribution algorithm too. It will facilitate the confidential and sensitive data to travel securely throughout the network. In this approach each node will acquire a secure RT that declares the degree of trustworthiness of particular node. During path innovation, node will request the RT values of neighbor nodes and the nodes whose RT value is more than some specific threshold value is considered for further communication. Finally mostly reliable nodes will select the path with highest path metric and the foremost finest path.
The rest of the paper is organized as, Section 2 briefly illustrates the related work. Section 3 explains the proposed system and the key distribution algorithm the design and implementation, the simulations and results are depicted in section 4, section 5 concludes the paper.

II. LITERATURE SURVEY

Zapata et al proposed the Securing Ad hoc Routing Protocol [3] to secure the routing packets of AODV. Hash chain prevents unauthorized modification of hop count whereas digital signature is used at node level to authenticate the receiver. Yih-Chun Hu et al proposed a Secure Efficient Distance Vector Routing (SEAD) [4] for Mobile Wireless Ad Hoc Networks. It is based on Destination Sequenced Distance Vector routing protocol. In this paper Message Authentication Code (MAC) is used to authenticate the neighbor node and one-way hash chain is used to authenticate routing updates. Sergio Marti et al proposed Mitigating Routing Misbehavior in Mobile Ad Hoc Networks [5], and introduced two extensions to DSR to diminish the effects of misbehaving nodes: Watchdog and Pathrater. Watchdog detects the malicious nodes. Pathrater assigns rating to each node and calculates path metric. Path with the highest path metric is selected. Asad Amir Pirzada et al proposed Establishing Trust in Pure Ad-hoc Networks [6] and make use of trust agents that reside on network nodes. In their proposed model they have used parameters like acknowledgement of packets, packet precision, gratuitous Route Replies,

K. Gowri Raghavendra Narayan, M.Tech Student of Dept. of Computer Science & Engineering, P. V. P. Siddhartha Institute of Technology (Autonomous), Vijayawada, Andhra Pradesh, India. Mobile No: +91 9705409393).

Dr. M.V. Rama Krishna, Professor & Head of Dept. of Computer Science & Engineering, P. V. P. Siddhartha Institute of Technology (Autonomous), Vijayawada, Andhra Pradesh, India., Mobile No: 9440672590

blacklisted nodes and salvaging for the trust levels of the node.

Shinichiro Inoue et al proposed Trust Level Evaluation for Communication Paths in MANETs by Using Attribute Certificates [7] in that offline phase where the trust value of each node is calculated. The calculating node gives trust value information to calculated node in the form of Attribute Certificate (AC). After path discovery the source node has to decide the most trustworthy path. Charusheela Pandit et al proposed Detecting Malicious Node: Survey [8] in their work they covered maximum network attacks and traditional routing protocol and emphasized on few secures routing protocols and its comparison with respect to its security issue and provided the comparison of few traditional routing protocols. Poonam et al proposed Trust Based Security in MANET Routing Protocols: A Survey [9], in their work they have presented an overview of systems that try to detect and correct a node's selfish or malicious misbehaviour Trust has been calculated as a measure of the forwarding mechanism by network nodes. However, they emphasise that such a measure is not only inadequate for trust computation, but is also vulnerable to deception.

Charusheela M. Pandit et al proposed Secure Routing Protocol in MANET Using TAC [10], in their work they have proposed an algorithm for computing trust in different ways and they allocated trust allocation certificate to all the nodes in that approach each node will acquire trust certificate and that certificate declares the degree of trustworthiness of particular node. Wenjia Li et al proposed Security through Collaboration and Trust in MANETs [11] in their work they have proposed a collaborative and multidimensional-trust based outlier detection algorithm for securing mobile ad hoc networks. The gossip-based outlier detection algorithm is used to identify the outliers, which are generally the nodes that have exhibited some kind of abnormal behaviors. Given the fact that benign nodes rarely behave abnormally, it is highly likely that the outliers are malicious nodes. Moreover, a multi-dimensional trust management scheme is proposed to evaluate the trustworthiness of the nodes from multiple perspectives. N. Chandrakant et al proposed, Restricting the Admission of Selfish or Malicious Nodes into the Network by using Efficient Security Services in Middleware for MANETs [12], a solution for security in middleware for MANETS using an algorithm named Security Services in Middleware they made the malicious/selfish node could not be a part of network based on its performance trust value obtained by its neighbors.

III. Description of the Proposed System

The figure 1 shows the basic architecture of the system. It is having four stages, the first stage is the Network initialization stage and the second is RT evaluation stage and the third is Route Assignment stage and the fourth is Route Modernization Stage.

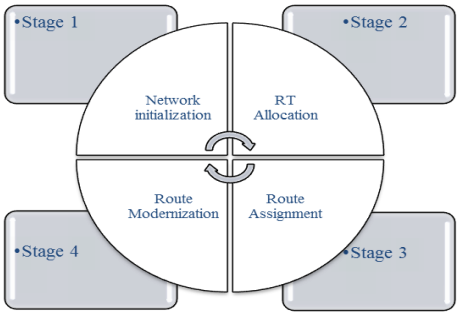

Figure 1: Basic Architecture of the Proposed System

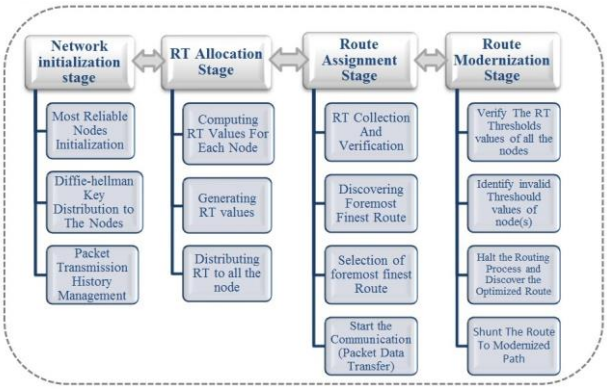

Figure 2: Detailed Description of Proposed Architecture

The above figure 2 shows the detailed description of the proposed architecture, in that each stages is described clearly with the operations and duties of each stage individually.

A. *Network initialization*

The network initialization is takes place and how the key distribution is done. At the beginning the network is initialized with most reliable and with the required number of nodes. After that we have used a key distribution algorithm to generate and distribute the keys to all the nodes in the network.

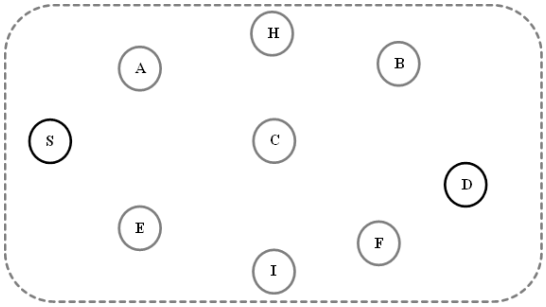

Figure 3: Nodes Initialization

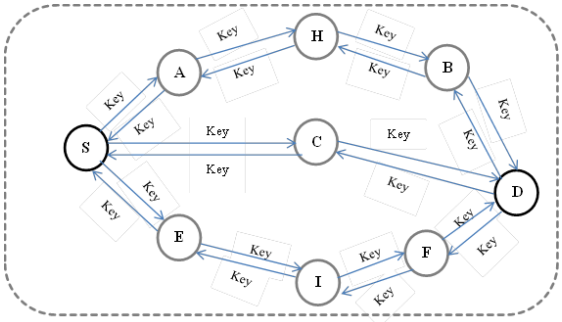

Figure 4: Key Distribution

Here in figure 3 we are just taking nine nodes to illustrate the procedure of initialization and the process of distribution of the keys to all the nodes in the network. Here we considered that the nodes S and D are the source and destination nodes respectively. The key distribution algorithm here used is the Diffie-Hellman key exchange algorithm [13] for generating and distributing the keys to all the nodes in the network the figure 4 shows the distribution of the keys using the Diffie-Hellman key Algorithm.

B. RT Allocation

The RT values are computed and allocated to the nodes. The reliable testimonial values are computed as well as generated based on the certain threshold values. Here we have used the threshold value from 0 to 1 range. We call these threshold values as trust values because the trust worthiness of a particular node is decided on the basis of these threshold values. If any node having the threshold value less than 0 then that node is considered as a malicious node i.e., a node is said to be a trusted node then its threshold value should be greater than zero. Initially all the nodes are given to 0.8 trust value. The format of RT is given below.

Computation of RT: Generally the maximum threshold value is 1 and the minimum value is 0. The number of packets lost is the parameter to calculate the RT values and its trust level. The nodes whose RT trust value is expired or if any node is new in the network whose RT trust value is calculated by its neighbor node whose RT trust value is greater than the minimum threshold value. The node keeps an eye on how the packets are processed by the receiving node. The RT trust computation algorithm is as follows. The algorithm 1 describes the process of computation of the RT trust values for each in node in different conditions.

Algorithm 1: RT Trust Computation

Initialization : MaxRTtrustVal=1;

: MinRTtrustVal=0;

1: if | RTtrustVal($Node_i$) >ΔRTExpTime || $Node_i$== NewNode |

2: RTtrustVal($Node_i$) ←Compute(RTtrustVal($Node_n$))

3: end

4: end

Where ΔRTtrustExpTime is the nodes trust value expire time.

Generation of RT: Here we are just considering a three node communication; the figure 5 shows the RT generation from nodes A to B and B to C. The RT values are generated as per the format of the RT. The figure 6 shows the format of RT, it is having the source and destination node id values and the source and destination nodes RT trust values and the validity for trust value and the digital signature from sender. The figure 7 is the examples of generation of RT values from A to B and B to C. The trust values of A, B and C are 0.6, 0.8, 0.7 respectively. Here the trust values of all the nodes are greater than zero so all the three nodes are considered as trusted nodes.

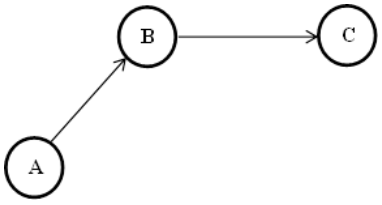

Figure 5: Generation of RT

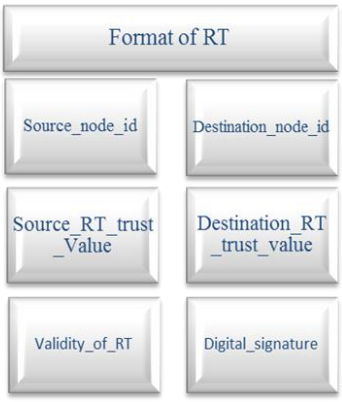

Figure 6: Format of RT

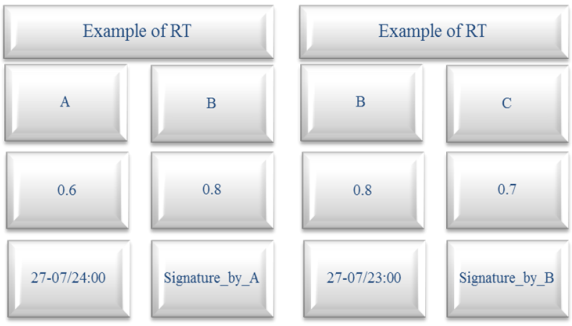

Figure 7: Examples of RT

Distribution of RT: The figure 8 and 9 shows the computing and distribution of RT values respectively for each node from source to destination.

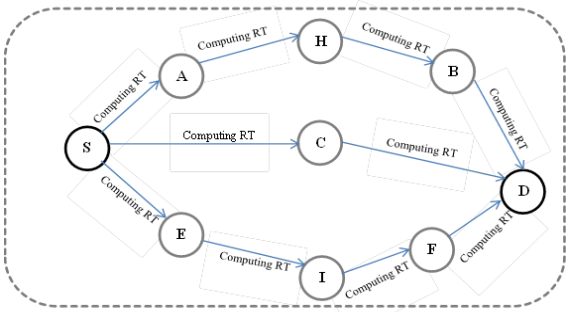

Figure 8: Computation of RT

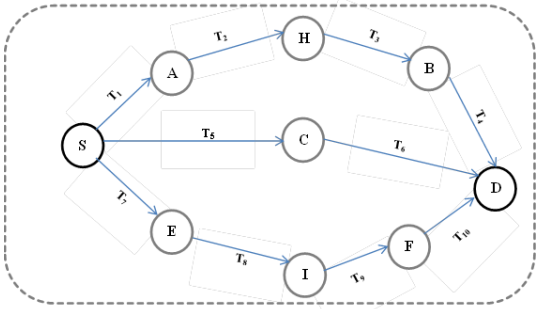

Figure 9: Distribution of RT

These trust values are allocated to all the nodes as RT trust values. The values T from 1 to 10 are the RT trust values assigned to each node individually.

C. Route Assignment

The route assignment is takes place. The route assignment is done by collection and verifying the RT values of each node and discovering the foremost finest route and then selection of the finest route.

RT Collection & Verification: The RT values are collected for each node individually. The nodes which are dropping the packets abnormally instead on forwarding them to next nodes those nodes are called as selfish nodes, then those nodes are treated as malicious and their threshold values are altered to below the actual range and those are not considered for further communication. If any node's RT values are expired then it will request it neighbor node for latest one. The new values are assigned depending on the previous or initial threshold values of the nodes. The nodes whose threshold values are less than the given range are not considered for communication and no more signatures are given to them. Only the nodes whose RT trust values are greater than the minimum threshold are considered for routing. After selecting the trusted nodes the route request and response are takes place. The finest path selected for the communication process.

Discovery of Route & Packet Transmission: the route discovery is done by using the path innovation and evaluation algorithm. The algorithm 2 describes the route selection from sender and receiver side individually. The route is discovered and selected based on the algorithm 2. The following figure 10 describes the pictorial representation of the route requests RREQ and route response RREP. The figure 11 shows the packet data transmission between the nodes in the selected path according to the algorithm 1 and 2.

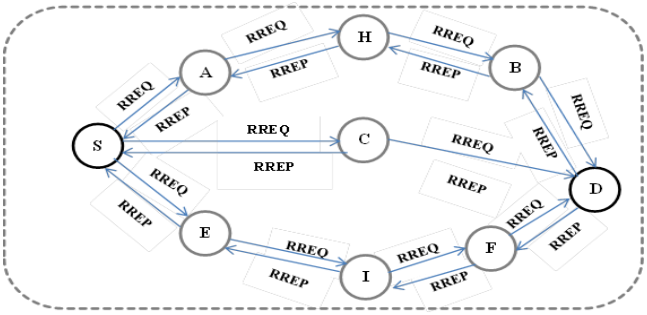

Figure 10: Discovery of Foremost finest Route

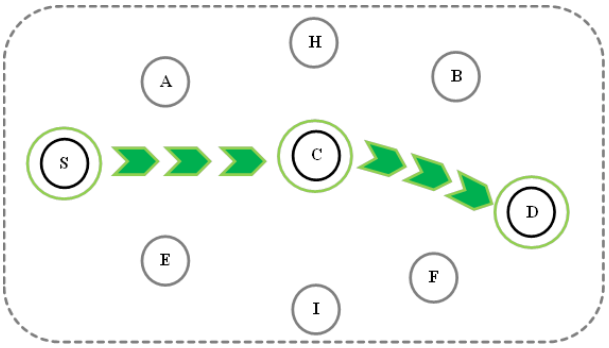

Figure 11: Selection of Route & Packet transmission.

Algorithm: 2 Route Innovations and Evaluation

Sender Side

1: $Node_{source}$ —Request→ RTtrustVal

2: Node ϵ (Source, intermediate) —Verify→ $RTtrustVal(Node_i)$

3: for valid RTtrustVal = 1to n

3.1: Node —Checks→ RTtrustVal(FromNode, ToNode)

3.2: if | FromRTtrustVal > thresholdVal && ToRTtrustVal > thresholdVal |

3.2.1: Node —Appends→ (Node_id, RTtrustVal) to RREQ

3.2.2: Node —Sends RREQ→ Node PathDiscoverer

3.3: else

3.3.1: Node —Discard→ RTtrustVal

Receiver side

4: Node —Receives→ RREQ

5. Node —Verify→ RREQ

6. if | ! $Node_{Destination}$ |

6.1. Repeat steps 1 to 3

7. else

7.1. for each RREQ

7.1.1: $Node_{Destination}$ —Computes→ Multiplies(RTtrustVal, $(ID_1, ID_2, \ldots ID_N)$)

7.1.2: $Node_{Destination}$ —Finds→ Maximum(Multiplies(RTtrustVal, $(ID_1, ID_2, \ldots ID_N)$))

7.2: $Node_{Destination}$ —Selects→ $Route_{optimum}$

7.3: $Node_{Destination}$ —Generate→ RREP

7.4: $Node_{Destination}$ —Sends RREP→ $Node_{Source}$

D. Route Modernization

The route modernization when there is any malicious nodes presence or any node is behaving abnormally like continuous dropping of packets or any considerable delay in the packet transmission. Each node will continuously verify the RT trust values or the threshold values of their neighbor nodes if there is any malicious node presence or any misbehavior of the nodes in the current transmission path then the intermediate nodes identifies the misbehavior or the presence of the malicious nodes by their threshold values and then stop the packet transmission and requests for new route. Then the source node will recomputed the RT trust values of the nodes present in the network and omits the nodes whose threshold values are less than the given range and finds the new optimized path for packet transmission.

The following figure 12 shows the behavior of the selfish node. In the figure the packet transmission takes place from source to destination through an intermediate node C in the network. Suddenly the node C is behaving selfishly and dropping the packets then the source node identifies the packet dropping behavior of the mode C and stop the packet transmission and it discovers the optimized path by omitting the malicious node then shunts the route to the modernized path. The figure 13 shows the route modernization in the network. The intermediate node is changed from C to H.

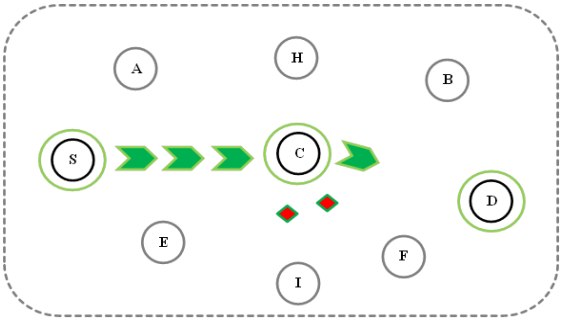

Figure 12: Identifying Selfish nodes during packet transmission

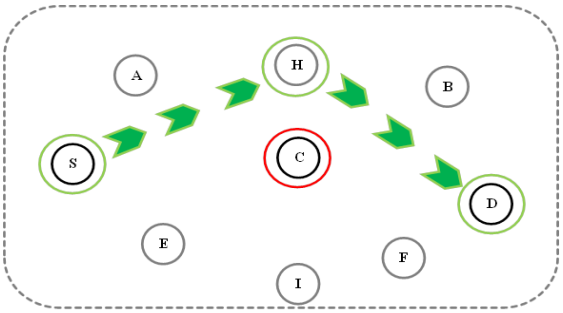

Figure 13: Halting the Selfish path and shunt the route to the modernized path

IV. Simulation Results

In this, first we describe the simulation environment used in our study and then the result analysis in detail. The simulation environment here we have used is NS-2.

Simulation Environment: NS-2 is the discrete-event network simulator, targeted primarily for research and educational use. It is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use [14] [15] [16].

The goal of the NS-2 project is to develop a preferred, open simulation environment for networking research: it should be aligned with the simulation needs of modern networking research and should encourage community contribution, peer review, and validation of the software. NS-2 helps in setting network topology by setting various parameters like protocol, routing algorithm, link, bandwidth etc. simulation parameters are as follows:

- Number nodes used are 50.
- Dimensions of field is 500m×500m
- The maximum velocity used is between 2 to 200units/sec.
- We have used two types of traffic for our simulation FTP and TCP
- Each simulation is run for 150 seconds and repeated for 5 times. We have compared our proposed system with conventional system.
- And also compared the performance with and without the presence of the attacker or the malicious nodes.

Simulation Results: The simulations are done in the network simulator as described in the above section. The figures 14 and 15 are the screen shots of the simulation environment, the NAM (Network Animator) used to make the simulation process in that figures the packet transmission between 15 nodes and 50 nodes are shown respectively. All the simulations are done by assigning the RT values and Diffie-Hellman key exchange algorithm to all the nodes and are done with AODV Routing protocol. The figures 16 and 17 are the screen shots of Xgraph tool with is used to plot the performance graphs for various measures, here it the performance graph for the throughput in kbps for the legitimate traffic and during the attacker traffic respectively. The figure 18 shows the overall performance graph for the legitimate traffic and during the attacker traffic, the graph clearly shows that during active attacker it has lower throughput, lower PDR higher delay, and higher routing overhead compared to legitimate traffic, it indicates that our proposed system is almost finding and omitting the selfish nodes, malicious nodes and improving the performance of the network in terms of throughput and PDR and delay.

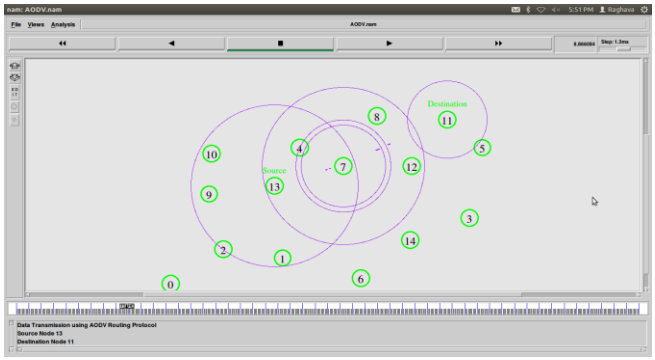

Figure 14: Simulation of 15 numbers of nodes with RT

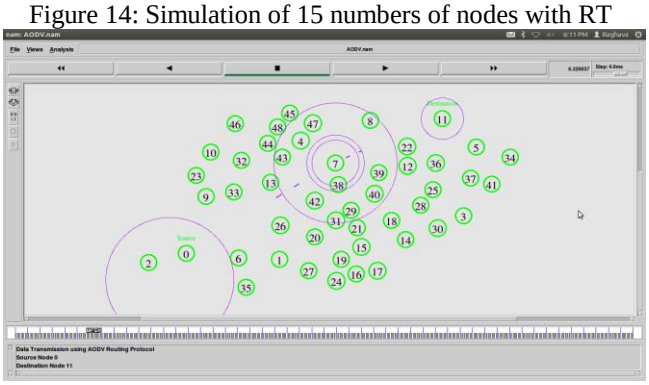

Figure 15: Simulation of 50 numbers of nodes with RT

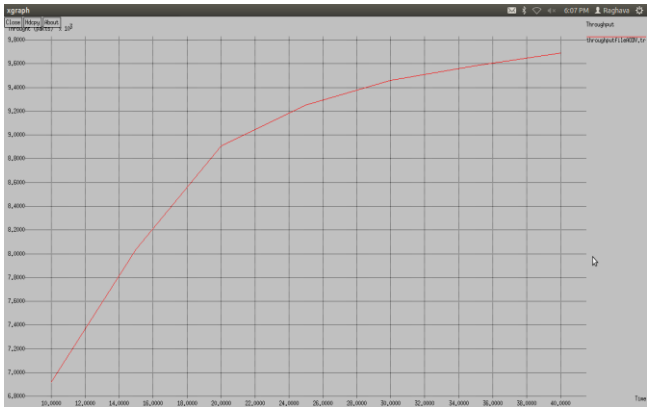

Figure 16: Xgraph for Throughput for legitimate traffic with RT

The figure 19 & 20 shows two performance graphs for the

Throughput in kbps; figure 19 is the graph for conventional vs. proposed model and figure 20 is graph for legitimate traffic vs. during the attacker traffic respectively. It clearly shows that our proposed model and legitimate traffic has more Throughputs, than the conventional model and during the attacker traffic.

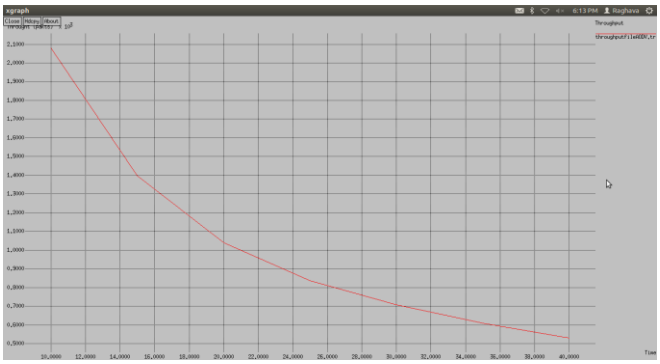

Figure 17: Xgraph for Throughput during the attacker in the network with RT

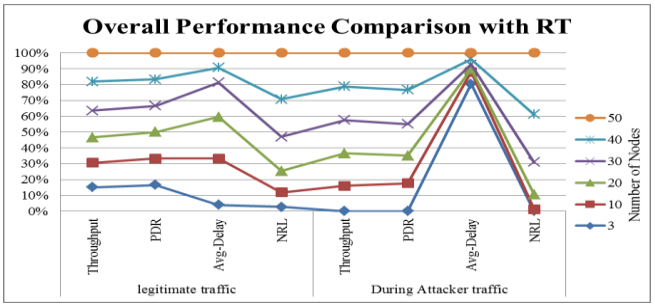

Figure 18: Overall performance Comparison

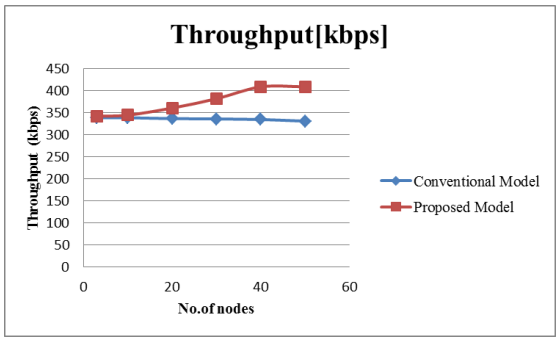

Figure 19: Throughput for conventional vs. proposed model

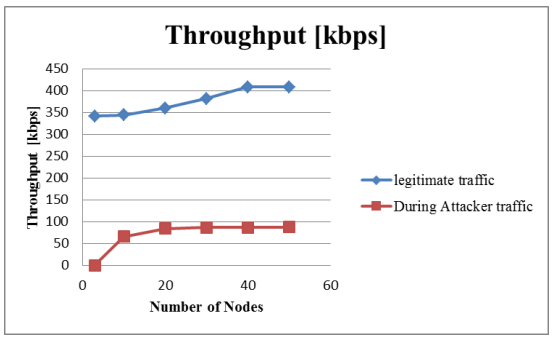

Figure 20: Throughput for legitimate traffic vs. during the attacker traffic

The figure 21 and 22 shows two performance graphs for the packet delivery ratio (PDR), the figure 21 is graph for conventional vs. proposed model and figure 22 is graph for legitimate traffic vs. during the attacker traffic respectively. It clearly shows that our proposed model and legitimate traffic has more PDR, than the conventional model and during the attacker traffic.

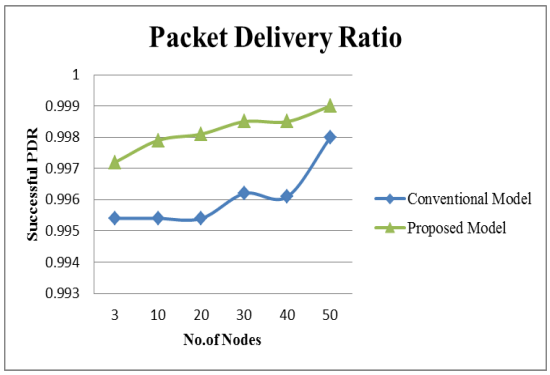

Figure 21: PDR for conventional vs. proposed model

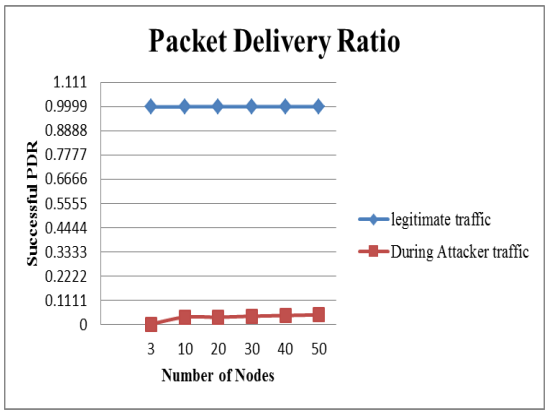

Figure 22: PDR for legitimate traffic vs. during the attacker traffic

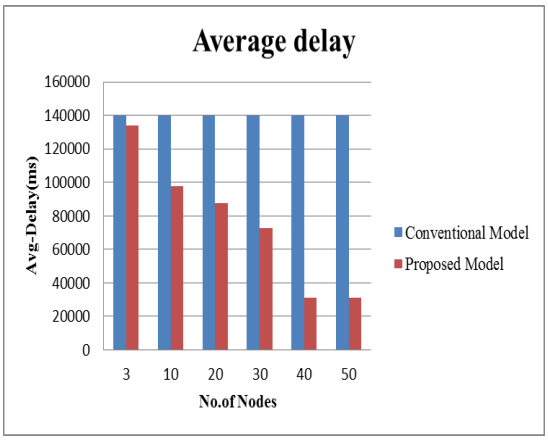

Figure 23: Average Delay for conventional vs. proposed model

The figure 23 and 24 shows two performance graphs for the Average Delay, the figure 23 is graph for conventional vs.

proposed model and figure 24 is the graph for legitimate traffic vs. during the attacker traffic respectively. It clearly shows that our proposed model and legitimate traffic has lower delay than the conventional model and during the attacker traffic.

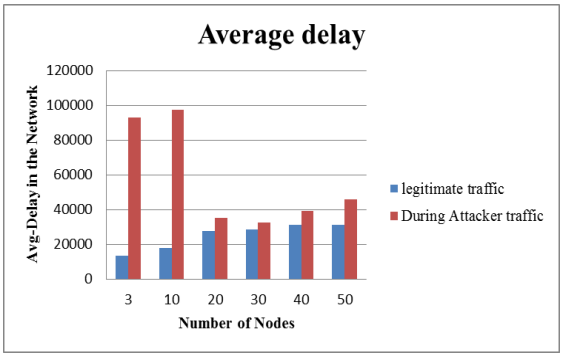

Figure 24: Average Delay for legitimate traffic vs. during the attacker traffic.

The figure 25 shows the RT collection overhead, RT value computation and its transmission causes overhead which are high in RREP packet based algorithms. Where as in our proposed algorithm's RT value computation and its transmission is on demand and expiration based and RT execution takes place in RREQ packets flow causing very less overhead compare to RREP based systems.

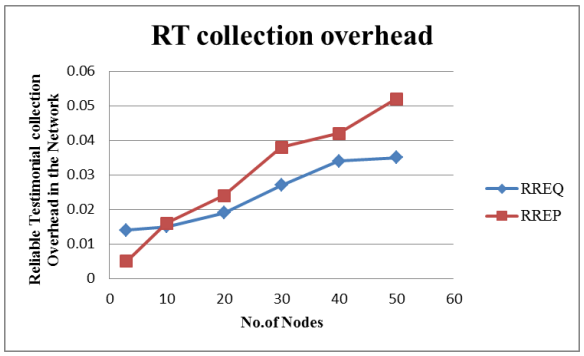

Figure 25: RT Collection Overhead

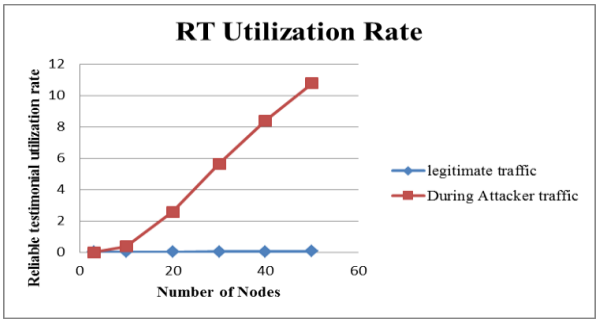

Figure 26: RT Utilization rate

The Utilization of RT ratio shown in figure 26 indicates in terms of legitimate traffic vs. during the attacker traffic. The unnatural behavior of the node causes delay, excessive network resource utilization etc. Our proposed protocol design avoids malicious nodes and finds reliable path. To accomplish this task it demands for fresh RT values, and then it will get legitimate traffic results.

V. Conclusion

The proposed RT Aware with Diffie-Hellman key exchange algorithm based method gives the malicious node free reliable path for MANET communication. It also takes care of RT overhead minimization with periodic RT expiration mechanism. Considering better guarantee and routing information sensitivity, it routes the information securely using cryptographic based hashed function resulting in better throughout and packet delivery ratio. Each node's trustworthiness is awarded before forwarding packet to the node. Packet promotion process depends upon credentiality of nodes. The proposed RT aware routing protocol with key exchange will gives reliable with maximum guarantee of non-malicious node absence and its detection.

Acknowledgment

The authors would like to thank the Department of Computer Science and Engineering of Prasad V. Potluri Siddhartha Institute of technology (Autonomous), Vijayawada, Andhra Pradesh, for allowing us to explore this interesting area.

References

[1] Wenjia Li, Anupam Joshi: "Security Issues in Mobile Ad Hoc Networks – A Survey". http://www.csee.umbc.edu/~wenjia1/699_report.pdf.

[2] Hao Yang, Haiyun Luo & more: "Security in mobile ad hoc networks - challenges and solutions", Wireless Communications, IEEE Volume: 11, Issue: 1 page 38 – 47.

[3] Manel Guerrero Zapata, N. Asokan: "Securing Ad hoc Routing Protocols", September 28, 2002, Atlanta, Georgia, USA. Copyright 2002 ACM 1-58113-585-8/02/0009.

[4] Yih-Chun Hu, David B. Johnson, Adrian Perrig: "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02) 0-7695-1647-5/02 $17.00 © 2002 IEEE.

[5] Sergio Marti, Gluli, Lai, Baker: "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Copyright ACM 2000 1-58113-197-6/00/08...$5.00 Copyright ACM 2000 1-58113- 97-6/00/08 …$5.00.

[6] Asad Amir Pirzada, Chris McDonald "Establishing Trust In Pure Ad-hoc Networks", in Conferences in Research and Practice in Information Technology-2004, http://crpit.com/confpapers/CRPITV26Pirzada1.pdf

[7] S.Inoue, M.Ishii, N.Sgaya, T. Yatagai, I. Sasase: "Trust Level Evaluation for Communication Paths in MANETs by Using Attribute Certificates", 978-1-4244-7057-0/10/$26.00 ©2010 IEEE

[8] Charusheela Pandit, Seema Ladhe, "Detecting Malicious Node: Survey", Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 4, Issue 1(Version 2), January 2014.

[9] Poonam, K. Garg, M. Misra, "Trust Based Security in MANET Routing Protocols: A Survey", Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India, September 2010.

[10] Charusheela M. Pandit, Seema A. Ladhe, "Secure Routing Protocol in MANET Using TAC", IEEE in Networks & Soft Computing (ICNSC), 2014 First International Conference on 19-20 August 2014.

[11] Wenjia Li, James Parker, Anupam Joshi, "Security through Collaboration and Trust in MANETs", Mobile Networks and Applications, Volume 17 Issue 3, June 2012, Springer-Verlag New York, Inc.

[12] N. Chandrakant, P. Deepa Shenoy, K. R. Venugopal, L. M. Patnaik, "Restricting the Admission of Selfish or Malicious Nodes into the Network by using Efficient Security Services in Middleware for

MANETs", Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, February 2011.
[13] Abdulrahman H. Altalhi, "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks", in Scientific Research, Communications and Network, 2012, 4, 83-87 doi:10.4236/cn.2012.41011 Published Online February 2012 , http://www.SciRP.org/journal/cn
[14] "Network simulator" http://www.isi.edu/nsnam/ns/, and https://www.nsnam.org.
[15] "NS Simulator for Beginners" written by Eitan_Altman_Tania_Jimenez.
[16] "Introduction to Network Simulator-2" second edition, written by T. Issariyakul et al 2012

Mr. K. Gowri Raghavendra Narayan Received his B.Tech degree in Computer Science & Engineering from Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. And he is currently pursuing M.Tech Degree in Computer Science & Engineering in Prasad V. Potluri Siddhartha Institute of Technology (Autonomous) Vijayawada, Andhra Pradesh, India and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. His area of research includes Computer Networks. He is a student Member of ACM.

Dr. M.V. Ramakrishna has been working as Professor & Head in the Department of Computer Science & Engineering, Prasad V. Potluri Siddhartha Institute of Technology (Autonomous) Vijayawada, Andhra Pradesh and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. He obtained B.Tech, M.Tech and Ph.D. from NIT- Suratkal, Jawaharlal Nehru Technological University, Hyderabad and Acharya Nagarjuna University, Guntur respectively. He has 23 Years of Teaching and 4 Years of Industry Experience. He had published 9 research papers in various International Journals and conferences. His areas of research include Computer Networks and Distributed Systems. He is a Member of ACM and IEEE Computer Society.