International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 8 – MAY 2017.

Enhanced Trust & HLA based public auditing architecture in MANET to Eliminate Packet Dropping Attacks

RAYUDU SUDHEER [#1] and CH SUBHASH [*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science & Engineering, JNTUK,A.P, India.*

[*]*Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— Mobility and portable nature of Mobile Ad hoc Networks (MANET) has increased its popularity by two fold. MANETs have become a commonly used network for various applications. But this advantage suffers with serious security concerns, mainly a wireless transmission medium perspective where such networks may be subject to packet dropping. Mobility and portable nature of Mobile Ad hoc Network may also lead to link failure. During packet forward, valuable packets may be dropped by malicious nodes present in the network. Link error and malicious packet dropping are the two sources for packet losses in MANET. In this paper, we propose a new routing mechanism to combat the common selective packet dropping attack based on associations between nodes are used to identify and isolate the malicious nodes through trust estimator. Simulation results show the effectiveness of our scheme compared with conventional scheme. This eliminates the overhead of invoking the trust estimator between companions. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown in the network.**

Index Terms*— Certificateless-effective key management (CL-EKM)), Energy Efficient System

I. INTRODUCTION

MANETs are a type of wireless networks which are rapidly growing because there is no such requirement for setting up an infrastructure for their operational purposes. In such networks, the topology is dynamic, and the nodes are mobile in nature. It must be able to continue their traffic even if the wireless transmission medium is out of range. This effectiveness and flexibility makes these types of networks attractive for many applications. Two nodes can communicate or send data packets to each other when they come within the radio range to each other, if they are not in the radio range neighbouring nodes forwards the packet to them. MANETs supports the multi hop communication between the nodes. While performing such operations, it may take into concern that the data cannot be dropped by malicious nodes or misbehaved links. It is still a challenging security concern [1].

Nodes in ad hoc networks rely on other nodes to forward and route data packets to the destination. Malicious nodes can exploit this situation and disrupt ad hoc network operation by dropping data packets and not delivering them to the next hop. In its obvious version, a malicious node will simply discard all the data packets that it is supposed to relay (this is referred to as the black hole attack [2]). The nodes in an ad hoc network communicate using wireless links which are by nature vulnerable to interference and channel errors that may corrupt some or many data packets. Moreover, the nodes share the physical medium, compete to transmit data packets and suffer collisions. Thus, one of the problems in detecting malicious nodes that drop packets is that it may not be clear as to whether the packet was dropped due to channel errors, collisions, or due to malicious intent [3].

In most detection mechanisms, the number of packets that are not forwarded is recorded by a passive listener. A threshold on the number of dropped packets is then used to decide whether or not a node is malicious. Depending on the threshold and data load, a burst of errors on the channel or an increase in the number of collisions can trip the threshold creating false alarms. Basic features of MANETs such as communication via wireless links, resource constraints cooperativeness between the nodes and dynamic topology make it easier to attack. Specifically in MANETs, one of very common attack is dropping data packets through malicious node. In dropping data packet attack and routing packet attack malicious node prevents packets to forward to other mobile nodes and then drop these packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is equally important and cooperative. That means, if a node claims it can reach another node by a certain path or distance, then protocol takes the claim as real and similarly, when a node reports a link break, the link will not be used for next transmission [4].

In dropping data packet attack and routing packet attack malicious node prevents packets to forward to other mobile nodes and then drop these packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is equally important and cooperative. That means, if a node claims it can reach another node by a certain path or distance, then protocol takes the claim as real and similarly, when a node reports a link break, the link will not be used for next transmission. AODV is the commonly used reactive routing protocol in MANET. It is an on-demand protocol, which initiate route request only when needed. AODV is also affected by packet dropping attack. AODV performs better comparing to another protocol like dynamic source routing protocol (DSR) [3]. The proposed work adds security features to AODV and has introduced protocol named SAODV. Here it basically deals with packet dropping in network layer. The first level of acknowledgment, such as Transmission Control Protocol Acknowledgment can detect end-to-end communication break, it is unable to identify accurately the malicious node which contributes that attack. Such mechanism is unavailable for connectionless transport layer protocols like User Datagram Protocol. Therefore, securing the basic operation of the MANET becomes one of the primary concerns in mobile environments in the presence of packets droppers [2]. The challenge lies in securing communication with the maintenance of connectivity between nodes under the crucial attacking situations and the frequently changing topology.

Detecting selective packet-dropping attacks is more challenging in a highly mobile wireless environment. The main difficulty is the requirement that need not to only detect the node where the packet is dropped, but also identify whether the drop is intentional or unintentional [5]. In order to precede a black hole attack, malicious node exploits the vulnerabilities of the AODV protocols which are generally designed with strong assumption of trustworthiness of all the nodes present in the network. Any node can easily misbehave and can make a severe harm to the network by targeting both data and control packets [5].

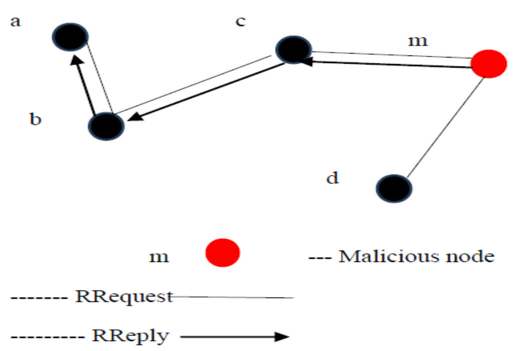

Fig. 1.Black hole attack in AODV

For making black hole attack malicious node should be in the routing path. Attack procedure can be explained as follows, as shown in Fig. 1, “m” is a malicious node whereas “a” and “d” are the source and destination nodes respectively. Initially the source node “b” broadcasts Route Request (RREQ) packet to its neighbors in one hop manner. After receiving this packet, each neighbor node is rebroadcasted if it has no route to destination. In this case malicious node “m” may spoof the IP address of the destination “d”, inciting the source node “a” to establish the path towards “e”, instead of “d” or malicious node can claim that it has the shortest path to the destination and sends a RREP to source node “a” . The source node “a” realizes that the route passing through the node “m” is the shortest path, and thus it starts transmitting data packets towards „m‟. In both cases „m‟ can drop all incoming packets or selected packets [4].

Dropping of routing packets causes failure for source node to identify path to destination. Source may conclude destination as unreachable. Dropping of data packets leads to communication failure between nodes. Dropping of routing packets and data packets is an equivalent complex issue, so initial detection of malicious nodes are important for proper delivery of packets to destination.

Link failures also have big part in packet dropping. In mobile wireless environment, link errors are quite significant, and shall not significantly smaller than the packet dropping rate of the malicious nodes [4].

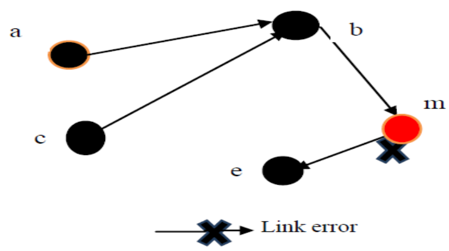

Fig.2. Link failure

Link failure is represented in Fig. 2, here link between “m” and “e” is broken. AODV protocol has option to inform neighboring nodes about the link failure. In the given figure node “e” informs malicious node “m’ about link failure between them via sending Route Error (RERR) message. Normal case node “m” should inform neighboring nodes about link failure and it will be forwarded to source node “a”. Link error Fig.2. Link failure Here “m” is malicious and there is a chance for not forwarding the link failure information. Due to this situation source node continue the packet sending through the same path a-c-m-e. Malicious node will drop all the packets coming through this path [4,5].

Most of previous works only proposed the dropping due to link failure or due to malicious drops separately. In this paper, we propose a new routing mechanism to combat the common selective packet dropping attack. Associations between nodes are used to identify and isolate the malicious nodes which can handle these kinds of attacks and should take preventive actions against attacks that consider malicious nodes as the main cause of packet dropping but link failure also have equal part in packet dropping. Main focusing of existing works is to identify data packet dropping. This work deals with both routing and data packets dropping and also gives equal importance to identify link failures. The proposed system can take preventive actions too using trust estimators. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol [6]. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown

II. LITERATURE SURVEY

A number of works have been done on the area of ad hoc network security especially for detection of packet dropping attacks by malicious nodes. This section mentions some of these works.

In the year 2003 Borzoo Shadpour, Shahrokh Valaee, Baochun Li [7] proposed paper titled "A Self-Organized Approach for Stimulating Cooperation in Mobile Ad Hoc Network" which contain the self-organized mechanism that is broke service, which allows for a broke node to use the network to transmit its traffic, in addition it providing an incentive to stimulate non-broke nodes to cooperate with broke ones. The main idea is to improve the connectivity of broke nodes in a pure ad-hoc networks. The proposed solution is loaning, which is interesting since it can be performed 'on-the-fly' by the nodes systems, and is suitable for the conditions of ad-hoc networks since it allows for nodes to remain self-organized. This scheme stimulates nodes to actively participate in the network, allowing the broke nodes to experience less delay when urgent transmission is desired.

In the year 2005 Wenyuan XU, Wade Trappe, Yanyoung Zhang, Timothy Wood [8] proposed a paper titled "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Network" which examine radio interference attacks from both sides of the issue: first, study the problem of conducting radio interference attacks on wireless networks, and second examine the critical issue of diagnosing the presence of jamming attacks. Specifically, proposes four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. The paper also study different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular the signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. The paper proposes two enhanced detection protocols that employ consistency checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. In the paper the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

In the year 2007 Jakob Erikson, Michalis Faloutsos, Srikanth V, Krishnamurthy [9] proposed a paper titled "Routing amid Colluding Attackers "with the first practical solution to the long-standing problem of secure wireless routing in the presence of colluding attackers. The secure routing protocol, Sprout1, continuously tries new routes to the destination. Routes are generated probabilistically, with complete disregard for performance metrics. This nature makes Sprout uniquely resilient to attack. it cannot be tempted by any kinds of shortcuts. To avoid compromised routes, and to ensure good overall performance, the quality of each active route is monitored by means of signed end-to-end acknowledgments. Based on this end-to-end acknowledgments amount of traffic sent on each route is adjusted accordingly. The vast majority of known routing layer attacks is mitigated by Sprout effectively, even when under assault from a large number of colluding attackers. . Sprout consistently delivers high, reliable performance in benign as well as hostile environments.

In the year 2009 William Kozma Jr , Loukas Lazos [10] proposed a paper titled "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Network based on Random Audits" the paper investigate the problem of uniquely identifying the set of misbehaving nodes who refuse to forward packets. The resource-efficient accountability for node misbehavior is identified by the new misbehavior identification scheme called REAct. The identification of misbehaving nodes based on a series of random audits triggered upon a performance drop is done in REAct. The source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes. Proofs are constructed using Bloom filters which are storage efficient membership structures, thus significantly reducing the communication overhead for misbehavior detection. REAct has three phases (a) the audit phase (b) the search phase (c) the identification phase.

In the year 2010 Divya Ann Luke, Dr Jayasundha. J .s [11] proposed a paper titled "Selective Jamming Attack Prevention Based on Packet Hiding Methods and Wormholes" contain a new method to prevent the selective jamming attack in a internal thread model. The wormhole is which will generate an alarm to

indicate the presence of jammer and sent IP address of jammer node to all other nodes in the network is used. We can send message through the network even though a jammer is present by sing a method called packet hiding. The technique called Strong Hiding Commitment Scheme (SHCS) this method is used. Here, the wormhole becomes the access point in a network region whenever it finds out any node that violates the rules in a particular network region. Such node is then considered as a jammer node. Wormhole sends IP address of jammer to all other nodes. The prevention of the jamming activity of the jammer is done by Wormhole, by encrypting the source ID of message along with the message packet. By doing so jammer is unable to identify its target node and the source can forward its message safely through jammer node itself.

In the year 2013 Mrs. K. Gomathy, Mr. P. Dinesh kumar [12] proposed a paper titled" Detection of Routing Misbehavior in Manet by Enhanced 2ack Scheme Using Dsr Protocol "which focuses on routing misbehavior in MANET and method for detection of misbehavior which is caused by links. All the interested nodes to participate in routing should be fully co operative in MANET. But some nodes get benefits for other nodes refuse to share their resources. Performance of network gets affected due to the node mobility, open structure and dynamic topology changes. To detect such behavior by sending acknowledgement through opposite direction of the routing path the 2ACK scheme is used. The proposed enhanced scheme using DSR protocol reduces the overhead of acknowledgement by 2ACK scheme. There are three modules in 2ACK system.

The work is classified into two categories. First category is based on malicious node dropping the packet which works on detecting the malicious node that causes the discarding of packets. Detection accuracy of malicious node is done by four ways i) whenever a node sends a packet it will earn a point for transmitting a packet. The malicious node which continuously discards the packet will lose its point [7] [6] [1] ii) Each node is monitored by its neighbor node. So the misbehaving node is monitored by the neighbor node iii) malicious node place will be identified and removed from the network. iv) Some cryptographic method is used to have the record of forwarded packets. All this ways of identifying the malicious node have disadvantages and these methods will not be applicable when the packets are highly selective. If a basic access procedure is used, the sender depends on feedback from the receiver to determine the cause of packet loss. If a packet with a corrupted header is received, the receiver sends nothing and the sender will timeout and assumes that a collision occurred. If a packet with a correct header is received but the data part is corrupted, the receiver can recognize the sender and reply with a NAK frame. Here, the sender will assume that the packet was lost due to channel error.

CONFIDANT [7] protocol as proposed by Buchegger et al extends the concepts of watchdog and pathrater. In this mechanism, misbehaving nodes are not only excluded from forwarding route replies, but also from sending their own route request. The scheme includes a trust manager to evaluate the level of trust of alert reports and a reputation system to rate each node. The reports from trusted sources are only processed by the nodes. However, it is not clear how fast the trust level can be adjusted for a compromised node especially if it has a high trust level initially.

Buttyan et al [13] have advocated the use of tamper-resistant hardware on each node of a MANET to encourage cooperation. Nodes are assumed to be unwilling to forward packets unless they are stimulated to do so. In this approach, a protected credit counter runs on the tamper-resistant device. It increments by one when a packet is forwarded. It refuses to send its own packets if the counter is smaller than a threshold. Public key cryptography is used to exchange credit counter information among the neighbors and verify if forwarding is really successful. However, the availability of tamper-resistant hardware is a very vital assumption for the successful working of the scheme that involves complexity in hardware design.

III. EXISTING SYSTEM

In the existing methods, they have proposed accurate algorithm is developed to detect the malicious packet drop. Here detection accuracy is very high which is achieved by finding the correlation of lost packets which is obtained by using the bitmap of packet reception provided by each node. By finding correlation between lost packets we can find whether packet loss is only because of link error or is the effect of combination of both link error and malicious packet drop because both correlation gives different patterns for packet loss. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, they verified that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection. Even though they obtain the highest accuracy in detecting the attackers but they fail to prevent the data from the attackers during the data transmission [14].

IV. LIMITATIONS

The major limitation in the existing methods, due to the open nature of wireless medium, a packet drop in the network could be caused by harsh channel conditions e.g., fading, noise, and interference, link errors, or by the insider attacker. In an open wireless environment, link errors are quite significant, and may not be significantly smaller than the packet dropping rate of the insider attacker. So, the insider attacker can camouflage under the background of harsh channel conditions. In this case, just by observing the packet loss rate is not enough to accurately identify the exact cause of a packet loss. They need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional and it should be prevented from the attacker [14].

V. PROPOSED SYSTEM

As our contribution for homomorphic linear authenticator (HLA) based public auditing architecture, we propose methods to overcome efficient packet dropping in MANET. We know that, Mobile ad hoc network (MANET) is a self-organizing, self-configuring confederation of wireless systems. MANET devices join and leave the network asynchronously at will, and there are no predefined clients or server. The dynamic topologies, mobile communications structure, decentralized control, and anonymity creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. In this paper, we propose a new routing mechanism to combat the common selective packet dropping attack. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of our scheme compared with conventional scheme. The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown .

The ultimate goal of this project is to avoid inclusion of intruder node in the route and to ensure reliability. The trust metrics are used to provide the security over communication. In the MANET communication, each and every node has the chance to select the next intermediate node. The best intermediate node is selected based on the trust value of a node. Each and every mobile node maintains the trust value for its neighbors. The trust value is calculated based on the node's QoS (Quality of Service) parameters. The throughput, packet loss rate and delay are also considered as the parameters used to calculate the trust value. The node with highest trust value is selected as next forwarder node. In the proposed method a node does not maintain the static route to reach the destination. Instead of that the node selects the next forwarder node during runtime. It is best suited for highly dynamic environment to handle the frequent link failure. So, the source node transmits the data to the destination node only via trusted node to ensure security in the MANET.

VI. SYSTEM ARCHITECTURE

The initially the network is configured with calling the Node configure function with number of nodes. And then Link create will create link, while creating link we need to specify the levels with which the node is associated. Once the network is configured we take up server as the destination and any of the nodes as the sender. Once the network is set we browse for the file we need to send. In the source we split the entire file in to number of packets these packets will be encrypted and Add bit function will help in adding bits to identify the change in number of packets and packet will be forwarded further.

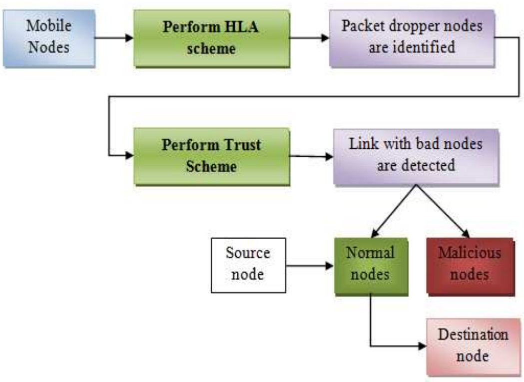

Fig. 3 System architecture

The packet will be received by the intermediated node in normal transition packet will be encrypted and forwarded whereas in attacker mode packet will be dropped or modified or both will be done and forwarded. Once the packet reach destination in normal node packet will be verified, bit identified, decrypted and finally merged. In attacker mode when packet is verified the packet dropped is identified, bit identification will let us know about packet modification. On modification or dropped packet cannot be decrypted. To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. By detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.

The main challenge in mechanism lies in how to guarantee that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflects the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets; this can be achieved by some auditing. Considering that a typical wireless device is resource-constrained, we also require that a user should be able to delegate the burden of auditing and detection to some public server to save its own resources. Public-auditing problem is constructed based on the homomorphism linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients. For identifying the entrusted nodes, we use trust aware routing for detecting the known and unknown nodes. By using trust classification, the nodes are identified as the known and unknown, the data transmission has been done through trust nodes which has higher trust value. The trust value calculation are handled by the trust estimators that is based on the trust routing table in which the neighbour node estimates the trust value depend on trust estimators in order to provide the secure data transmission.

A. SYSTEM MODULES

The proposed system contains five modules.
1. Network modeling.
2. Independent auditing.
3. Setup phase.
4. Packet dropping detection
5. Trust management

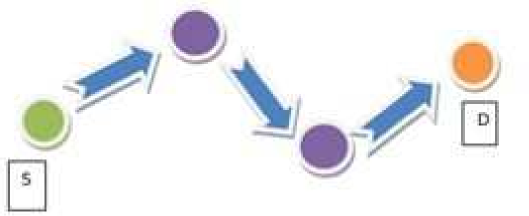

Fig.4. Intermediate nodes with source and destination.

B. Network modeling

The wireless channel is modeled of each hop along PSD (Path to Source and Destination) as a random process that alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. It is assumed quasi-static networks, whereby the path PSD remains unchanged for a relatively long time. Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, maintaining stable connectivity between nodes is a greater concern than detecting malicious nodes. A sequence of M packets is transmitted consecutively over the channel.

C. Independent auditor

There is an independent auditor Ad in the network. Ad is independent in the sense that it is not associated with any node in PSD. The auditor is responsible for detecting malicious nodes on demand. Specifically, it is assumed S receives feedback from D when D suspects that the route is under attack. Once the destination click on verify, the action takes places to identify the packet loss. To facilitate its investigation, Ad needs to collect certain information from the nodes on route PSD.

D. Setup phase

This phase takes place right after route PSD is established, but before any data packets are transmitted over the route. In this phase, S decides encrypt the packets and sent through the route to destination. Destination after receiving packets can verify the packet and after verification it can decrypt the packets.

E. Packet drop detection

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are transmitted consecutively over a wireless channel. Under different packet dropping conditions, packet loss is identified.

F. Trust management

In the proposed technique, every node maintains a trust value for each of its neighbors (nodes that are within its radio range). This value is a measure of the level of trust it has on its neighbor. For scalability, we have designed our trust model such that the trust value is calculated using only local information. Let Ti (j) denote the level of trust of node i on neighbor j. The values of Ti (j) range from 0 (denoting absolutely no trust) to 1 (denoting full trust) $0 \le Ti\ (j) \le 1$. We have taken Ti (j) to be the weighted average of two components.

$$T_i(j) = aT_{i(self)}(j) + bT_{i(neighbor)}(j) \quad (1)$$

Ti(self)(j) represents the trust of node i on node j, based on node i's observation of node j's behavior (e.g. by monitoring traffic of node j). Ti (neighbor) (j) represents the trust that neighbors' of node i have on node j. These neighbors of node i are also neighbors of node j. a +b = 1 and $0 \le a, b \le 1$. Let a1, a2, a3. . . an be the neighbors of node i (where n is the number of neighbors) such that they are also neighbors of node j. Then Ti (neighbor) (j) is given by:

$$T_{i(neighbor)}(j) = \frac{1}{n}\sum_{l=1}^{n} T_{al}(j) \quad (2)$$

By varying the values of a and b, we can thus vary the weight of self-trust as compared to neighbors' trust in evaluating the overall trust. It is clear that Ti (neighbor) (j) is the average of the existing trusts of the neighbors. Thus, in our node trust model, the past history is also taken into account. This is important when we want to evaluate trust based not only on present observations but also on past behavior.

The node trust Ti (self) (j) is calculated as

$$T_{i(self)} = \sum_{l=0}^{n-1} \frac{Forwarded(l)}{ToForwarded(l)} \quad (3)$$

The To-Forward and Forwarded data structures correspond to those that are kept by node i for node j. Thus, Ti (self) (j) is the ratio of the number of packets forwarded to the number of packets to be forwarded. Every node uses the above formula periodically (after every 'NodeTrustUpdate' interval) to update the node trust of its neighbours.

Based on these module, we make trust aware routing module. Where the problem of packet dropping is avoided by making the transmission in the trust aware routing nodes.

VII. PERFORMANCE EVALUATION

A. Simulation Parameters

The NS2 tool is used to study the performance of our Enhanced Trust & HLA based public auditing architecture. We employ the IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s . We comparative the normal HLA based public auditing architecture with proposed Enhanced Trust & HLA based public auditing architecture in order to prove that proposed simulation results are better in detecting the packet dropping attackers as well as provide secure routing path for source to destination. We choose the two evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, delay – the average time taken for a packet to be transmitted from the source to destination,

Performance Metrics: The metrics used to evaluate performance of proposed approach:

a)Packet Delivery Ratio (PDR): It is defined as the total number of packets received by the destination node and total number of packets originated by source node.

b) Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination.

c) Packet loss: It is defined as the packet failed to reach the destination with respectively to the time period

A graph is plotted between time and packet size to study the delay in the proposed system and is shown in Fig. 7 , packet delivery ratio in fig .6 , packet loss and in the fig. and routing overhead in fig . The result shows that Enhanced Trust & HLA based public auditing architecture performances is better than HLA based public auditing architecture for the detection of malicious node and secure routing path for data transmission.

TABLE I. STIMULATION PARAMETERS

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	700m*700m
Simulation time	800

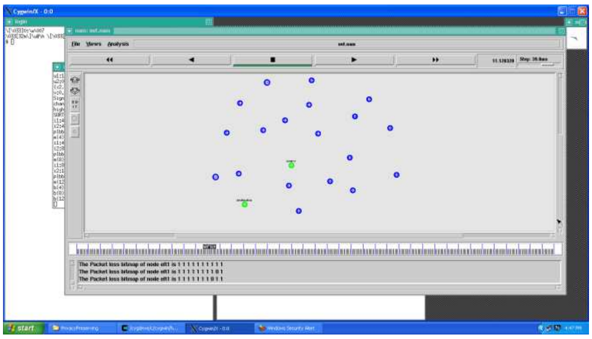

Fig.5 HLA based public auditing architecture

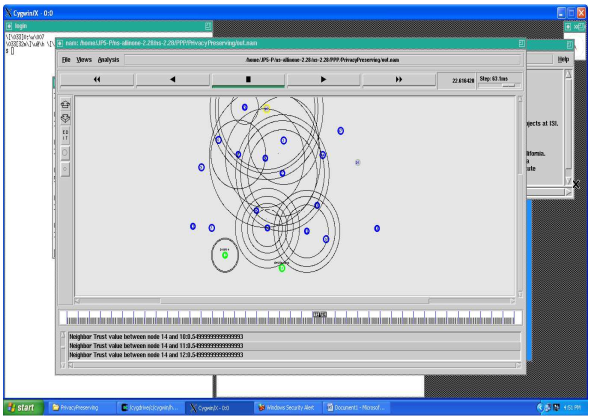

Fig.6 Enhanced Trust & HLA based public auditing architecture

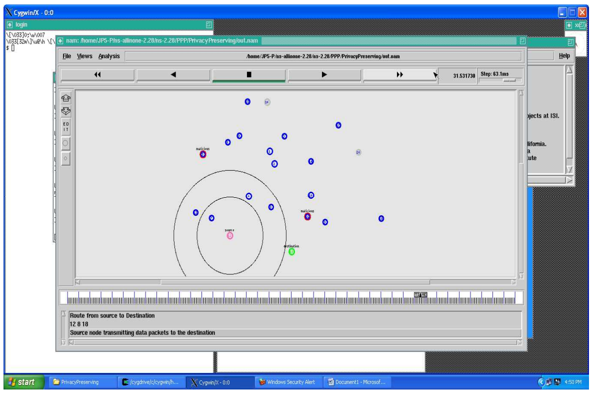

Fig .7 Detection of the malicious node using trust mechanism

B. SIMULATION RESULTS

We used the performance metrics to validate the proposed algorithm with results obtained in this papers are shown in Figure 6 and figure 7.

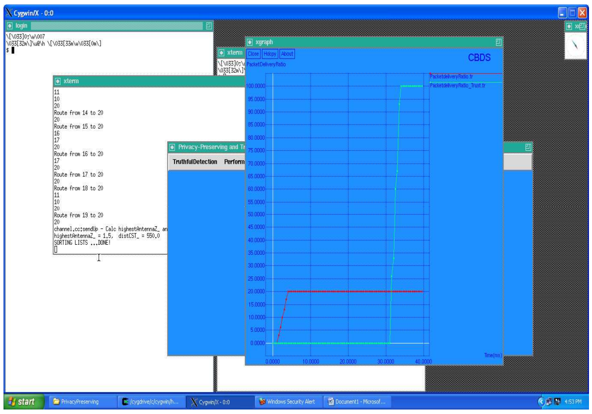

Fig. 8 Packet delivery ratio

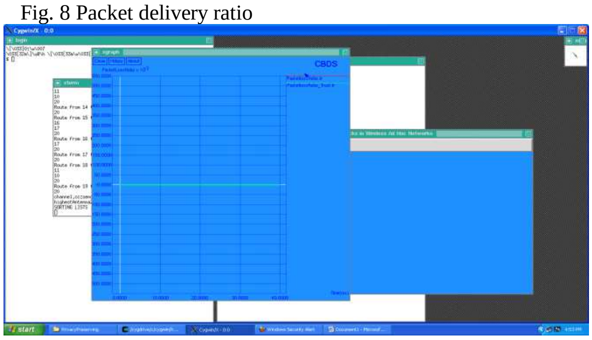

Fig. 9 Packet Loss

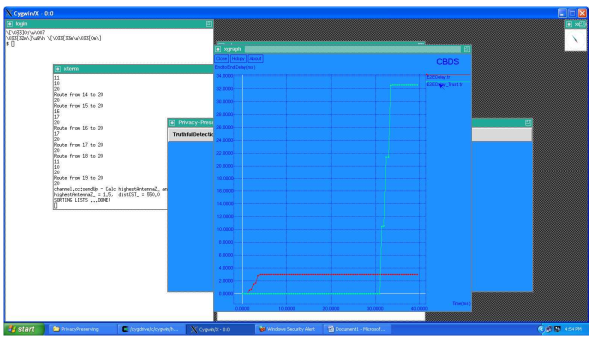

Fig. 10 Delay

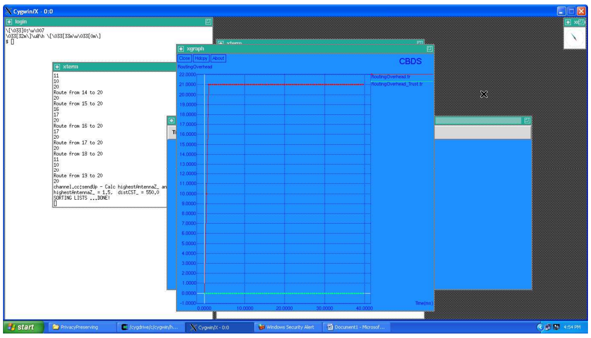

Fig. 11 Routing head

Thus the proposed scheme is very significant and effective when comparing with existing methods.

VIII. CONCLUSION

Mobile Ad hoc Network (MANET) is a type of Ad-hoc Network which changes its location dynamically and configures itself. MANET does not have a fixed topology which causes priorities to different kind of attacks. In this work, it deals with detection and prevention of packet dropping attack. Link error and malicious packet dropping are two sources for packet losses in wireless ad hoc network. In this paper, we propose a new routing mechanism to combat the common selective packet dropping attack based on associations between nodes are used to identify and isolate the malicious nodes through trust estimator. Simulation results show the effectiveness of our scheme compared with conventional scheme. This eliminates the overhead of invoking the trust estimator between companions. Further the overheads due to the calculations of trust relationship are minimal compared to the CONFIDANT protocol. In the experiment, proposed method is compared with HLA based auditing and experimental results show that enhanced trust based HLA outperforms existing method, which balances the packet delivery ratio, end to end delay, packet loss and routing overhead prolongs the function lifetime, and guarantees high QoS of MANET. In future work, we concentrate to prevent more attackers in MANET.

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling," Ph.D. dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004.

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.

[3] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[4] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[7] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[8] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[9] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[10] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003.

[11] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.

[12] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[13] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

[14] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[15] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in Ad Hoc Networking. Reading, MA, USA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[16] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.

AUTHOR PROFILE

RAYUDU SUDHEER is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Software Engineer). His Area of interest includes Mobile Computing and its objectives in all current trends and techniques in Computer Science & Engineering.

CH.SUBHASH M.TECH is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.