Trust-Based Cross-Layer Security Mechanisms against Attacks in MANETS

Dr.R.Naveen Kumar

Professor, Department of CSE

Vaagdevi College of Engineering

Warangal,Telangana,India

naveensmitha@gmail.com

Dr. V.Bapuji

Professor, Department of Computer Science

Vaageswari College of Engineering

Karimnagar,Telangana,India

bapuji.vala@gmail.com

ABSTRACT

 To increase the network efficiency among the different layers a cross-layer design concept is used to protect from various attacks. A trust based cross layer defense framework is designed to detect the vulnerability of attacks at different layers. A cross-layer attack is a collection of attack activities that are conducted coordinately in multiple network layers in order to achieve specific attack goals. A trust based packet forwarding scheme detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below trust threshold, the corresponding intermediate node is marked as a malicious. The experimental results show the proposed framework can efficiently minimize the attacks. A cross-layer attack is a collection of attack activities that are conducted coordinately in multiple network layers in order to achieve specific attack goals.

Keywords—Cross layer; Trust; IDS; MANETs; TCLS.

#  INTRODUCTION

 In Ad Hoc networks, secure routing protocols is one of the fundamental challenges. While many secure routing schemes focus on preventing attackers from entering the network through secure key distribution/authentication and secure neighbor discovery, trust management can guard routing even if malicious nodes have gained access to the network. Trust is a concept encountered in everyday life. In mathematical terms, trust has been defined as follows [1]. “Trust is a measure of probability with which an agent can assess a particular action performed by another agent or group of agents, both before the agent can monitor such action and which may in turn affects the agents own action.” The introduction of probability in the definition of trust makes trust more concrete than abstract-like as it has been defined in psychology and in sociology. Thus trust can now be measured with a mathematical model. Trust can be placed on or be represented with a probabilistic distribution with different values of expectations. This definition recognizes that trust is applicable where there is probability of distrust, betrayal, exit or defection [2]. Probabilistic distribution of trust can have a range of values from the lowest value representing distrust to the highest value representing trust.

**Trust Management:** A trust management approach used to set trust level for a route is based on the past behavior of a node. Trust is computed by direct neighbors according to past experience with a particular node or according to current observed behavior of a node. When a node behaves as it is expected trust increases, otherwise trust decreases. The current perception of trust management for network security was proposed [3]; a distributed trust management framework that first delved into the “trust management problem”, moving the idea of trust security away from simple third party certificating. The framework aimed to allow for flexibility to support trust relationships and localized control through binding public keys to access control without hard security authentication. This carried the idea that the subjective value of trust could be realized by each party/node within the network, rather than just on a global scale.

# DISCOVERY AND THE COMPUTATION OF TRUST

In distributed ad-hoc networks, trust levels are devised from the analysis of collected data from observations for specific actions [4]. This could include packet routing, where a node might observe the routing behavior of another node. It could log that a particular node forwards some packets as normal, and then drops other packets. It could receive this through direct neighbor sensing and calculate trust from direct experience [1].



Figure 1: Neighbor Sensing

Trust between immediate neighboring nodes is known as Direct Trust and is required for cases where a trust relationship is formed between two nodes without previous interactions (Figure 1).



Figure.2: Node Recommendation

It may also receive this information second hand through the form of recommendations Figure.2. This is transitive trust; known as Indirect Trust. From this a belief level can be calculated on the routing behavior of this node it received from other nodes.



Figure 3: Hybrid Approach

A node may use a hybrid of these two approaches Figure 3, such as would be seen in reputation based trust management approaches**.**

**Trust Aggregation** - As trust is propagated through the network, multiple accounts of trust for a single node will be received by a node. The different values of trust will be required to be aggregated in order to calculate a final value of trust. Advantages of this approach can be observed when a node requests information regarding the shortest routing path. If a node that is required to provide information misbehaves when that node is the only node requested to provide information, then incorrect information could be provided regarding the shortest routing path. However, if trust values are propagated by many nodes, to which the aggregation of these values is calculated, then the misbehaving node’s bad information should be repressed. This is considered to be composable trust*.* Peer-to-Peer networks offer good examples of Trust Aggregation.

**III. ATTACKS OF TRUST SCHEMES IN MANETS**

 The autonomous nature of the security decisions that derive from Trust computations mean that trust schemes can be the target of attacks themselves. The following are examples of attacks that can occur:

* **Bad Mouthing Attack:** In a bad mouthing attack a node might intentionally provide a bad recommendation of another node. Recommendation attacks without aggregation are usually affected where inaccurate recommendations are not compared with multiple observations [6].
* **Denial-of-Service Attack:** Attackers take advantage of trust propagation by consuming as much resources as possible by flooding an already resource conscious mobile network with trust recommendations. Trust schemes that don’t rely on trust propagation, such as neighbor sensing methods do not suffer from denial of service attacks.
* **On-Off Attack:** For the majority of the interactions and routing a node might behave correctly and where attacks occur only at opportunistic moments. The idea of adding context to transactions can be applied here. This might include a weighting to transactions depending on location or time where the weighting of the transaction might decrease over time [6]. Aggregation would then eventually provide a defense against such attacks.
* **Conflicting Behavior Attack:** Similarly to an on-off attack, when a node displays conflicting behavior where it provides differing recommendations about a node to different nodes. Over time the performance of the trust management system would degrade over time.

For the same reasons as an on-off attack, the performance of the system should remain if similar aggregation methods are deployed.

* **Camouflage Attack:** An attacker will provide recommendations based on the majority verdict, and then at times provide false information to degrade the trust scheme. Providing a greater service to honest nodes and heavily penalizing the dishonest nodes provides protection against such attacks [7].
* **Sybil and Newcomer Attacks:** A malicious node can create fake IDs that can take the blame for malicious actions or a node might create leave and re-join a network with a new ID and perform malicious attacks as a newcomer to the network [9]. Any trust scheme without a centralized administrative node is vulnerable to such attacks. Some of the research in social networks determined that defense against such attacks in those honest nodes and malicious nodes can be differentiated among the number of trust relationships established [8]. Particularly for newcomer attacks, trust metrics can be leveraged to reflect this, where in recommendation based systems new nodes or nodes with little previous trust relationship history can labeled as an unknown node.
* **Collusion Attack:** In recommendation trust schemes, a collusion attack consists of more than one node collaborating to provide false information regarding a normal honest node. Neighbor sensing and hybrid approaches that utilize direct trust are usually immune to such attacks. Reducing the recommendation field has been considered to reduce attacks where recommendations are confined to neighboring nodes enabling behavior changes to be identified [9],[22].

 In this work a Trust-Based Packet forwarding scheme in MANETs is proposed, which does not use any centralized infrastructure. For Ad Hoc routing the associated trust values are investigated with two actions forwarding packets and making recommendations. Each node maintains its trust record associated with these two actions. When a node (source) wants to establish a route to the other node (destination), the source first tries to find as many routes as possible to the destination.

**IV. TRUST MANAGEMENT SYSTEMS AND ITS APPLICATIONS IN AD HOC NETWORKS**

 In this work, a comprehensive framework of trust management for distributed networks is considered, as illustrated in Figure 4 [10].

****

Figure 4: Trust Management for Distributed Networks

 This framework contains five basic building blocks. *Trust record* is constructed through the *trust establishment* process, which builds direct trust values from observations and indirect trust values form recommendations, and updated by the *record maintenance* process, which assigns initial trust values and addresses dynamic properties of trust

 *Trust requests management* serves as the interface between applications that request trust values and trust management. It also handles the requests for trust recommendations. In addition, *malicious node detection* is performed based on trust record and its output also affects some entries in the trust record. This framework can be used in a variety of applications, such as Ad Hoc networks, peer-to-peer networks, and sensor networks. To demonstrate its usage, the implementation of such a framework in Mobile Ad Hoc Networks was presented [10].

There are three primary aspects associated with evaluating trust in distributed networks.

* The ability to evaluate trust offers an incentive for good behavior. Creating an expectation that entities will “remember” one’s behavior will cause network participants to act more responsibly.
* Trust evaluation provides a prediction of one’s future behavior. This prediction can assist in decision-making. It provides a means for good entities to avoid working with less trustworthy parties. Malicious users, whose behavior has caused them to be recognized as having low trustworthiness, will have less ability to interfere with network operations.
* The results of trust evaluation can be directly applied to detect selfish and malicious entities in the network.

**V. RELATED WORK**

 A “Secure Routing and Intrusion Detection in Ad Hoc Networks*”* based on AODV over IPv6 was proposed [9]. The Security features in the routing protocol contain mechanisms for non-repudiation and authentication that does not require a Certificate Authority (CA) or a Key Distribution Center (KDC) to be available. AODV and IDS was proposed to detect and thwart malicious attacks [11]. The IDS is independent of the routing protocol, though in this case SecAODV for routing was used. The routing protocol has the ability to create and maintain routes.

The protected network was still vulnerable to packet mangling attacks, routing disruption attacks, denial of service attacks and grey holes that use MAC vulnerabilities to disrupt communication were still possible.

 Host Based IDS mechanism deployed on a mobile device had a limitation on the radio ranges. The implementation of collaborative IDS offered a collective response to misbehaving or intrusive nodes. In addition to using thresholds the work used signal strengths of neighboring nodes for detecting misbehaving nodes. The distance of the neighboring nodes can be determined by the mow quality signal and can be used to make a decision of the node’s misbehavior or the accessibility in a certain range. The selection of nodes to monitor is helpful to check the accuracy of the IDS in terms of scalability and detection.

 “A Node misbehavior detection Mechanism for Mobile Ad Hoc Networks” was proposed [12]. The authors concentrated on the detection phase and proposed a mechanism known as Packet Conservation Monitoring Algorithm (PCMA), which is used to detect selfish nodes in MANETs. Two scenarios were given to illustrate how the new algorithm works. PCMA succeeded in detecting selfish nodes which perform full/partial packets attack.

 This work also tried to classify types of partial dropping attack, in order to differentiate between this attack and the need for some nodes to drop part of their packets because of error checking or congestion. This can be done by setting certain threshold in which the node is considered selfish if it exceeds it.

 “Vulnerabilities of Intrusion Detection Systems in Mobile Ad Hoc Networks - The routing problem” was proposed [13]. The possible attacks against the routing system were reviewed, and some of the IDSs proposed. Routing system is the most vulnerable point from Mobile Ad Hoc Networks. This vulnerability implies a risk of Denial-of-Service attacks against certain nodes, or even the whole network, is high. Furthermore, this risk is not acceptable in those scenarios which are more susceptible to implement Mobile Ad Hoc Networks such as those exposed in the introduction: battlefield, and establishing communications after natural disasters.

 “A Secure Incentive Protocol for Mobile Ad Hoc Networks” was proposed [14]. The proper functioning of Mobile Ad Hoc Networks depends on the hypothesis that each individual node is ready to forward packets for others. This common assumption, however, might be undermined by the existence of selfish users who are reluctant to act as packet relays in order to save their own resources. Such non-cooperative behavior would cause the sharp degradation of network throughput. SIP can be implemented in a fully distributed way and does not require any pre-deployed infrastructure. In addition, SIP is immune to a wide range of attacks and is of low communication overhead by using a Bloom filter.

 An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs also known as 2ACK scheme was proposed [15]. The scheme was used as an add-on technique by routing schemes to detect misbehavior of nodes in routing formation and access the adverse effect created. The 2ACK scheme sends two-hop acknowledgment packets in the reverse direction of the routing path. The additional routing overhead can be reduced by sending acknowledgements for a fraction of the received data packets.

 The focus was on link misbehavior [15]. The study on the behavior of a single node was difficult due to the fact that communication takes place between two nodes. Therefore, the decision of punishing any node associated with the misbehaving links is to be done carefully. If either of the two nodes associated with the link misbehaving, the link misbehavior can be detected. The study of behavior of links is useful to draw decisions of punishing a node and is a potential direction for the present work.

 The security problems and attacks that exist in routing protocols were explored [16]. The design and analysis of a secure on-demand routing protocol, called RSRP which tries to overcome the problems mentioned in the existing protocols was proposed. The broadcast mechanism used in RSRP does not require clock synchronization and facilitates instant authentication.

 An approach based on the relationship between the nodes to make them to cooperate in an Ad Hoc environment was proposed [17]. The trust values of each node in the network are calculated by the trust units. The relationship estimator has determined the relationship status of the nodes by using the calculated trust values. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the network simulator-2.za

 A trust based framework to improve the security and robustness of Ad Hoc network routing protocols was proposed [18]. For constructing their trust framework they have selected the Ad Hoc on demand Distance Vector (AODV) which is popular and used widely. Making minimum changes for implementing AODV and attaining increased level of security and reliability is their goal. The schemes were based on incentives & penalties depending on the behavior of network nodes. Their schemes incur minimal additional overhead and preserve the lightweight nature of AODV.

 A possible framework of a Link Level Security Protocol (LLSP) for deployment in a Suburban Ad Hoc Network (SAHN) was proposed [19]. The authors have analyzed various security aspects of LLSP to validate its effectiveness. To determine LLSP's practicability, the authors have estimated the timing requirement for each authentication process. Their initial work has indicated that LLSP is a suitable link-level security service for an Ad Hoc network similar to a SAHN.

 The security issues of wireless sensor networks were explored, and an efficient link layer security scheme was proposed [20]. To minimize computation and communication overheads of the scheme, a lightweight CBC-X mode Encryption/Decryption algorithm was designed which attained Encryption/Decryption and Authentication all in one. A novel padding technique was also designed, enabling the scheme to achieve zero redundancy on sending Encrypted/Authenticated packets. As a result, security operations incur no extra byte in their scheme.

**VI. OBJECTIVES & OVERVIEW OF THE PROPOSED PROTOCOL**

 In this work a refinement is proposed to Trust-Based Cross-Layer Security Protocol (TCLS) [14]. Confidentiality and Authentication of packets is obtained in both routing and link layers of MANETs and is desired to have the following objectives:

* **Light-Weight –** The use of Symmetric Key algorithms and cryptography based hash functions helps to extend the network lifetime.
* **Co-Operative –** The high level security mechanisms use mutual collaboration/cooperation between the nodes.
* **Attack-Tolerant –** The network resistant to attacks and has the ability to heal since it can detect and eliminate the sources of attacks.

**VII. OVERVIEW OF THE PROTOCOL**

 The proposed Trust based packet forwarding scheme in MANETs does not use any centralized infrastructure. For Ad Hoc routing, the trust values associated with two actions such as forwarding the packets and making recommendations based on trust were investigated. Each node maintains its trust record associated with these two actions. When a node (source) wants to establish a route to the other node (destination), the source first tries to find multiple routes to the destination. Then the source tries to find the packet-forwarding trustworthiness of the nodes on the routes from its own trust record or through requesting recommendations. Finally the source selects the trustworthy route to transmit data. After the transmission, the source node updates the trust records based on its observation of route quality.

 The trust records are also used for malicious node detection. All the above is achieved in a distributed manner. The trust values associated with a Trust Counter (TC) is used to favor packet forwarding for every node. A node can be punished or rewarded by increasing or decreasing the trust counter values for each node. Each intermediate node adds its hash value (also known as MAC) and forwards the packet to the destination node. The destination node can increment or decrement based on the verification of hash value received. After decrementing, if the trust counter value is found to be below a trust threshold, then the corresponding intermediate node can be marked as malicious.

 This scheme does not require any pre-deployed infrastructure and can provide a solution to the selfish behavior of nodes. The focus was on the Propagating Cipher Block Chaining (PCBC) mode Encryption/Decryption algorithm to satisfy the necessity of minimum computational and communication overhead. This algorithm supports Encryption/Decryption and Authentication of packets on a one-pass operation. The upper layers of the protocol stack are provided with security services obviously.

 A PCBC mode symmetric key mechanism is devised to employ link layer security system. Encryption/Decryption and authentication operations are included into a single step which reduces the computational overhead to half, instead of calculating them individually. The padding technique used states that this method has no cipher text expansion for the transmitted data payload. Thus the communication overhead can be reduced significantly.

**VIII. EFFICIENT MAC LAYER SECURITY PROTOCOL & TRUST-BASED FORWARDING SCHEME**

 In the proposed protocol, the nodes trust counter values are calculated dynamically. The source node can select one or more trusted routes instead of selecting the shorter routes. The malicious nodes are isolated from participating in the network and the affect of malicious nodes will be reduced. The AODV routing protocol is modified as follows:

Each node on the network maintains an additional data structure namely *Neighbors’ Trust Counter Table (NTT)*

|  |  |  |
| --- | --- | --- |
| **Node** | **Trust counter(Tc)** | **No. of packets forwarded thru (FC)** |

Figure 5: Structure of NTT

Let {$T\_{c\_{1}},T\_{c\_{2}},…\}$ denote the initial trust counters of the nodes {$n\_{1},n\_{2},…\}$ for a route R1 formed between a source node, S to the destination node, D. Initially a node is not aware of the trust reliability of its neighbors. The source S sends a RREQ packet to the destination to form a route. The number of packets forwarded by a node through a route is calculated using a forward counter (FC). When a node $n\_{k}$receives a packet from a node $n\_{i}$, then the node $n\_{k}$,increases the forward counter of node$ n\_{i}$.

$ FC\_{n\_{i}}= FC\_{n\_{i}}+ $ 1 $i=1,2,…..$ (1)

The NTT of node $n\_{k}$is modified accordingly with the values of $FC\_{n\_{i}}$.

 This process is similar for all the nodes to determine NTT. The destination D now, measures the number of packets received (Prec.) after the accumulated RREQ message is received. *A* MAC on Prec.is computed usingthe shared key of the sender and the destination. The digitally signed RREP packet consists of the source and destination ids, the MAC value, the accumulated route from the RREQ. The RREP is sent back to the source using the reverse route towards R1. The RREP packet is then checked at each intermediate node from D to S. The success ratio for ever node is computed as,

$ SR\_{i= }FC\_{n\_{i}}/Prec $ (2)

 The FC values for a node $n\_{i}$can be obtained from the NTT of that node. The success ratio value $SR\_{i}$is then appended to the RREP packet.

 The digital signature of the destination node is stored in the RREP packet and verified at each intermediate node. If the verification succeeds, it is signed and forwarded to the next node in the reverse route otherwise the RREP packet is dropped. After the RREP packet is reached at the source S, verification is done to check, the first id of the route stored by the RREP is its neighbor. If the verification succeeds, then all the digital signatures of all the intermediate nodes are verified, in the RREP packet. The verification process is conducted by the intermediate node by verifying the digital signature and the MAC stored in the RREP packet. If the verification fails, the RREP packet is dropped. Otherwise further signed by the intermediate node and reverted back from destination to source in a previous manner. If the verification process of the digital signature by the intermediate node i.e. contain in RREP is successful, then trust counter is incremented as

$T\_{C\_{i}}= T\_{C\_{i}}+ δ\_{1}$ (3)

 If the verification fails then trust counter is decremented as

$ T\_{C\_{i}}= T\_{C\_{i}}- δ\_{1}$ (4)

Where

 $δ\_{1}$ is the small fractional step value. After the completion of verification stage, the source S checks the success ratio values $SR\_{i}$ of the node $n\_{i}$. For any node $n\_{k}$, if $SR\_{k}< SR\_{min}$, where $SR\_{min}$ is the minimum threshold value, its trust counter value is further decremented as

 $T\_{C\_{i}}= T\_{C\_{i}}- δ\_{2}$ (5)

If $SR\_{k}> SR\_{min}$, the trust counter values for all other nodes are incremented as

 $T\_{C\_{i}}= T\_{C\_{i}}+δ\_{2}$ (6)

Where

 $δ\_{2}$ is a small step value (0.25) such that $δ\_{2}< δ\_{1}$ .

if $T\_{C\_{k}}< T\_{C\_{thr}}$ , where $T\_{C\_{thr}}$ is the threshold value, then the node $n\_{k}$ is considered as malicious.

 A route breakage or failure may occur when the source does not get the RREP packet after a time period of t seconds. Then the route discovery process can be again initiated by the source.

 The routes R2, R3, etc. also use the similar procedure to select a route which do not contain a malicious node or a route with least number of malicious nodes. Such a route is considered as the reliable route. The proposed work can be efficient and more secure, since authentication is performed for route reply operation. The cryptographic computations are performed by the nodes which are stored in the current route.

**IX. PCBC MODE**

 The proposed approach replaces the link layer security scheme adapted to the packet format [21]. But the encryption and decryption mechanisms are different. It works between the link layer and the radio layer. The proposed method encrypts the data and computes the MAC, when the application data payload is passed from the link layer to the radio layer. With the help of the radio channel, the encrypted message is sent out bit-by-bit. Confidentiality and authentication are the of security services which are present in the proposed packet format.

The packet format of the proposed scheme is illustrated in Figure 6. The fields of the packet are the Destination Address Field (Dest), Active Message Type Field (A), and the Length Field (L), Group Field (G), Random Number Mode Field (Ran), Data Field (Data) and MAC field.

 A one byte group field is used in the proposed scheme to make it general and applicable. It also uses a 4 byte MAC field since it can provide enough security of integrity and authenticity for the Mobile Ad Hoc Networks. Any error alteration during message transmission can be detected by re-computing the MAC and the error message would be discarded to improve efficiency.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dest2 | A1 | L1 | G1 | Ran3 | Data(0-29) | MAC4 |

Figure 6: Packet Format

 In this scheme, the generic communication interfaces are given to the upper layer and uses the lower radio packet interfaces. The nodes in the communication are not conscious of the operations on encryption/authentication because the security services are given clearly.

 To make the scheme easier, the encryption and authentication for every packet is carried out by the default mode in a single pass. In order to finish the message authentication and encryption concurrently before sending message, an authentication and encryption scheme is built and called as PCBC mode.

**PCBC Mode Operations**

 The Propagating Cipher-Block Chaining (PCBC) mode is used to cause small changes in the cipher text to propagate indefinitely when decrypting, as well as when encrypting. The PCBC mode is designed to extend or propagate a single bit error in the cipher text. The transmission errors can be captured and the resultant plaintext can be rejected. The Encryption is given by

**

as shown in Figure 7, where p0  c0is the initialization vector (IV), Ci is the cipher text in ith round, Pi is plain text in ith round , and $⊕ $is the XOR operation.



Figure 7: Propagating Cipher Block Chaining (PCBC) Mode Encryption

The method of decryption is given by



as shown in Figure 8, where P0$ ⊕$*C*0 is the initialization vector (IV).



Figure 8: Propagating Cipher Block Chaining (PCBC) Mode Decryption

X. SIMULATION MODEL AND PARAMETERS

 The simulations in the proposed algorithm are obtained by using Network Simulator 2 (NS2). In the simulations, the channel capacity of mobile hosts is set to 2 Mbps. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In the simulations, 100 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. Each node is assumed to move independently with the same average speed. All nodes have the same transmission range of 250 meters. The speed(s) is varied from 10 m/s to 50m/s. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in Table 2.

Table 1: Simulation Parameters

|  |  |
| --- | --- |
| No. of Nodes | 100 |
| Area Size  | 1000 X 1000 |
| MAC  | 802.11 |
| Radio Range  | 250m |
| Simulation Time  | 50sec |
| Traffic Source  | CBR |
| Packet Size  | 512 |
| Mobility Model  | Random Way Point |
| Speed | 10,20,30,40,50,60 m/s |
| Pause time | 5 |

**Performance Metrics**

The performance is evaluated according to the following metrics.

**Control overhead:** The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

**Average end-to-end delay:** The end-to-end delay is averaged over all surviving data packets from the sources to the destinations.

**Average Packet Delivery Ratio:** Ratio of the number of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next section. The TCLS protocol is compared with the LLSP [21] protocol in presence of malicious node environment.

**XII. RESULTS BASED ON ATTACKERS**

 In the first experiment, the number of misbehaving nodes is varied as 10, 20, 30, 40, 50 and 60. The use of trust mechanism for nodes behavior in TCLS improves the average delivery ratio of packets as given in figure 3.4. When the number of malicious nodes is 10 the delivery ratio is 0.8 and as the number of malicious nodes increases to 20, 30, 40, 50 and 60 there is a chance of the attackers being increased. So the delivery ratio starts dropping down.



Figure 9: Attackers Vs Delivery Ratio

With the use of trust management approach it can be observed from the Figure 9, the results obtained for average packet delivery ratio for the misbehaving nodes 10, 20, 30, 40, 50, 60 that the TCLS scheme achieves more delivery ratio than the LLSP scheme since it has both reliability and security features. The delivery ratio remains constant even the no of attackers increased from 50 to 60.

**Based on Speed**

 In the second experiment, the speed is varied as 10, 20, 30, 40, 50 and 60 m/s with 5 attackers. The use of trust mechanism for nodes behavior in TCLS improves the average delivery ratio of packets as given in Figure 9. The number of misbehaving nodes is 5 which is maintained as constant and the speeds 20, 30, 40, 50, 60 for the 100 nodes the TCLS scheme achieves more delivery ratio than the LLSP scheme since it has both reliability and security features. With the use of trust management approach it can be observed from the Figure 10, the results are obtained for average packet delivery ratio for the misbehaving nodes 10, 20, 30, 40, 50, 60.

 The TCLS scheme achieves more delivery ratio than the LLSP scheme since it has both reliability and security features and the delivery ratio remains constant even though the speeds are increased from 40 to 60 m/s.



Figure 10: Speed Vs Delivery Ratio



Figure 11: Speed Vs Delay

 In the second experiment, the speed is varied as 10, 20, 30, 40, 50 and 60 m/s with 5 attackers. The use of trust mechanism for nodes behavior in TCLS improves the of average end-to-end delay as given in Figure 11. The number of misbehaving nodes is constant and the speeds are varied as10, 20, 30, 40, 50 and 60 m/s for the 100 nodes.

 The TCLS scheme has slightly lower delay than the LLSP scheme because of authentication routines and still the simulations show that the increase of speed from 30 to 60 m/s is not going to affect the delay and it remains constant.

**XIII. SUMMARY**

 In this work, a framework was presented to enhance the Trust-Based Cross-Layer protocol which quantitatively measures trust, model propagation of trust. The trust evaluation systems can defend against malicious attacks. Defense techniques are developed based on the identification of attacks against the trust systems. Use of the proposed trust evaluation system ensures security in Ad Hoc networks by establishing secure routing and assisting in malicious node detection. The distributed concept of the proposed system can significantly improve throughput in the network and effectively detect malicious behaviors in Ad Hoc networks.

[1]. A. A. Pirzada and C. Mcdonald, *“Trust Establishment in Pure Ad Hoc Networks,”* *Wireless Personal Communications*, vol. 37, no. 1-2, pp. 139-168, Apr. 2006.

[2]. D. Gambetta’ *“Can we trust trust?,”* in D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, chapter 13, pages 213.237. Department of Sociology, University of Oxford, electronic edition, 2000.

[3]. M. Blaze, J. Feigenbaum, and J. Lacy, *“Decentralized trust management,” in Security and Privacy, 1996. Proceedings.,” IEEE Symposium on*, 1996, pp. 164–173, 1996.

[4]. S. Marsh, “*Formalizing Trust as a Computational Concept*,” PhD thesis, University of Stirling, Uk, 1994.

[5]. A.Rajaram and Dr.S.Palaniswami *“A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks,”* in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

[6]. P. Michiardi, *“Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,”* *Proceedings of the IFIP TC6/TC11 Sixth*, pp. 107–121, 2002.

[7]. Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, *“Attacks on trust evaluation in distributed networks,”* in *Information Sciences and Systems, 40th Annual Conference* , pp. 1461–1466, 2006.

[8]. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, *“The eigen trust algorithm for reputation management in p2p networks,”* in *Proceedings of the 12th international conference on World Wide Web*, pp. 640–651, 2003.

[9]. Reddy DS, Bapuji V, Govardhan A, et al. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In: 2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET), Chennai, India, 16–18 February 2017, pp.1–5. New York: IEEE

[10]. P. Velloso, R. Laufer, D. D. O. Cunha, O. C. Duarte, and G. Pujolle, *“Trust management in mobile ad hoc networks using a scalable maturity-based model,”* *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172-185, Sep. 2010.

[11]. A. Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha “*Threshold-based Intrusion Detection in Ad hoc Networks and Secure AODV*” Elsevier Science Publishers B. V., Ad Hoc Networks Journal (ADHOCNET), June 2008.

[12]. Tarag Fahad and Robert Askwith *“A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks*”, in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[13]. Ernesto Jiménez Caballero*,“Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem”,* 2006*.*

[14]. Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang*, “A secure incentive protocol for mobile ad hoc networks”,* Wireless Networks(WINET), vol 13, No. 5, October 2007.

[15]. Liu, Kejun Deng, Jing Varshney, Pramod K. Balakrishnan and Kashyap “*An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs*”, IEEE Transactions on Mobile Computing, May 2007.

[16]. Afzal, Biswas, Jong-bin Koh,Raza, Gunhee Lee and Dong-kyoo Kim, *"RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks",* in proceedings of IEEE Conference on Wireless Communications and Networking, pp.2313-2318, April 2008.

[17]. Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam, *"Trust Enhanced Dynamic Source Routing Protocol for Ad hoc Networks*", in proceedings of World Academy of Science, Engineering and Technology, Vol. 36, pp.1373-1378, December 2008.

[18]. Meka, Virendra, and Upadhyaya*, "Trust based routing decisions in mobile ad-hoc networks*" in Proceedings of the Workshop on Secure Knowledge Management, 2006.

[19]. Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, *"A Link Layer Security Protocol for Suburban Ad-Hoc Networks",* in proceedings of Australian Telecommunication Networks and Applications Conference, December 2004.

[20]. Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou and Kefei Chen *"Efficient Link Layer Security Scheme for Wireless Sensor Networks",* Journal of Information And Computational Science, Vol.4, No.2,pp. 553-567, June 2007.

[21]. Chin-Yang Henry Tseng, *“Distributed Intrusion Detection Models for Mobile Ad Hoc Networks,”* University of California at Davis Davis, CA, USA, 2006.

[9]. Reddy DS, Bapuji V, Govardhan A, et al. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In: 2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET), Chennai, India, 16–18 February 2017, pp.1–5. New York: IEEE

[22]. Haifeng Yu et al, “*Defense against Sybil Attacks via Social Networks*”, SIGCOMM 2006, Pisa, Italy, September, 2006