# TRUST-BASED CROSS-LAYER SECURITY MECHANISMS AGAINST ATTACKS IN MANETS

## 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.

## Authors

**Dr.R.Naveen Kumar**
Assistant Professor
Department of CSE
Vaagdevi Engineering College
naveensmitha@gmail.com

**Dr. V.Bapuji**
Professor, Department of CSE
Vaageswari College of Engineering
Karimnagar, Telangana,India
bapuji.vala@gmail.com

## I. INTRODUCTION

Security is one of the main issues in Mobile Ad Hoc Networks. Although there are many security routing schemes that aim to prevent attackers from entering the network through key security/authentication and security proximity detection, Trust can intercept traffic even if malicious individuals have entered the network. Trust is a concept that we encounter in daily life. Mathematically, trust is defined as [1]. "Confidence is the measure of the probability that an agent will evaluate a particular behavior performed by another agent or agents in a way that may affect the agent's behavior, without the agent following such a pattern of behavior”. Therefore, reliability can now be measured with mathematical models. Confidence can be placed or represented by a probability associated with different outcomes. This definition recognizes that trust applies to situations where there is a possibility of distrust, betrayal, withdrawal, or separation [2]. The probability distribution for confidence can have a range of values, from the lowest value representing skepticism to the highest value representing confidence.

1. **Trust Management:** The trust management method used to set the trust of the path is based on the past behavior of the nodes. Confidence is calculated by close neighbors based on a node's previous experience or the node's current behavior. Trust increases when nodes behave as expected, otherwise trust decreases. Present the current view of trust management in network security [3]; part of religious administration, first of all, to delve deeper into the "management problem" and move the concept of religious security away from simple third-part certification. The framework is designed to support the relationship between trust and local control by linking public keys to access control without requiring complex authentication. This means that the trust value is visible to every party/node in the network, not globally.

## II. DISCOVERY AND COMPUTATION OF TRUST

In distributed ad hoc networks, trust is established by analyzing data collected from the analysis of specific tasks [4]. This may include packet routing, where one node can observe the behavior of another node.

It can be written that one of the normal sends some packets and leaves some. It can take this knowledge directly from community experience and involve trust based on direct experience [1]

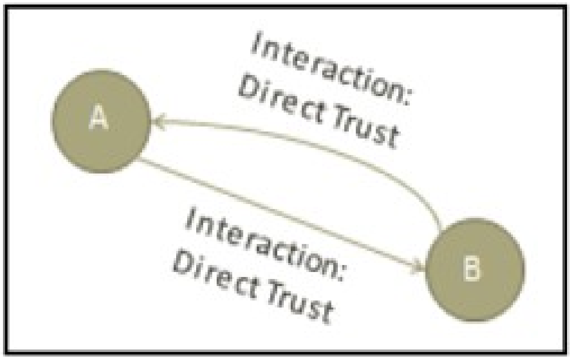

**Figure 1:** Neighbor Sensing

Awareness Trust between close neighbors is called direct trust and is appropriate for the situation where there is a trust relationship between two nodes without being affected first (Figure 1)

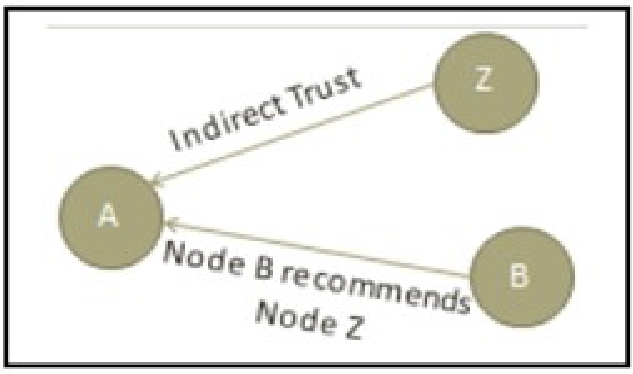

**Figure.2:** Node Recommendation

It is also possible to receive this information as a second recommendation as shown in Figure 2. This is transitive confidence and also called implicit trust. Confidence can be calculated from the node's behavior received from other nodes.

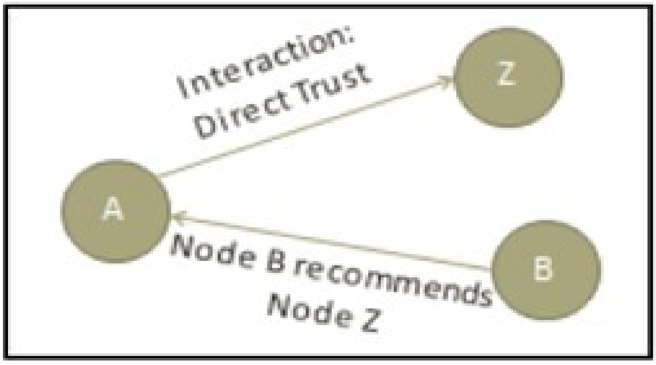

**Figure 3:** Hybrid Approach

In hybrid approach nodes can use a combination of the two approaches as shown in Figure 3, such as reputation, for trust management.

1. **Trust Aggregation** - As trust spreads across the network, a node will gain more trust in each other. Different confidence values must be added to calculate the final confidence value. The advantage of this approach can be seen when a node requests information about the shortest path.

   If the requested node misbehaves when it is the same as the requested node, it will give false information about the shortest routing path. However, if reliability results are presented by many nodes and the sum of these results is calculated, negative information from the negative side should be prohibited. This is considered a trust. Peer-to-peer networks provide a good example of trust.

## III. ATTACKS OF TRUST SCHEMES IN MANETS

"The fact that security decisions are independent of trust means that trust itself can be targeted for attack. The following are examples of attacks that can occur:

1. **Bad Mouthing Attack (BMA):** 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].

2. **Denial-of-Service (DoS) Attack:** Attackers use trust advertising to exploit as much as possible, safely flooding already resource-sensitive mobile networks. Trust strategies that do not rely on trust reporting, such as neighbor-aware routing, prevent denial-of-service attacks.

3. **On/Off Attack:** Nodes can behave correctly for most interactions and paths, and attacks only occur at random times. The idea of adding content to the business can be used here. This may include the weight of changes based on location or time, where the weight of change will decrease over time [6]. Aggregation will ultimately protect against such attacks.

4. **Conflicting Behavior Attack:** Similar to switching, different nodes provide different input when they see conflicting behavior. At the same time, the performance of trust management degrades over time. For the same reason as the change, the operation of the system should remain the same if a similar mounting method is used,

5. **Masquerade Attack:** The attacker generally makes judgmental advice and then sometimes gives false information to undermine trust. Better service to honest people and heavy fines to dishonest people can prevent these attacks [7].

6. **Sybil/ Newcomer Attacks:** Malicious nodes can create false identities, be responsible for malicious activities, or perform malicious attacks as newcomers to the network by leaving and rejoining the network with new identities [9]. Any trust strategy without a central authority is vulnerable to such attacks.

7. **Collusion Attack:** Reliably, collusion attack consists of many cooperating to provide false information about honest nodes. Neighbor awareness and cooperation using direct trust often prevents attacks. Reducing consensus response is believed to reduce opposition when consensus is limited to neighbors and allows behavior change [9], [22]". "#

In this work, trust-based packet forwarding in MANETs is proposed without using centralized protocols. Check reliability results by forwarding packets and making recommendations for Ad Hoc forwarding. Each node holds trust information about these two functions. When a node (destination) wants to establish a path to another node (destination), the node first tries to find as many paths to the destination as possible.

.

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

In this study, a general framework for network trust management is shown in Figure 4 [10].

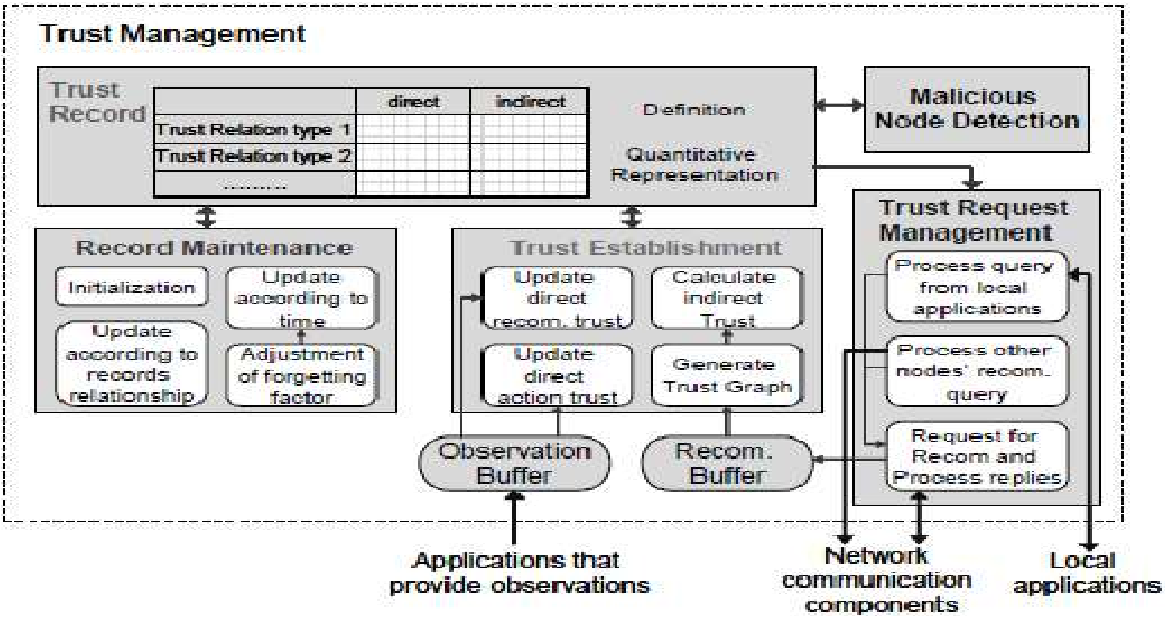
Trust Management
Trust Record
direct
indirect
Trust Relation type 1
Trust Relation type 2
………
Definition
Quantitative Representation
Malicious Node Detection
Trust Request Management
Record Maintenance
Initialization
Update according to time
Update according to records relationship
Adjustment of forgetting factor
Trust Establishment
Update direct recom. trust
Calculate indirect Trust
Update direct action trust
Generate Trust Graph
Process query from local applications
Process other nodes' recom. query
Request for Recom and Process replies
Observation Buffer
Recom. Buffer
Applications that provide observations
Network communication components
Local applications

**Figure 4:** Trust Management for Distributed Networks

“#The framework consists of five building blocks. Trust data is generated by the trust-building process, which produces direct results from observations and indirect trust from recommendations, and is replaced by standard management information that establishes initial trust and addresses the dynamic characteristics of trust, it also works on requests. Additionally, vulnerability detection is based on reliable data, and its results may also reflect some entries in trusted data.

The framework can be used for many applications such as Ad Hoc networks, peer-to-peer networks, and sensor networks. To demonstrate its implementation, a method is proposed to use such a framework in mobile ad hoc networks [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]. Security features in the regulatory framework include non-denial and authentication mechanisms that do not require a certificate authority (CA) or a Key Distribution Authority (KDC). AODV and IDS have been proposed to detect and block malicious attacks [11]. Although this example uses SecAODV to work, the IDS are not communication independent. Routing protocols can create and manage routes. "#

Defense networks are also vulnerable to packet disruption attacks, interception attacks, denial of service attacks, and gray hole attacks that use MAC vulnerabilities to attack communication"#. .

Host-based IDS mechanisms deployed to mobile devices have radio limitations. The implementation of a collaborative IDS provides a coordinated response to nodes misbehavior or disruption. In addition to using the threshold, this function also uses the signal strength of the neighbors to detect faulty nodes. "# "#The distance between adjacent nodes can be determined by signal quality shearing and can be used to determine the negative direction of nodes or reachability in a place. Selecting the nodes to monitor helps the IDS audit detect and detect the truth. "#

"#A Node misbehavior detection mechanism for Mobile Ad Hoc Networks was proposed [12]. Focusing on the detection phase, the authors proposed a method called Packet Protection Tracking Algorithm (PCMA) to perform the identification of MANETs. Two scenarios are given to illustrate how the new algorithm works. PCMA intelligently detects dirty nodes performing full/partial packet attack. "#

This task also attempts to identify the type of partial drop to distinguish it from situations where some nodes have to partially drop packets due to control errors or collision. This can be done by setting a threshold at which a node is considered selfish.

.

"# Vulnerabilities of Intrusion Detection Systems in Mobile Private Networks - Routing Problem was proposed [13]. Possible attacks against the system have been analyzed and some IDSs have been proposed. Communication is most convenient in a mobile ad hoc network. Vulnerability means there is a high risk of denial of service against part or even the entire network. Also, this risk is unacceptable in situations where it is easier to use mobile ad hoc networks, such as the situations that occurred in the Introduction: combat fire, post-natural disaster communication. "#

"A Secure Incentive Protocol for Mobile Ad Hoc Networks" was proposed [14]. The efficiency of mobile ad hoc networks depends on the assumption that each individual is ready to send packets to other nodes. However, this assumption may be affected by the presence of selfish users who refuse to track packet transits to save their own resources. This uncooperative behavior can cause a drop in network connectivity. SIP can be used as a fully distributed system without the need for any pre-implemented protocols. Also, SIP provides protection against various attacks and communication load is low using Bloom filter.

“#An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs also known as 2ACK scheme was proposed [15]. This method is used as an additional method to routing to identify poor behavior of nodes in the design path and poor quality of the visit. The 2ACK scheme sends two-hop acknowledgment packets on different routing paths. The additional routing overhead can be reduced by sending acknowledgment to a small fraction of received packets. “#

The focus was on link misbehavior [15]. Since communication takes place between two nodes, learning each other's behavior is difficult. Therefore, the decision to punish a person associated with an incorrect link must be made carefully. If two of the two associated with the link are displaying bad behavior, the bad behavior of the link can be detected. Studying link behavior helps to decide on penalty nodes and is a guide for current study.

Investigates the security problems and attacks that exist in routing protocols were [16]. Since communication takes place between two nodes, learning each other's behavior is difficult. Therefore, the decision to punish a person associated with an incorrect link must be made carefully. If two of the two associated with the link are displaying bad behavior, the bad behavior of the link can be detected. Studying link behavior helps to decide on penalty nodes and is a guide for current study.

An approach based on the relationship between the nodes to make them to cooperate in an Ad Hoc environment was proposed [17]. The confidence value of each part of the network is calculated with confidence. The relationship estimator determines the relationship between nodes using a confidence value. The development process was compared with the standard DSR protocol and the results were 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]. To increase their confidence, they chose the popular and widely used Optional Ad Hoc Distance Vector (AODV). Their purpose is to use AODV with minimal modification and to increase the level of security and reliability. The plan is based on incentives and penalties based on the behavior of network nodes. Their strategy includes minimal overhead and maintains the weight 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 analyzed various security features of LLSP to confirm its effectiveness. To determine the effectiveness of LLSP, the authors estimate the time required for each authentication process. Preliminary studies show that LLSP is a link-level security service suitable for Ad Hoc networks similar to SAHN.

The security issues of wireless sensor networks were explored, and an efficient link layer security scheme was proposed [20]. To reduce the computational and communication overhead of the schema, a lightweight CBC-X type encryption and decryption algorithm is designed, which integrates encryption, decryption and authentication. A new padding technique has also been developed to ensure zero redundancy when sending encrypted/authenticated messages. Therefore, secure transactions do not generate extra bytes in their input.

## VI. OBJECTIVES & OVERVIEW OF THE PROPOSED PROTOCOL

This study proposes improvements for the trust-based security system (TCLS) [14], confidentiality and authentication of packets is done at the guide and link layers of MANET and is expected to perform the following:

1. **Light-Weight:** Is used symmetric key algorithms and encryption based hash Network lifecycle.
2. **Co-Operative:** Advanced security techniques using collaboration/collaboration between nodes
3. **Attack-Tolerant:** The network is resilient to attacks and works well as it can detect and eliminate the attack zone.

.

## VII. OVERVIEW OF THE PROTOCOL

The proposed Trust based packet forwarding scheme in MANETs does not use any centralized infrastructure. The trust cost associated with two tasks for Ad Hoc routing, sending packets and making trust-based recommendations, are examined. Each node holds trust information about these two functions. When a node (destination) wants to create a route to another node (destination), the node first tries to find multiple routes to the destination. The source then tries to find packets sent to the trusted nodes of the route from its own trust information or by asking for recommendations. Finally, the source chooses a reliable route to send the data. After transmission, the source node updates the trust information based on the performance evaluation

Trust data is also used for vulnerability detection. The trust value associated with the trust counter (TC) is used to support the packet sent to each node. Nodes can be penalized or benefited by increasing or decreasing each trust value counter. Each environment adds the hash (also known as the MAC) and sends the packet to the destination. The location of the site can be increased or decreased according to the analysis of the received hashes. If, after mitigation, the confidence value is found to be lower than the confidence level, the neutral effect can be marked as malicious.

This solution does not require any pre-implemented protocols and can provide solutions to the selfish behavior of nodes. The goal is to offer Cipher Block Chaining (PCBC) type encryption/decryption algorithms to meet low computational and communication overhead needs. The algorithm supports packet encryption/decryption and authentication in a single operation. Layers of the protocol stack explicitly provide security services.

A PCBC type symmetric key mechanism is designed to use a secure connection mechanism. Encryption/decryption and authentication takes place in a single step, reducing the computational load in half instead of calculating them separately. The padding technique used indicates that the path does not have a cipher text extension for the data to be sent. Therefore, the communication load can be reduced significantly.

.

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

Throughout the planning system, the node agree with counter price is dynamically calculated. The basis node can pick out o ne or extra consider paths in preference to shortcuts. Malicious nodes are isolated and unable to sign up for the community, lowering the impact of malicious nodes. The AODV routing protocol is changed as follows:

Every network maintains Neighbor agree with Counter table (NTT) for added records.

| Node | Trust counter($T_c$) | No. of packets forwarded Via (FC) |
|---|---|---|

**Figure 5:** Shape of NTT

Let $\{T_{c_1}, T_{c_2}, \ldots\}$ denote the initial trust counters of the nodes $\{n_1, n_2, \ldots\}$ 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 $n_i$ .

$$FC_{n_i} = FC_{n_i} + 1 \qquad i = 1,2, \ldots .. \tag{1}$$

The NTT of node $n_k$ is modified accordingly with the values of $FC_{n_i}$.

This procedure is similar for all of the nodes to determine NTT. The destination D now, measures the range of packets acquired (Prec.) after the accumulated RREQ message is obtained. *A* MAC on Prec. Is computed the use of the shared key of the sender and the destination. The digitally signed RREP packet includes the source and destination ids, the MAC fee, the accrued path from the RREQ. The RREP is sent lower back to the source using the opposite course towards R1. The RREP packet is then checked at every intermediate node from D to S. The success ratio for ever node is computed as;

$$SR_{i=} FC_{n_i}/Prec \tag{2}$$

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 spot node is saved in the RREP packet and verified at every intermediate node. If the verification succeeds, it's miles signed and forwarded to the following node in the reverse route in any other case the RREP packet is dropped. After the RREP packet is reached on the source S, verification is accomplished to test, the first id of the path saved by using the RREP is its neighbor. If the verification succeeds, then all the virtual signatures of all of the intermediate nodes are proven, inside the RREP packet. The verification method is conducted by using the intermediate node via verifying the virtual signature and the MAC saved in the RREP packet. If the verification fails, the RREP packet is dropped. Otherwise similarly signed by using the intermediate node and reverted lower back from destination spot to supply in a previous manner. If the verification system of the digital signature by way of the intermediate node i.e. contain in RREP is a success, then consider counter is incremented as;

$$T_{C_i} = T_{C_i} + \delta_1 \tag{3}$$

If the verification fails then trust counter is decremented as

$$T_{C_i} = T_{C_i} - \delta_1 \tag{4}$$

Where

$\delta_1$ 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;

$$T_{C_i} = T_{C_i} - \delta_2 \tag{5}$$

If

$SR_k > SR_{min}$, the trust counter values for all other nodes are incremented as

$$T_{C_i} = T_{C_i} + \delta_2 \tag{6}$$

Where

$\delta_2$ is a small step value (0.25) such that $\delta_2 < \delta_1$ .

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, and many others also use the similar technique to pick a route which does not incorporate a malicious node or a direction with least wide variety of malicious nodes. This sort of route is considered as the reliable path. The proposed work may be green and more comfy, considering authentication is executed for path reply operation. The cryptographic computations are done by using the nodes which can be saved inside the present day route.

## IX. PCBC MODE

The proposed method replaces the hyperlink layer protection scheme adapted to the packet format [21]. However the encryption and decryption mechanisms are special. It really works among the link layer and the radio layer. The proposed approach encrypts the records and computes the MAC, while the software information payload is passed from the link layer to the radio layer. With the assist of the radio channel, the encrypted message is dispatched out bit-via-bit. Confidentiality and authentication are the of security services which can be gift inside the proposed packet format. The packet format of the proposed scheme is illustrated in parent 6. The fields of the packet are the vacation spot cope with discipline (Dest), lively 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 within the proposed scheme to make it widespread and applicable. It additionally uses a four byte MAC field due to the fact it could provide enough safety of integrity and authenticity for the Mobile Ad Hoc Networks. Any error alteration during message transmission can be detected with the aid of re-computing the MAC and the mistake message might be discarded to improve the efficiency.

| Dest | A | L | G | Ran | Data | MAC |
|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 3 | (0-29) | 4 |

**Figure 6:** Packet Format

This scheme, the prevalent communication interfaces are given to the higher layer and use the lower radio packet interfaces. The nodes in the verbal exchange are not conscious of the operations on encryption/authentication because the safety offerings are given actually. To make the scheme less difficult, the encryption and authentication for each packet is completed via the default mode in a single bypass.

In order to complete the message authentication and encryption concurrently before sending message, an authentication and encryption scheme is constructed 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

$$C_i = E_K(P_i \oplus P_{i-1} \oplus C_{i-1}), P_0 \oplus C_0 = IV$$

as shown in Figure 7, where $p_0 \oplus c_0$ is the initialization vector (IV), $C_i$ is the cipher text in $i^{th}$ round, $P_i$ is plain text in $i^{th}$ round , and $\oplus$ is the XOR operation. “#

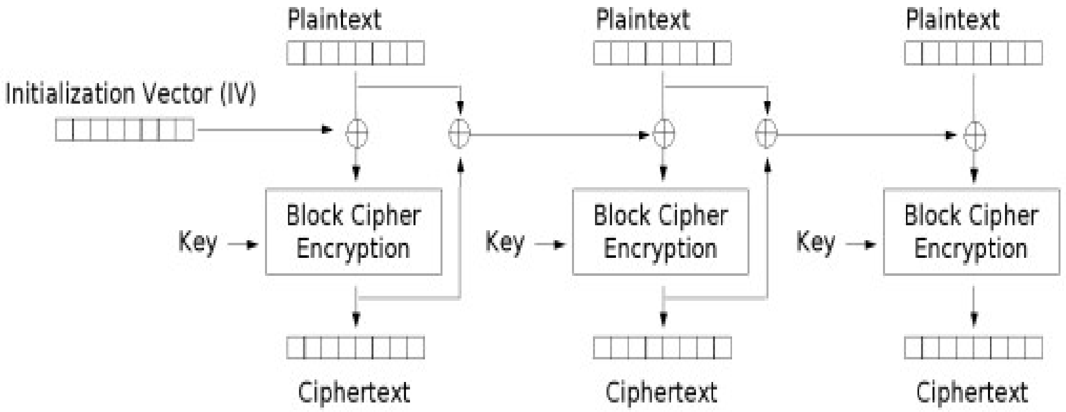

**Figure 7:** Propagating Cipher Block Chaining (PCBC) Mode Encryption

The method of decryption is given by

$$P_i = D_K(C_i) \oplus P_{i-1} \oplus C_{i-1}, P_0 \oplus C_0 = IV$$

as shown in Figure 8, where $P_0 \oplus C_0$ is the initialization vector (IV).

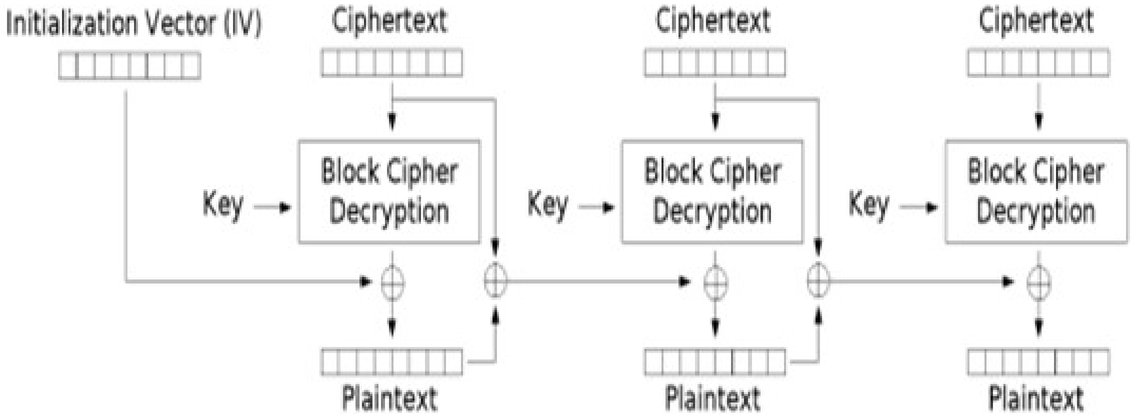

**Figure 8:** Propagating Cipher Block Chaining (PCBC) Mode Decryption

## 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 1. “#

**Table 1: Simulation Parameters**

| | |
|---|---|
| No. of Nodes | 120 |
| Area | 1000 x 1000 |
| MAC | 802.11 |
| Radio Coverage Range | 275 m |
| Simulation Time | 50 Secs |
| Traffic Source | CBR |
| Packet Size | 512 |
| Mobility Model | RWP |
| Speed(s) | 10,20,30,40,50,60 - m/s |
| Pause Time | 5 |

1. “#**Performance Metrics:** The performance is evaluated according to the following metrics.

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

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

4. **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. “#

## XI. 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.

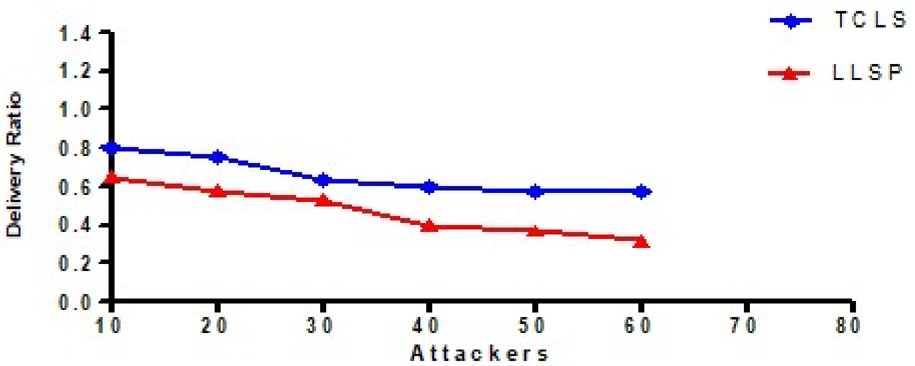

**Figure 9:** Attackers Vs Delivery Ratio

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.

Even though the speeds are increased from 40 to 60 m/s the TCLS scheme achieves more delivery ration than the LLSP scheme. It has both reliability and security features and the delivery ratio is remains constant.

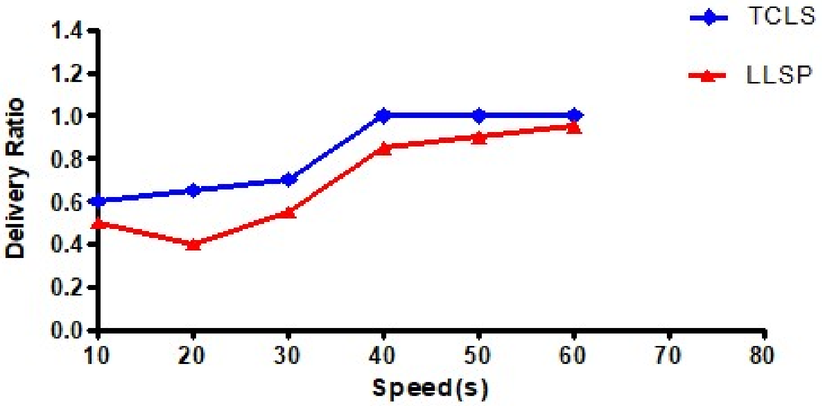

**Figure 10:** Speed Vs Delivery Ratio

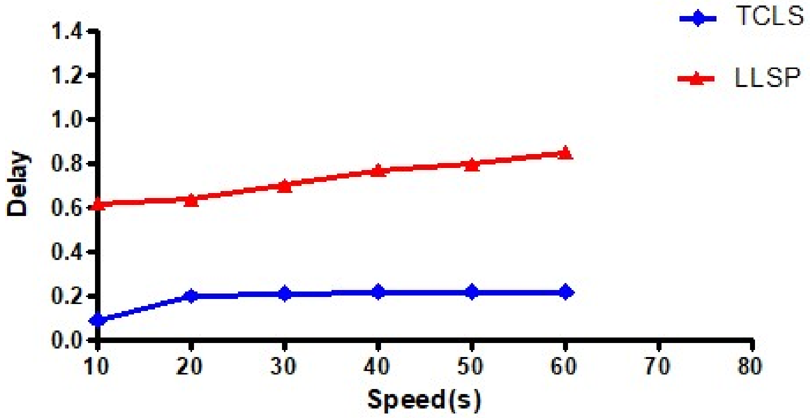

**Figure 11:** Speed Vs Delay

The simulation results shows the speed of 5 attackers varied between 10, 20,30,40,50 and 60 m/s. Using behavioral reliability in TCLS increase the average end-to-end latency as shown in Figure 11. The number of bad behavior is fixed and the variation for 100 nodes is 10, 20, 30, 40, 50 and 60 m/s. The latency of the TCLS strategy is slightly lower than the LLSP strategy due to the validation routine, and the simulation also shows that increasing the speed from 30 to 60 m/s does not affect the latency and remains constant.

## XII. SUMMARY

A framework was proposed to enhance the trust, the Trust-based cross layer protocol quantitatively evaluates the trust and propagation of the trust. This can prevent malicious attacks. This defense system is designed by identifying attacks on trusted systems. For reliability testing to secure Ad Hoc networks by establishing security mechanisms and helping detect vulnerabilities. The system's distributed strategy can increase the number of connections and detect malicious behavior in Ad Hoc networks.

## REFERENCES

[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.

[22] 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

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