The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks

A.Rajaram
Anna University Coimbatore
India.

Dr. S. Palaniswami
Registrar, Anna University Coimbatore
India.

***Abstract*—In this paper, we develop a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for 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 a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, we show that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay, high speed and overhead.**

Keywords- MANETs, MAC-Layer, Security Protocol, Encryption, authentication, Packet Delivery, Overhead, High speed.

I. INTRODUCTION

A. Mobile Ad-hoc Networks

An ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such a environment, it may be necessary for one node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

B. Security Threats in MANETS

The current mobile ad-hoc networks allow for many different types of attacks. Although the analogous exploits also exits in wired networks but it is easy to fix by infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this the attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation.

Attacks using Modification

Modification is a type of attack when an authorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DOS attacks by modifying message fields or by forwarding routing message with false values.

Attacks using Impersonation

As there is no authentication of data packets in current ad-hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can either.

Attacks through Fabrication

Fabrication is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages

Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

Lack of Cooperation

Mobile ad-hoc networks rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources..

The following are the types of active attacks and its relevant solutions:

A. Black hole attack

In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consumes or intercepts the packet without any forwarding. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped. Let H be a malicious node. When H receives a Route Request, it sends back a Route Reply immediately, which constructs the data and can be transmitted by itself with the shortest path. So S receives Route Reply and it is replaced by H->S. then H receives all the data from S.

B. Neighbor attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without redirecting its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors (i.e. one hop away from each other), resulting in a disrupted route. The neighbor attack and black hole attack prevent the data from being delivered to the destination. But the neighbor attacker does not catch and capture the data packets from the source node. It leaves the settings as soon as sending the false messages.

C. Wormhole attack

The wormhole attack is one of the most powerful attacks presented here, since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.

D. DoS (Denial of Service) attack

Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad-hoc network. Specific instances of denial of service attack include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating node and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

E. Information Disclosure attack

In this, a compromised node may leak confidential information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes or, optimal routes to unauthorized nodes in the network. Attacks such as location disclosure and traffic analysis come under this category.

F. Rushing attack

On demand routing protocols that use route discovery process are vulnerable to this type of attack. An attacker node which receives a “route request” packet from the source node floods the packet quickly through out the network before other nodes which also receive the same “route request” packet can react. Nodes that receive the legitimate “route request “ packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets.

G. Jellyfish attack

Similar to blackhole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them. These results in significantly high end-to-end delay and delay jitter, and thus degrade the performance of real-time applications. In this a malicious node receives and sends RREQ and RREP normally. But before forwarding it delays the data packets without any reason for some time.

H. Byzantine attack

Here a compromised intermediate node or a set of compromised intermediate nodes collectively carries out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services within the network. It is also called as impersonation attack because the malicious node might imitate another normal node. It also sends false routing information for creating an anomaly update in the routing table. In addition to this, attacker may get unauthorized admission to resources and sensitive information.

I. Blackmail attack

This attack is applicable against routing protocols which use mechanisms for the recognition of malicious nodes and broadcast the messages which try to blacklist the offender. By adding other legitimate nodes to their blacklists, an attacker might blackmail a legitimate node. Thu the nodes can be avoided in those routes.

J. Sybil attack

In the Sybil attack, an attacker pretends to have multiple identities. A malicious node can behave as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Sybil attacks are classified into three categories: direct/indirect communication, fabricated/stolen identity, and simultaneity.

K. Misrouting attack

In the misrouting attack, a non-legitimate node redirects the routing message and sends data packet to the wrong

destination. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.

L. Resource consumption attack

In this attack, a malicious node deliberately tries to consume the resources (e.g. battery power, bandwidth, etc.) of other nodes in the network. The attacks could be in the form of unnecessary route request control messages, very frequent generation of beacon packets, or forwarding of stale information to nodes.

M. Routing table or Route cache poisoning

In this attack, a malicious node sends false routing updates to other uncompromised nodes. Such an attack may result in suboptimal routing, network congestion or even make some part of the network inaccessible.

N. Gray hole attack

Under this attack, an attacker drops all data packets but it lets control messages to route through it. This selective dropping makes gray hole attacks much more difficult to detect then blackhole attack.

II. Related Work

Farooq Anjum et al. [1] have proposed an initial approach to detect intrusions in ad hoc networks. Anand Patwardhan et al. [2] have proposed a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol-independent Intrusion Detection and Response system for ad-hoc networks. Chin-Yang Henry Tseng [3] has proposed a complete distributed intrusion detection system has consisted of four models for MANETs with formal reasoning.

Tarag Fahad and Robert Askwith [4] have concentrated on the detection phase and they have proposed a mechanism Packet Conservation Monitoring Algorithm (PCMA) is used to detect selfish nodes in MANETs. Panagiotis Papadimitratos and Zygmunt J. Haas [5] have proposed the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol SMT and SSP robustly detect transmission failures and continuously configure their operation to avoid and tolerate data loss, and to ensure the availability of communication. Ernesto Jiménez Caballero [6] has reviewed the possible attacks against the routing system, some of the IDSs proposed.

Yanchao Zhang et al. [7] have proposed a credit-based Secure Incentive Protocol (SIP) to stimulate cooperation in packet forwarding for infrastructure less MANETs. Liu et al. [8] have proposed the 2ACK scheme that has served as an add-on technique for routing schemes to detect routing misbehavior and to mitigate the adverse effect

Li Zhao and José G. Delgado-Frias [9] have proposed a scheme MARS and its enhancement E-MARS to detect misbehavior and mitigate adverse effects in ad hoc networks. Patwardhan et al. [10] have proposed an approach to secure a MANET using a threshold-based intrusion detection system and a secure routing protocol. Madhavi and Tai Hoon Kim [11] have proposed a MIDS (Mobile Intrusion Detection System) suitable for multi-hop ad-hoc wireless networks, which has detected nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets.

Syed Rehan Afzal et al. [12] have explored that the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which confiscated the problems mentioned in the existing protocols. In addition, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication

Bhalaji et al. [13] have proposed an approach based on the relationship between the nodes to make them to cooperate in an ad hoc environment. 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. Their proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the network simulator-2.za

Kamal Deep Meka et al. [14] have proposed a trust based framework to improve the security and robustness of adhoc network routing protocols. 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. Their schemes are based on incentives & penalties depending on the behavior of network nodes. Their schemes incur minimal additional overhead and preserve the lightweight nature of AODV.

Azal et al. [12] have explored the security problems and attacks in existing routing protocols and then they have presented a design and analysis of a new secure on-demand routing protocol, called RSRP which confiscates the problems mentioned in the existing protocols. Moreover, unlike Ariadne, RSRP uses a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication.

Muhammad Mahmudul Islam et al. [15] have presented a possible framework of a link level security protocol (LLSP) to be deployed in a Suburban Ad-hoc Network (SAHN). They have analyzed various security aspects of LLSP to validate its effectiveness. To determine LLSP's practicability, they 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.

Shiqun Li et al. [16] have explored that the security issues of wireless sensor networks, and in particular propose an efficient link layer security scheme. To minimize computation and communication overheads of the scheme, they have designed a lightweight CBC-X mode Encryption/Decryption algorithm that attained encryption/decryption and authentication all in one. They have also devised a novel padding technique, enabling the scheme to achieve zero redundancy on sending encrypted/authenticated packets. As a result, security operations incur no extra byte in their scheme.

Stefan Schmidt et al. [17] have proposed security architecture for self-organizing mobile wireless sensor networks that prevented many attacks these networks are exposed to. In addition, it has limited the security impact of some attacks that cannot be prevented. They analyzed their security architecture and they have showed that it has provided the desired security aspects while still being a lightweight solution and thus being applicable for self-organizing mobile wireless sensor networks.

III. Objectives & Overview Of The Proposed Protocol

A. Objectives

In this paper, we propose to design a Trust-based MAC-layer Security protocol (TMLS) based on a MAC-layer, approach which attains confidentiality and authentication of packets in routing layer and link layer of MANETs, having the following objectives:

- **lightweight** in order to considerably extend the network lifetime, that necessitates the application of ciphers that are computationally efficient like the symmetric-key algorithms and cryptographic hash functions
- **cooperative** for accomplishing high-level security with the aid of mutual collaboration/cooperation amidst nodes along with other protocols
- **attack-tolerant** to facilitate the network to resist attacks and device compromises besides assisting the network to heal itself by detecting, recognizing, and eliminating the sources of attacks;
- **flexible** enough to trade security for energy consumption;
- **compatible** with the security methodologies and services in existence
- **scalable** to the rapidly growing network size

B. Overview of the Protocol

We propose a Trust based packet forwarding scheme in MANETs without using any centralized infrastructure. 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. Each intermediate node marks the packets by adding its hash value. And forward the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, other wise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious.

This scheme presents a solution to node selfishness without requiring any pre-deployed infrastructure. It is independent of any underlying routing protocol.

We focus on the CBC-X 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 CBC-X mode symmetric key mechanism is devised to employ our 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 states that this method has no cipher text expansion for the transmitted data payload. Thus the communication overhead is reduced significantly.

IV. Efficient MAC Layer Security Protocol

A. Trust Based Forwarding Scheme

In our proposed protocol, by dynamically calculating the nodes trust counter values, the source node can be able to select the more trusted routes rather than selecting the shorter routes. Our protocol marks and isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious nodes are reduced. We make changes to the AODV routing protocol. An additional data structure called *Neighbors' Trust Counter Table (NTT)* is maintained by each network node.

Let $\{Tc_1, Tc2\ldots\}$ be the initial trust counters of the nodes $\{n_1, n2\ldots\}$ along the route R1 from a source S to the destination D.

Since the node does not have any information about the reliability of its neighbors in the beginning, nodes can neither be fully trusted nor be fully distrusted. When a source S wants to establish a route to the destination D, it sends route request (RREQ) packets.

Each node keeps track of the number of packets it has forwarded through a route using a forward counter (FC). Each time, when node n_k receives a packet from a node n_i, then n_k increases the forward counter of node n_i.

$$FCn_i = FCn_i + 1,\ i=1, 2\ldots\ldots \quad (1)$$

Then the NTT of node n_k is modified with the values of FCn_i.

Similarly each node determines its NTT and finally the packets reach the destination D.

When the destination D receives the accumulated RREQ message, it measures the number of packets received Prec. Then it constructs a MAC on Prec with the key shared by the sender and the destination. The RREP contains the source and destination ids, The MAC of Prec, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1.

Each intermediate node along the reverse route from D to S checks the RREP packet to compute success ratio as,

$$SR_i = FCn_i / Prec \quad (2)$$

Where Prec is the number of packets received at D in time interval t1. The FCn_i values of n_i can be got from the corresponding NTT of the node. The success ratio value SR_i is then added with the RREP packet.

The intermediate node then verifies the digital signature of the destination node stored in the RREP packet, is valid. If the

verification fails, then the RREP packet is dropped. Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route.

When the source S receives the RREP packet, if first verifies that the first id of the route stored by the RREP is its neighbor. If it is true, then it verifies all the digital signatures of the intermediate nodes, in the RREP packet. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Tc_i = Tc_i + \delta 1 \quad (3)$$

If the verification is failed, then

$$Tc_i = Tc_i - \delta 1 \quad (4)$$

Where, δ1 is the step value which can be assigned a small fractional value during the simulation experiments.

After this verification stage, the source S check the success ratio values SR_i of the nodes 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

$$Tc_i = Tc_i - \delta 2 \quad (5)$$

Which involve regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad-hoc network of peer workstations. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN.

The DCF sublayer makes use of a simple CSMA (carrier sense multiple access) algorithm. The DCF does not include any collision detection function (i.e. CSMA/CD). The dynamic range of the signals on the medium is very large, so that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission.

To ensure smooth and fair functioning of the algorithm, DCF includes a set of delays that amounts a priority scheme.

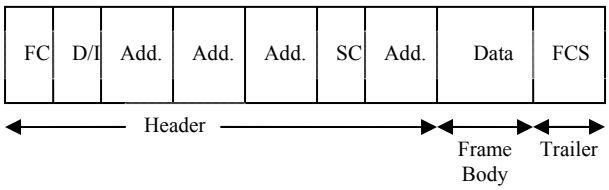


Figure.1. MAC frame format

FC- frame Control, SC- sequence Control, Oct. - Octets

D/I-duration/connection control, FCS-frame checks sequence.

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

$$Tc_i = Tc_i + \delta 2 \quad (6)$$

Where, δ2 is another step value with δ2 < δ1.

For a node n_k, if $Tc_k < Tc_{thr}$, where Tc_{thr} is the trust threshold value, then that node is considered and marked as malicious.

If the source does not get the RREP packet for a time period of t seconds, it will be considered as a route breakage or failure. Then the route discovery process is initiated by the source again.

The same procedure is repeated for the other routes R2, R3 etc and either a route without a malicious node or with least number of malicious nodes, is selected as the reliable route.

In this protocol, authentication is performed for route reply operation. Also, only nodes which are stored in the current route need to perform these cryptographic computations. So the proposed protocol is efficient and more secure.

B.MAC Frame Format

There are two types of proposals for a MAC algorithm: Distributed access protocols, which, like Ethernet, distribute the decision to transmit over all the nodes using a carrier-sense mechanism; and centralized access protocols,

Frame control indicates the type of frame and provides control information. Duration/connection ID indicates the time the channel will be allocated for successful transmission of a MAC frame. Address field indicates the transmitter and receiver address, SSID and source & destination address. Sequence control is used for fragmentation and reassembly.

C. CBC-X Mode

Our proposed link layer security scheme works between the link layer and the radio layer. Our proposed method encrypts the data and computes the MAC, when the application data payload is passed from the AM 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 our proposed packet format.

The packet format of the proposed scheme is illustrated in Figure.2; the fields of the packet are the destination address field, the active message type field, the length field and the data field. We keep the one byte group field in the proposed scheme to make it general and applicable. We also use a 4 byte MAC field since it can provide enough security of integrity and authenticity for the mobile adhoc 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. It uses an 8 byte initial vector (IV) and a block cipher mechanism to encrypt the data field of the packet. The fixed portions of both IVs are the destination address field, the AM type field and the length field. These fields take 4 bytes totally.

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

Figure.2. Packet Format

In our 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 our default mode in a single pass. In order to finish the message authentication and encryption concurrently before sending message, we built an authentication and encryption scheme called as CBC-X mode.

1) CBC-X Mode Operation:-

The basic steps involved in the encryption and decryption operations are illustrated in figure 3 and figure 4, respectively.

If the first block has index 1, the formula for CBC encryption is

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

While the formula for CBC decryption is:

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

The working of the present CBC mode is described below: One cipher text block will be returned for each plaintext block, if a part of the plaintext is encrypted. In encryption of the last block of the plaintext, one or two cipher text blocks can be returned. On the other hand, decryption works in the reverse order. Apart from the decryption of the last block, a one plaintext block will be returned for each cipher text block. After the decryption of the last plaintext block, its padding is calculated and cut off, returning a valid plaintext.

2) CBC Padding Schemes. Plaintext is divided into blocks of 8 bytes (64 bits). The final plaintext block must be padded: the final a plaintext bytes $0 \le a \le 7$ are followed by $8 - a$ padding bytes, valued $8 - a$.

For example:

$messagebyte_1$ || $messagebyte_2$|| '06'|| '06'|| '06'|| '06'|| '06'|| '06'

ESP.

X padding bytes $1 \le X \le 255$

'01'||'02'|| '03'||…..|| 'X'

V. Performance Evaluation

A.Simulation Model and Parameters

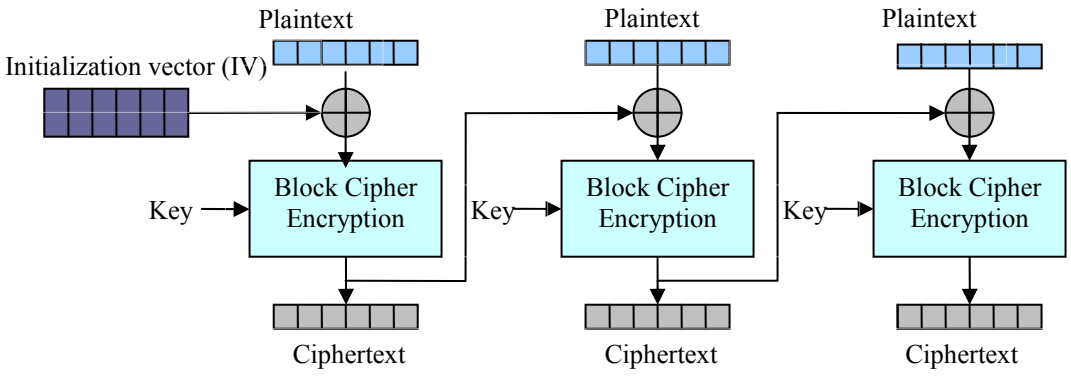
We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed is varied from 10 m/s to 50m/s. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1.

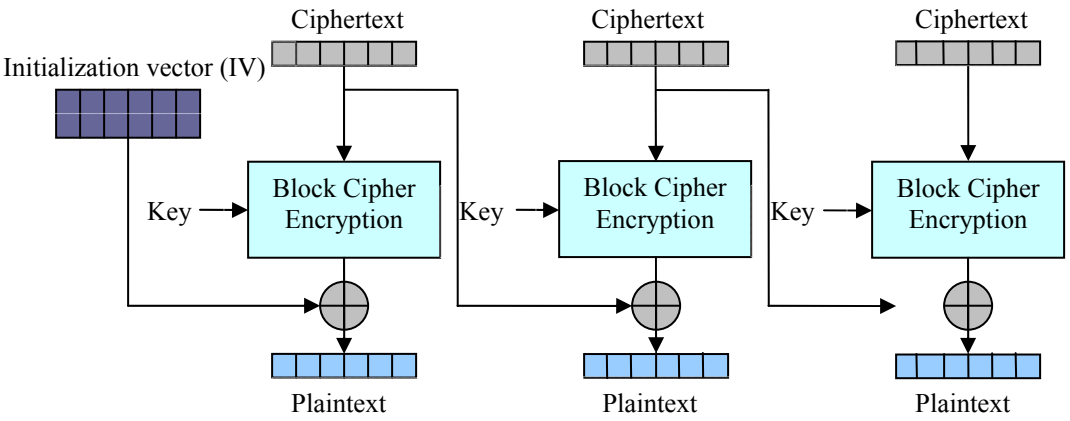
Table 1

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



Cipher Block Chaining (CBC) mode Encryption

Figure.3. Encryption



Cipher Block Chaining (CBC) mode decryption

Figure 4- Decryption

B. Performance Metrics

We evaluate mainly the performance 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: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next section. We compare our TMLS protocol with the LLSP [15] and RSRP [12] protocol in presence of malicious node environment.

C. Results

A. Based On Attackers

In our First experiment, we vary the no. of misbehaving nodes as 10,20,30,40 and 50.

Figure 5 show the results of average packet delivery ratio for the misbehaving nodes 10, 20…50 scenarios. Clearly our TMLS scheme achieves more delivery ratio than the LLSP and RSRP scheme since it has both reliability and security features.

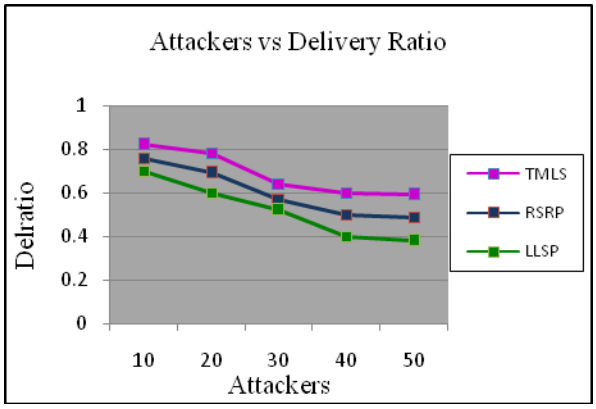


Figure. 5 Attackers Vs Delivery Ratio

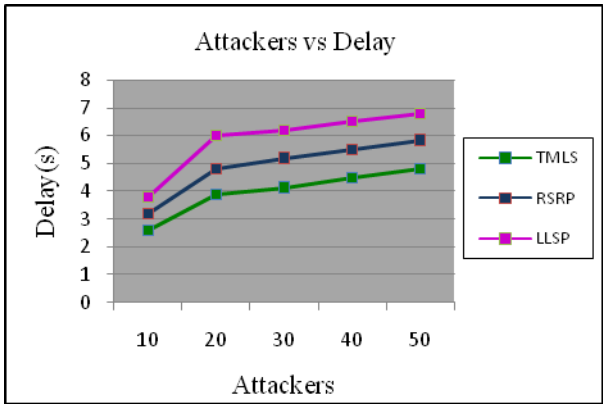


Figure.6 Attackers Vs Delay

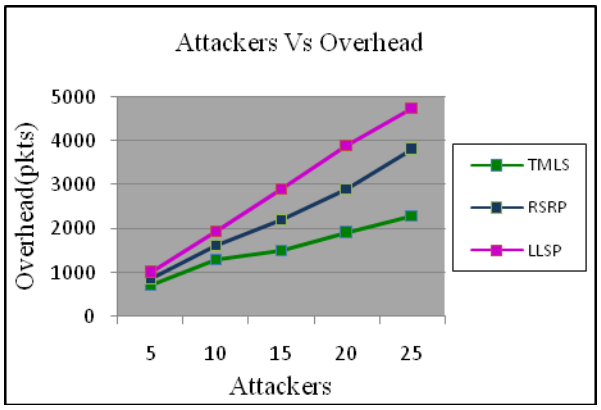


Figure. 7 Attackers Vs Overhead

Figure 6 shows the results of average end-to-end delay for the misbehaving nodes 10, 20…50. From the results, we can see that TMLS scheme has slightly lower delay than the LLSP and RSRP scheme because of authentication routines.

Figure 7 shows the results of routing overhead for the misbehaving nodes 5, 10….25. From the results, we can see that TMLS scheme has less routing overhead than the LLSP and RSRP scheme since it does not involve route re-discovery routines.

B. Based On Speed

In our Second experiment, we vary the speed as 10,20,30,40 and 50, with 5 attackers.

Figure 8 show the results of average packet delivery ratio for the mobility10, 20…50 for the 100 nodes scenario. Clearly our TMLS scheme achieves more delivery ratio than the LLSP and RSRP scheme since it has both reliability and security features.

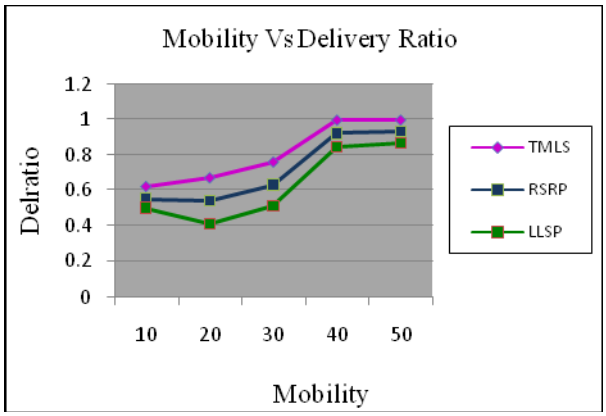


Figure. 8. Mobility Vs Delivery Ratio

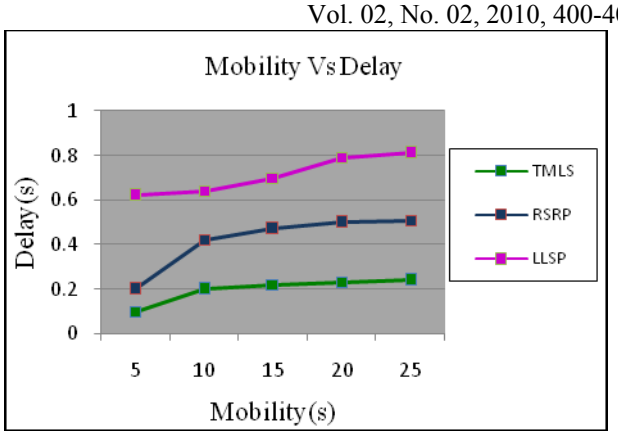


Figure.9. Mobility Vs Delay

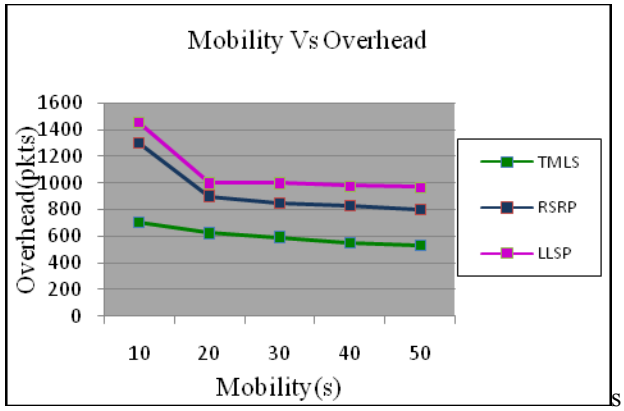


Figure. 10. Mobility Vs Overhead

Figure 9 shows the results of average end-to-end delay for the mobility5, 10, 15, 20, and 25. From the results, we can see that TMLS scheme has slightly lower delay than the LLSP and RSRP scheme because of authentication routines.

Figure 10 shows the results of routing overhead for the speed 10, 20….50. From the results, we can see that TMLS scheme has less routing overhead than the LLSP and RSRP scheme.

VI. CONCLUSION

In this paper, we have developed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we have designed a trust based packet forwarding scheme for 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 a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, we have shown that the proposed MAC-layer security protocol

achieves high packet delivery ratio while attaining low delay and overhead.

REFERENCES

[1] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003.

[2] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

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

[4] 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.

[5] Panagiotis Papadimitratos, and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[6] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.

[7] 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.

[8] 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.

[9] Li Zhao and José G. Delgado-Frias "MARS: Misbehavior Detection in Ad Hoc Networks", in proceedings of IEEE Conference on Global Telecommunications Conference,November 2007.

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

[11] S.Madhavi and Dr. Tai Hoon Kim "AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC networks" International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[12] 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.

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

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

[15] 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.

[16] 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.

[17] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen, "A Security Architecture for Mobile Wireless Sensor Networks", In proceedings of First European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), August 2004.

[18] M. O. Pervaiz, M. Cardei, and J. Wu, " Routing Security in Ad-hoc Wireless Networks" Network Security , S. Haung, D. Maccallum, Springer, 2008.

[19] B. Awerbuch, D. Holmer, C. Nita-Rotaru, " An On-Demand Secure routing protocol Resilient to Byzantine failures", Proceedings of ACM workshop on wireless security 2003, Sep. 2003.

[20] K. Sanzgir, and B. Dahill, " A secure routing Protocol for ad-hoc networks", Proceeding of the 10th IEEE International Conference on Network Protocols, 2002, pp.1-10.

AUTHORS PROFILE

S. Palaniswami received the **B.E.** degree in electrical and electronics engineering from the Govt., college of Technology, Coimbatore, University of Madras, Madras, India, in 1981, the **M.E.** degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Bharathiar University, Coimbatore, India, in 1986 and the **Ph.D.** degree in electrical engineering from the **PSG** Technology, Bharathiar University, Coimbatore, India, in 2003. He is currently the Registrar of Anna University Coimbatore, Coimbatore, India, Since May 2007. His research interests include Control systems, Communication and Networks, Fuzzy logic and Networks, **AI**, Sensor Networks. . He has about 25 years of teaching experience, since 1982. He has served as lecturer, Associate Professor, Professor, Registrar and the life Member of **ISTE**, India.

A. Rajaram received the **B.E.** degree in electronics and communication engineering from the Govt., college of Technology, Coimbatore, Anna University, Chennai, India, in 2006, the **M.E.** degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Anna University, Chennai, India, in 2008 and he is currently pursuing the full time **Ph.D.** degree in electronics and communication engineering from the Anna University Coimbatore, Coimbatore, India. His research interests include communication and networks mobile adhoc networks, wireless communication networks **(WiFi, WiMax HighSlot GSM),** novel **VLSI NOC** Design approaches to address issues such as low-power, cross-talk, hardware acceleration, Design issues includes **OFDM MIMO** and noise Suppression in **MAI** Systems, **ASIC** design, Control systems, Fuzzy logic and Networks, **AI**, Sensor Networks.