International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 7,July 2015

Secure Routing In Manets Based On Cross Layer Design Approach

[1] Madhuri Bhagwat,[2] Dr Prof. Amol Pande
[1] ME Student, Dept of Computer Engineering, Datta Meghe College of Engineering,Airoli, India
[2] HOD, Dept of Computer Engineering, Datta Meghe College of Engineering,Airoli, India
[1] madhu123.bhagwat@gmail.com,[2] amolpande69@gmail.com

Abstract- **Security of Wireless Networks is very important and essential for secure communication. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. The paper reviews the proposed work on one method that shows secure routing in MANETs. By using the best security mechanism between mobile nodes the paper "cross layer based secure routing in MANETs" is proposed by authors [1]. The cross layer design is the new research topic used in computer networks which is used to satisfy the network requirements. The proposed method gives enhancement to the CSR-MAN method in which the passing of information from physical layer and MAC layer to the network layer based on the parameters obtained from the lower layers. The ns2 simulation results show evaluation of this method. So comparison between CSR-MAN and SCSR-MAN on different parameters on different conditions shows good network performance.**

Key Terms: Cross layer, MANETs, Routing and Security.

I. INTRODUCTION

Manets are self-configuring networks in which mobile devices are connected by wireless links. These networks classify into infrastructure networks, where the network communication is established without any fixed infrastructure such as, battlefields, military applications and other emergency disaster situations. Security is important concern due to their increased vulnerability and exposure to varying types of attacks.

Unreliable wireless links, frequently changing network topology and lack of centralized system to handle the security needs of the network to contribute to insecure and standalone systems in wireless networks.

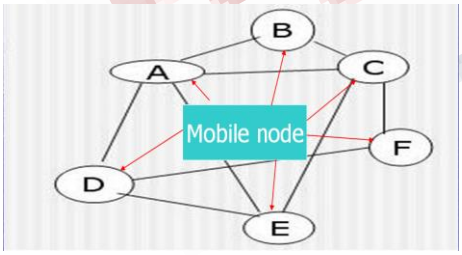

Fig.1. Manet view

Security features of MANETs [5]:

Availability: Availability is to keep the network service or resources available to legitimate users.

Confidentiality: Confidentiality is to keep the information sent unreadable to unauthorized users or resources.

Authentication: Authentication is to be able to identify a node or a user and to be able to prevent impersonation.

Integrity: Integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission.

Non-repudiation: It is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it.

Access Control: It is to prevent unauthorized use of network services and system resources.

Routing Attacks in MANETs:

There are two types of routing attacks [5]:

Passive Attacks: These attacks do not disrupt the operation of routing protocols. Example: Traffic analysis, Eavesdropping, Monitoring.

Active Attacks: These attacks disrupt the operation of routing protocols. Example: Modification, Spoofing, Jamming, Replaying, DoS (Denial of Service).

Further active attacks are classified in two ways. External attacks: These attacks do not belong to domain of network. External attacks also known as outsider attacks. External attacks come from node that does not have the authentication of network. Internal attacks: These attacks come from compromise nodes that have the legal private key of network. This compromise node can modify routing packets to disrupt the operation of routing protocols and generate the unnecessary routing information. Internal attacks are actually part of network.

Below table shows attacks on each layer.

TABLE-I

Layers	Attacks
Application layer	Data corruption, Repudiation
Transport layer	SYN flooding, Session hijacking
Network layer	Black hole, Byzantine, Flooding, Wormhole
Data link layer	Monitoring, Traffic analysis
Physical layer	Eavesdropping, Jamming, Interception
Multi layer	Impersonation, Replaying, Denial of services

To overcome these attacks the mechanism know as the cross layer based secure routing is proposed in which passing of information from physical layer and mac layer to network layer is there.These machanism is uesd in Ad-hoc Distance Vector Routing protocol to provide best security to Manets.For that the cross layer design is used.

All Protocols proposed in MANET have to take in their account the basic inherent characteristics of the network which are dynamic topology, variable link capacity and bandwidth constraints, energy constraints nodes and multi-hop communications.

All these characteristics are seriously challenged the OSI layer design which is characterized by Modularity and permit to create a new methodology named cross-layer. The cross-layer design refers to an optimized approach design done by allowing layers to exchange state information in order to obtain performance gains. The sharing of information enables each layer to have global pictures of the constraints and characteristics of the network. The cross layer design enables the network protocols and applications to observe and respond to the changing network and channel condition. Below figure shows cross layer design method.

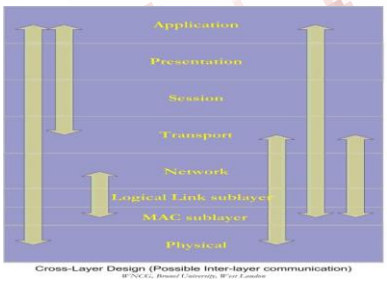

Fig. 2. Cross Layer Architecture

So by using this method in proposed work we get efficient results.

II. Literature review

Here the existing system is AODV and SAODV routing protocol.So AODV Routing protocol[4] in this paper the author describes the working of AODV protocol in which AODV is on demand distance vector routing protocol designed for the operation of mobile ad-hoc networks.Protocol provides self-starting, dynamic, loop-free, multi-hop routing. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in the network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to destination that are in active communication. Routes are created on demand.

AODV protocol works in two different phases

1. Route Discovery Process
2. Route Maintenance Process

Route Discovery Process: It uses Route Request (RREQ) and Route Reply (RREP) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path. RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for route freshness, loop prevention and faster convergence. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also unicast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up.

Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link to that neighbor node has broken then it generates route error message (RERR). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number.

In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighboring nodes that are likely to use it as a next hop towards each destination. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In addition to these routing messages, the route reply acknowledgment (RREP ACK) message must be sent by sender node of RREQ in response to a RREP message with the 'A' bit set. This provides assurance to the sender of RREP that the link is bidirectional.

Security issues of AODV Protocol:

AODV routing protocol does not provide any security mechanisms to guard against attack. The major vulnerabilities present in AODV protocol are:

1. Attacker can impersonate a source node S by forging a RREQ with its IP address as IP address of source node S.
2. Attacker can impersonate a destination node D by forging a RREP with its IP address as IP address of the destination node D.
3. Decreasing hop count in RREQ/RREP.
4. Increasing sequence number in RREQ/RREP.
5. Forging the RRER message.

And also presents the secure ad-hoc distance vector roting protocol (SAODV) to overcome these security issues. SAODV uses cryptographic computations but it also has some security issues.

1. SAODV provides the less security to AODV protocol.
2. There is nothing to prevent a node from increasing a hop count arbitrarily from leaving it unchanged.
3. It does not do anything to protect the sender IP address field S, which is used as next hop information in routing tables. This can be used to disrupt the routing information.

B. Ramachandran have discussed about a simple CLD between physical layer and MAC layer for power conservation based on transmission power control [7]. The carrier sense multiple access with collision avoidance of IEEE 802.11 is integrated with the power control algorithm. The exchange of Request-To-Send (RTS) / Clear-To-Send (CTS) control signal is used to piggyback the information to enable the sender node to discover the minimum power requirement to transmit the data.

M. Conti have discussed that the protocols belonging to different layers can cooperate by sharing the network status information but at the same time maintaining the separation of layers for protocol design [8].

The proposed solution has the advantage of balanced cross-layer design. The cross-layering is limited to parameters and implemented through data sharing called network status, which is a shared memory that every layer can access. Interlayer cooperation is obtained by variable sharing and the protocols are still implemented in each layer.

So AODV protocol does not contain any security mechanism. So to provide security in Manets there is need of best security mechanism and by using cross layer design we can achieve this.

III. PROPOSED WORK

The cross layer design uses the parameters such as Received Signal Strength, Available Bandwidth, Threat Value and Digital Signature parameter. These parameters are calculated based on formulas given in paper, Cross layer based secure routing in Manets [1].The proposed mobility cross-layer design couples the route discovery process with physical layer related received signal strength information of mobile nodes to built stable and optimum routes. Selection of the routing at Network Layer is based on the high signal strength due to mobility between nodes.

The Radio propagation models:

1. Free space model
2. Two-ray ground model

In the free space model:

There exists a clear line-of-sight between the transmitter and receiver. .

The received signal strength (RSS) [9]at distance d in this situation is defined as follows:

$$P_r(d)=(Ptx \cdot Gtx \cdot Grx.\lambda^2)/((4\pi d)^2) \text{ ---------- (1)}$$

Where, Ptx is the transmitted signal power, Gtx and Grx are the antenna gains of the transmitter and receiver, λ is the wavelength.

For the purposes of this analysis,

Ptx = Gtx = 1 and Grx with the assumed receiver antenna gain. The total amount needed to transmit, is calculated as follows:

$$Ptx=(Prx)\ (\ 4\pi d/((\lambda)\ ))^2 \text{ ---------- (2)}$$

Where Prx is the received signal power, can be calculated by multiplying the amount of noise present in the system.The noise level can include the thermal noise and aggregate noise caused by concurrent transmissions too weak to cause a collision.

In Two-ray ground model:
A single line-of-sight path between two mobile nodes is seldom the only means of propagation. The two-ray ground reflection model considers both the direct path and a ground reflection path. It is shown [8] that this model gives more accurate prediction at a long distance than the free space model. The received power at distance d is predicted by

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

Where, ht and hr are the heights of the transmit and receive antennas respectively. Note equation in [8] assumes L = 1. To be consistent with the free space model, L is added here. By comparing these two models the two-ray ground model gives better results.
A neighbor table maintains neighboring table at every node which contains the RSS, node id , distance , Average distance and timestamp at which packet was received.RSS is higher then transmission will be more durable.The available bandwidth is calculated at the mac layer. To find an optimal path such that the available bandwidth on the path is above the minimum requirement.Bandwidth measurements are realized according to 802.11 operations. Abw is carried out at the seder side by calculating the relationship between the size of the measurement packet and the dSN duration necessary to its transmission on the channel. Available bandwidth is given by the equation:

Abw = Dl / dSN

Where, Abw indicates Available bandwidth; Dl indicates the Data length; dSN can be split into two parts namely variable part and a constant part. [The variable part depends on the channel occupancy and on the duration of the contention window. The constant part corresponds to the transmission of the control and data frames when station S is in emission phase.]
The Threat value parameter is calculated at the Routing Layer for the entire route.Tvp is uesd for secure communication among nodes in MANETs.The path is selected in such a way that the node with less Tvp values are selected along with the considerations of the other two parameters received from the lower layer (cross-layer parameters). In the process of calculating Tvp, drop values are calculated from each node to its neighboring node. Drop values =(total number of packets sent - total number of packets received) /(total number of packets sent).
The Threat value parameter (Tvp):Tvp=Dvsa + Dvab + Dvbc +…..+ Dvyz / ((total number of nodes along the route)-1)
Where,Tvp is the Threat Value parameter; Dv indicates the drop value and sa indicates source to node a, similarly bc indicates node b to node c etc., yz indicates node y to destination node z. Tvp is calculated for each route available during route discovery and is checked against the threshold value.
The threshold value is assumed as 15. If higher than the threshold value, then there is a possibility for this node to be marked as node with prone to attacks for the current transmission and node/s are assumed to be under malicious activity and hence an alternate path is selected for routing.
Digital Signature: To overcome other attacks like man-in the middle, SHA1 algorithm is used. To protect the hop count values, hash values are found by SHA-1 algorithm for those fields. Here packets are sent along with the hash values. Now, the malicious node, which forwards the false routing information, can be effectively defended [7].
Algorithm:

1. Sender generate route request packet.
2. Append signature extension to route request packet;
3. Broadcast route request to all the neighbor nodes,
4. Intermediate node receives route request packet,
5. Node verifies signature with the public key of source(from Route Request packet),
   If (valid packet)
   Then update routing information of source in any(establishment of reverse path);
6. If(destination IP=node IP)
   {
   Generate RREP;
   Signs all the nodes with private key
   Apply hash to the seed to generate hash chain field,
   Append signature extension to RREP packet,
   Unicast RREP to the neighbor which is in the reverse path for the source node,
   } else if
   {((node has valid route for destination)&&!(destination tag))
   Generate RREP;
   Copy the signature of source to signature extension and sign all the nodes with private key
   Apply hash to the seed to generate hash field;
   Append signature extension to RREP packet;
   Unicast RREP to the neighbor which is in the reverse path for the source node,
   }else
   Node IP=insecure node IP
   Then
   free packet;

So, the digital signature is used with RSS, Abw, Tvp parameters. It gives best security to the routing layer.The

destination node selects the optimal route after receiving RREQ packets at the destination, which contains information about the received signal strength, available bandwidth,threat value and digital signature. The fields in RREQ packets are updated at each intermediate node with the new values of cross-layer parameters received from the lower layers and Tvp and digital signature at the Routing layer. Here the Tvp and digital signature have higher priority for selecting route. The Routing Table maintains neighboring table at every node which includes value of RSS of neighbor packet, node ID, Distance, Avg Distance and Timestamp at which packet was received.

IV. SIMULATION

All Simulations have been carried out using the NS2. The following simulation parameters are set to run the experiment. These options are available in the simulator NS2. Below table describes the parameters used in our simulation.

TABLE-II.

Simulator	NS2
Channel type	Channel/Wireless Channel
Radio Propogation Model	Propogation/TwoRayGround
Network Interface Type	Phy/WirelessPhy
MAC Type	Mac/802_11
Interface Queue Type	Queue/Droptail/Priority Queue
Antenna Model	Antenna/Omniantenna
Link Layer Type	LL
Routing Protocol	AODV
Simulation Area	500*400

The Parameters Avererage energy, Control overhead, Packet Dropping Ratio, Jitter, Packet Delivery Ratio, Throughpt are measured by CSR-MAN and SCSR-MAN Protocols. Also the CSR-MAN at freespace propagation model and CSR-MAN at two-ray ground propagation model compared using above parameters. Extensive simulations are conducted to analyze the performance of the proposed solution in both normal and malicious conditions. The nodes used in the simulations were based on IEEE 802.11 with different data rates such as 1, 2, 5.5 and 11 mbps. The application traffic consists of constant bit rate (CBR) with a radio range of 100 m. The source and destination nodes were randomly selected. The packet size used is 512 bytes. The random waypoint mobility model is used.

The Simulations are conducted by using graph compared by using node, Interval, Packet Size and speed with the parameters.

The Packet delivery Ratio of SCSR-MAN is more as compared with CSR-MAN.

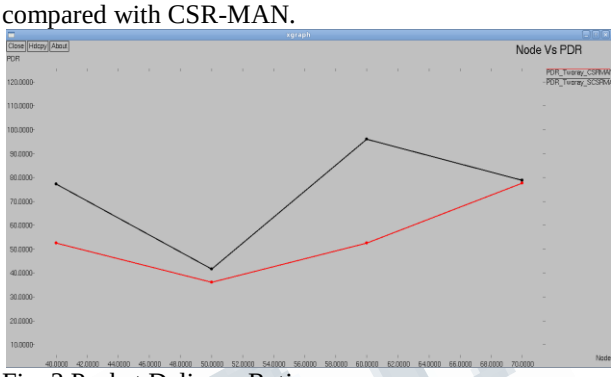

Fig. 3 Packet Delivery Ratio

Fig. 4 Delay

SCSR-MAN protocol shows less delay as compared with CSR-MAN protocol.

Dropping Ratio of SCSR-MAN is less as compared with CSR-MAN.

Packets dropped in SCSR-MAN protocol are less as compared with CSR-MAN protocol.

The Jitter is calculated which shows SCSR-MAN protocol gives less jitter as compared with CSR-MAN protocol.

The SCSR-MAN protocol gives more throughputs as compared with CSR-MAN protocol.

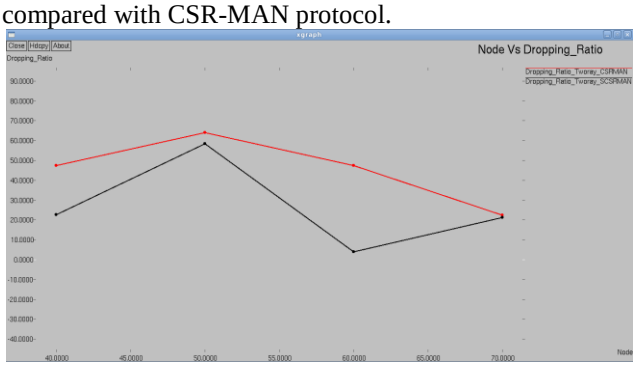

Fig. 5 Dropping Ratio

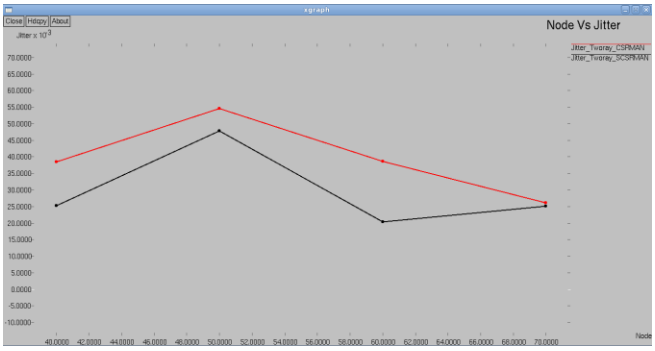

Fig. 6 Jitter

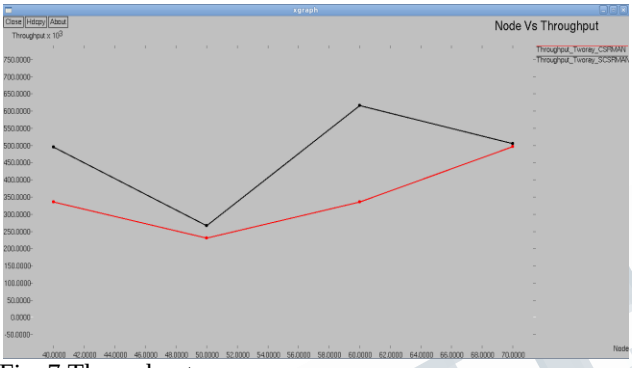

Fig. 7 Throughput

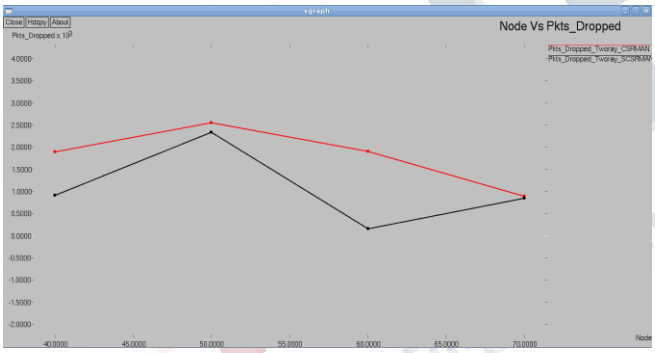

Fig. 8 Packets dropped

The all of the above graphs shows that the SCSR-MAN protocol gives good results as compared with CSR-MAN protocol. CSR-MAN is more secured as compared with AODV, SAODV protocol but SCSR-MAN gives more security than CSR-MAN.

CONCLUSION

Securing AODV is still an open area for research work. Conventional security techniques are not directly applicable to MANETs due to their very nature. SCSR-MAN is one of the steps towards securing and optimizing the routing performance of secured protocols with the help of cross-layer parameters that are shared to the network layer and with the help of Threat value parameter and digital signature at the network layer, the route is chosen with the most secure and optimal routing.

The performance of the SCSR-MAN is analyzed in the malicious nodes. The evaluations have showed that SCSR-MAN is better choice in highly mobile and malicious network environment. SCSR-MAN is not only secure, but also ensures and selects the most optima path having enough energy and bandwidth. Simulation results shows that SCSR-MAN gives better results as compared with CSR-MAN.I propose enhancement that is to provide secure cross layer approach from application layer to lower layers so that each layer will be secure and optimal routing should be there.

REFERENCES

[1] Sreedhar C, Dr. S. Madhusudana Verma, Dr. N. Kasiviswanath, " Cross-Layer Based Secure Routing In Manets" in Sreedhar C et al. Int. Journal of Engineering Research and Applications.ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.725-731.

[2] B. Ramachandran and S. Shanmugavel, "Received Signal Strength based Cross-Layer Designs in Mobile Ad-Hoc Networks", IETE Technical Review, Vol. 25. No. 4, pp. 192-200, 2009.

[3] M. Conti, G. Maselli, and G. Turi, "Cross-Layering in Mobile Ad-Hoc Network Design", IEEE Computer Society, pp. 48-51, Feb. 2004.

[4] Preeti Sachan and Pabitra Mohan Khilar , "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism",in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[5] Todd R. Andel, Alec Yasinsac, "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communications Surveys, 4th Quarter, No.4, 2007.

[6] Jiazi YI, Polytech'Nantes, "A NOTE ON THE SECURITY OF MANETS"March, 2008.

[7] P. Kiran Rao, Mrs. S. Vasundhara,"Channel Aware routin in MANETs with secure hash algorithm",International journal of scientific and Research publications,volume 2, issue 1,January 2012.

[8] T. S. Rappaport. Wireless communications, principles and practice. Prentice Hall, 1996.

[9] B. Ramachandran and S. Shanmugavel, "*Received Signal Strength based Cross-Layer Designs in Mobile Ad-Hoc Networks*", IETE Technical Review, Vol. 25. No. 4, pp. 192-200, 2009.