RESEARCH ARTICLE OPEN ACCESS

Cross-Layer Based Secure Routing In Manets

Sreedhar C*, Dr. S. Madhusudana Verma**, Dr. N. Kasiviswanath***
*(Department of Computer Science & Engineering, G. Pulla Reddy Engineering College, Kurnool)
** (Department of OR&SQC, Rayalaseema University, Kurnool)
*** (HOD, Department of Computer Science & Engineering, G. Pulla Reddy Engineering College, Kurnool)

ABSTRACT
The security of wireless networks has been a constant topic in the recent years. With the advance of wireless networks, building reliable and secure communication is becoming extremely important. Security is an essential requirement in Mobile Ad-hoc Networks (MANETs) to provide protected communication between mobile nodes. In this paper, we propose a novel security mechanism: Cross-layer based Secure Routing in MANETs (CSR-MAN). Cross-layer design is a promising method to satisfy the network requirements which has gained its popularity during the recent years. A cross-layer based secure routing mechanism is proposed in this paper which includes passing of the information from physical layer and MAC layer to the network layer. The route is selected based on the parameters obtained from the lower layers. An evaluation of this mechanism has been provided using simulations with ns-2. The simulation results illustrate good comparison of network performance parameters for different conditions.
Keywords - Cross-layer, MANETs, Routing, Security.

I. INTRODUCTION

MANETs are self configuring networks in which mobile devices connected by wireless links. These networks classify into infrastructure networks, where the 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 a critical issue in such areas [1] [2]. Many ad-hoc routing protocols have been proposed previously [3] [4] [5] [6] [7] [8], these protocols does not consider the security issues and requirements.

In this paper, we present a novel approach towards securing MANETs – Cross-layer based Secure Routing in MANETs (CSR-MAN) by considering the various parameters at the lower layers and thereby choosing the path at the Network layer. Ad-hoc On-Demand Distance Vector Routing protocol (AODV) is considered in this paper. AODV is a reactive protocol: the routes are created only when they are needed. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles and route information is stored in al intermediate nodes along the route in the form of route table entries. Route request (RREQ) is broadcasted by a node requiring a route to another node, route reply message (RREP) is unicasted back to the source of RREQ and route error (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbours.

Traditional packet based network architectures assume that communication functions are organized into nested levels of abstractions called protocol layers. Each layer implements a specific service: the architecture forbids the direct communication between non-adjacent layers, while the communication between adjacent layers works by using standard interfaces. Alternatively, protocols can be designed by violating the reference architecture, by allowing interactions and state information flowing among non-adjacent levels of protocol stack. Cross-layer design is said to be the violation of the layered architecture in order to get performance gains ink.

II. RELATED WORK

The A. J. Goldsmith have identified that cross-layer approach to network design can increase the design complexity [10]. The layered protocol is useful in allowing designers to optimize single layer design without complexity and concerning other layers. The cross-layer design must consider the advantages of the layering keeping some form of separation among the layers. Each layer is identified by certain parameters that are to be shared by the layers just above or below it. The parameter sharing of the layers assists in determining the operation modes that are suitable for application conditions, network, and current channel situation.

B. Ramachandran have discussed about a simple CLD between physical layer and MAC layer for power conservation based on transmission power control [9]. 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 [12]. 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.

As an optimization for the current basic AODV, in [11], a novel stable adaptive enhancement for AODV routing protocol is proposed, which considers joint route hop count, node stability and route traffic load as a route selection metric. A QoS routing protocol based on AODV to provide higher packet delivery ratio and lower routing overheads using a local repair mechanism is proposed in [13]. The received signal strength changing rate is used to predict the link available time between two nodes to find out a satisfying routing path in [14], which reports improvement in route connection time. In [15], route fragility coefficient (RFC) is used as routing metric, to cause AODV to find a stable route. Mobility aware agents are introduced in ad-hoc networks and Hello packets of AODV protocol is modified in [16] to enhance mobility awareness of node to force it to avoid highly mobile neighbour nodes to be part of routes and ultimately to reduce the re-route discovery. On receiving the Hello Packet with GPS co-ordinates of the originator, mobility agent compares them with previous ones and hence has awareness about the mobility of the originator with references to itself.

III. PROPOSED SOLUTION

It has recently become evident that a traditional layering network approach (separate routing, scheduling, secure communication and power control) is not efficient for ad-hoc wireless networks. Cross-layer is an escape from the pure waterfall-like concept of the OSI communications model with virtually strict boundaries between layers. The cross layer approach transports feedback dynamically via the layer boundaries to enable the compensation. In the original OSI networking model, strict boundaries between layers are enforced, where data are kept strictly within a given layer. Cross-layer design removes such strict boundaries to allow communication between layers by permitting one layer to access the data of another layer to exchange information and enable interaction. A cross-layer approach is proposed in this research to provide secure communication by obtaining the information from the lower layers and this information is used to best and secure communication. Cross-layer design breaks away from traditional network design, where each layer of the protocol stack operates independently. Cross-layering is not the simple replacement of a layered architecture, nor is it the simple combination of layered functionality; instead it breaks the boundaries between information abstractions to improve end-to-end efficient communication. Information in cross-layer architecture is exchanged between non-adjacent layers of the protocol stack, typically using a broader and more open data format. Cross-layering attempts to share information amongst different layers, which can be used as input for algorithms, for decision processes.

3.1 CROSS-LAYER PARAMETER: RSS

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. Mobility can be determined based on the connectivity changes with the neighbours. Connectivity change is found out using the value of RSS of the selected links. Mobility is defined as the average change in distance over the time between all nodes. When the mobility of nodes in a network is high, link errors can occur frequently and this results in high stale route information in the routing table. Selection of the routing at Network Layer is based on the high signal strength.

In the free space model, there exists a clear line-of-sight between the transmitter and receiver. The amount of transmit power also depends on the propagation model used. In the free space model, there exists a clear line-of-sight between the transmitter and receiver. The received signal strength (RSS) at distance d in this situation is defined as follows [40]:

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

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, therefore, is calculated as follows:

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

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 [40].

A neighbour table maintains neighbouring table at every node which contains the RSS, node id and

the time stamp. A neighbouring table entry consists of three fields:

- nodeID,
- RSS of the neighbor packet (estimated using equation (1)) and
- timestamp at which this packet was received.

The higher the RSS value, the more durable of the transmission and hence this parameter is considered as the parameter for optimal routing in the proposed solution. Security is provided at the Routing layer. Though the objective this research is to provide secure routing, it also aims at optimal and best available path among the various paths available from the source to the destination by considering the cross-layer parameters received from the lower layer to the Routing layer. The main objective of using the RSS as the cross-layer parameter is that, at the Network layer, the routing decision has to be made efficiently by judging the route with the node having high signal strength. Even though security is provided at the routing layer, if the signal strength is weak such that transmission of the packets cannot be done and in such case the idea of performance gain which is termed for the cross-layering is not achieved. Hence along with the security, the two cross-layer parameters are considered in this research for the better performance nodes in MANETs. AODV routing protocol has its own merits in selecting the efficient route. AODV does not consider the security mechanism. It is the issue of the researchers to provide strong security measures to thwart various attacks and cross-layering in one of the solution.

3.2 CROSS-LAYER PARAMETER: RSS

The goal of the cross-layer parameter A_{bw} is to find an optimal path such that the available bandwidth on the path is above the minimum requirement. Figure 1 describes the Abw cross-layer parameter which is used to compute the bandwidth constrained optimal path. The available bandwidth must be known on each link along the path. Throughputs can be measured by MANETs based on the IEEE 802.11 standards. However, these applications consume significant amounts of resources and can suffer from an inefficient and unfair use of the wireless channel. Therefore a new solution is needed which can pass this information to the Routing layer and in-turn routing decision is based on the requirement of bandwidth need for the communication. CSR-MAN routing process is based on the AODV routing protocol and uses security extensions at the Routing layer. Bandwidth measurements are realized according to 802.11 operations without influencing them. These measurements are thus passive and compatible with the reactive routing process. Figure 2 shows the possible network scenario for the process of calculating the Abw.

An estimate of A_{bw} is carried out at the sender side by calculating the relationship between the size of the measurement packet and the duration necessary to its transmission on the channel. The information of available bandwidth between two nodes is critical due to the dynamic topology of MANETs. A_{bw} is carried out at the sender side by calculating the relationship between the size of the measurement packet and the d_{SN} duration necessary to its transmission on the channel. Available bandwidth is given by the equation:

$$A_{bw} = D_l / d_{SN} \quad \text{------ (3)}$$

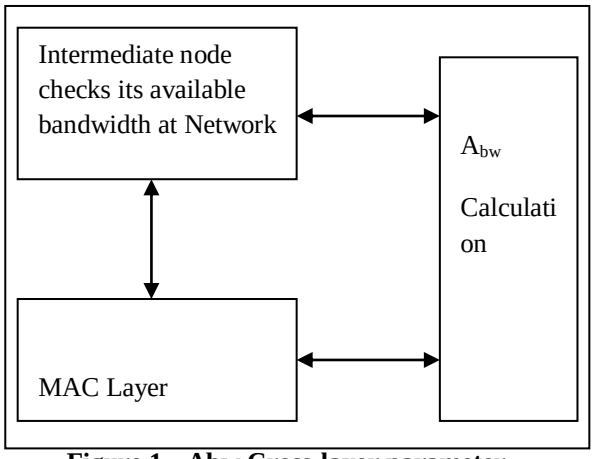

Figure 1. Abw Cross-layer parameter

A_{bw} indicates Available bandwidth; D_l indicates the Data length; d_{SN} 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, A_{bw} can be given as:

$$A_{bw} = D_l / T_{busy}+T_{cw}+T_{cst} \quad \text{---------- (4)}$$

Where T_{busy} corresponds to the sequence of the various Network Allocation Vector (NAV) timers imposed by the stations in emission, until the station has the right to emit, is directly a function of the traffic in the neighbourhood and interference zones.

T_{cw} is related to the backoff algorithm of 802.11 standard; T_{cst} known as Constant term is given by the equation:

$$T_{cst} = T_{rts} + T_{cts} + T_{mpdu} + 3T_{sifs} + T_{ack} + 4T_{phy} \quad \text{---- (5)}$$

The available bandwidth on the link is related to the sender's and receiver's neighbouring flows and also to the flows in the interference zone of the receiver. In the proposed solution, MAC layer calculates the available bandwidth and is passed to the Routing layer and at the Routing layer, along with the RSS value received; it selects the best and optimal route by choosing the highest RSS and the bandwidth. And at the Routing layer, calculation of Threat value parameter (T_{vp}) is done. The overall

path is chosen in such a way that the route with the highest RSS, bandwidth and lowest T_{vp} path is chosen. Figure 3 describes the overall flow of CSR-MAN. Nodes on receiving the messages at the PHY layer, it calculates the RSS and includes the timestamp.

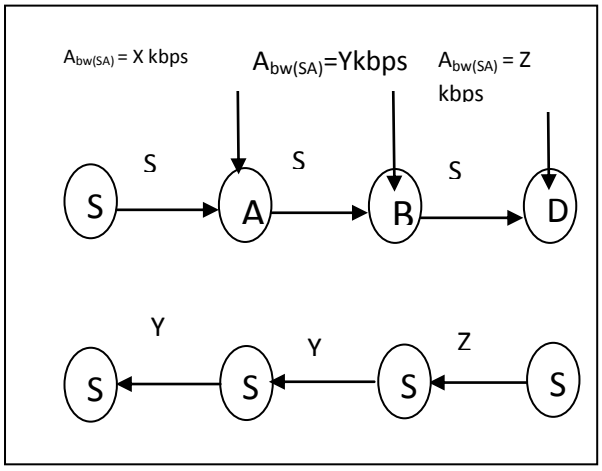

Figure 2. vailabe bandwidth calculation

Replay attacks are only counteracted if the timestamp field is included. An attacker which records messages to replay them later can only do so in the time interval between the timestamp and the MaxTimeDiff later. MaxTimeDiff indicates the maximum difference time intervals for a packet at the receiving node. It cannot replay the messages after this time interval. At the MAC layer, it obtains the nodeID and measures the bandwidth available. If the neighbour table has the entry for the nodeID obtained, then it creates the entry for the nodeID, RSS and timestamp. Else it updates entry of the RSS and timestamp.

3.3 THREAT VALUE PARAMETER CALCULATION

The Threat value Parameter (T_{vp}) is based on the parameters shown in Table 1. The table calculates the overall Tvp, which is required in proposed routing protocol for secure communication among nodes in MANETs and at the network layer, T_{vp} is calculated for the entire route. The path is selected in such a way that the node with less T_{vp} 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 neighbouring node. Drop values are the key factor in calculating the T_{vp}. Figure 4 describes the MANET scenario taken into consideration for the proposed solution.

The Threat value parameter (T_{vp}) is given by the equation:

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. The drop values of all the nodes along the route are calculated. Tvp is calculated for each route available during route discovery and is checked against the threshold value. The threshold value in this context 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 will not be suitable for further routing along the route which it is selected and an alternate path is selected for routing. Drop values are calculates such that the difference of total number of packets sent and total number received is performed division with the total number of packets sent.

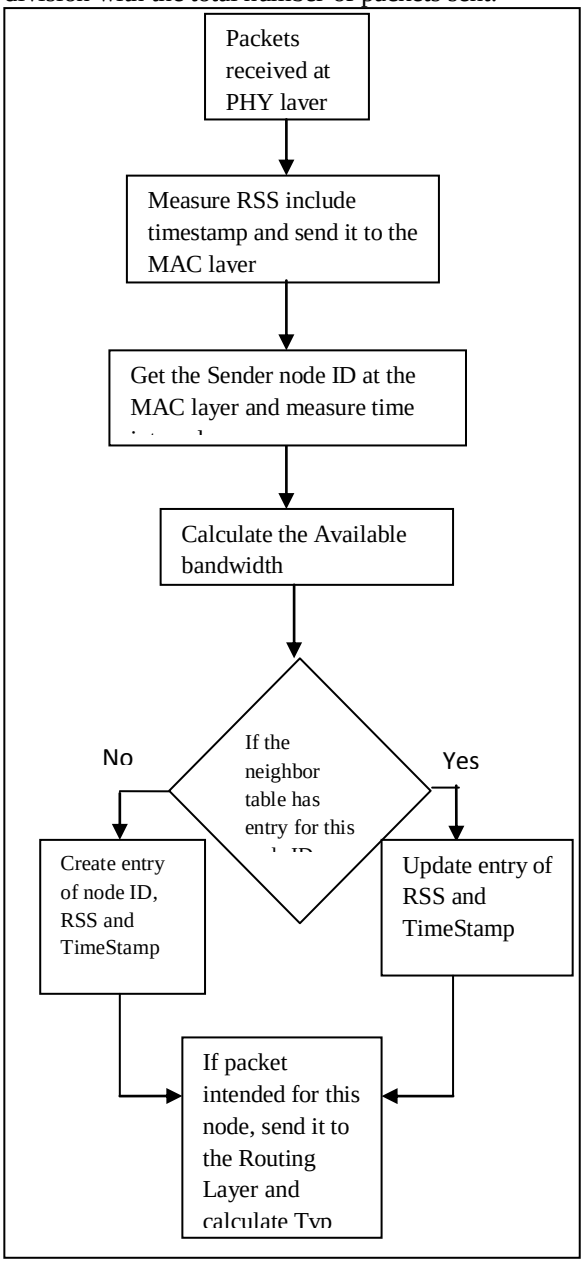

Figure 3. Abw Cross-layer parameter

In the proposed solution, it uses the on-demand principle of route discovery as the routes are discovered only when they are needed. The destination node selects the optimal route after receiving RREQ packets at the destination, which contains the information about the received signal strength, available bandwidth and the threat value parameter. 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 T_{vp} at the Routing layer.

The destination node receives seven RREQ packets, in which the values of T_{vp} are presented along with the various routes available to reach from the Source to the Destination as:

Route 1 : [1.4866]
Route 2 : [2.9625]
Route 3 : [2.2633]
Route 4 : [1.8166]
Route 5 : [3.94]
Route 6 : [3.97]
Route 7 : [1.82]

The destination node selects the most secure route Route 1, since it has the lowest threat value and unicasts RREP packet to the source node (SRC) and by considering the other two parameters received from the lower layers. In this context, T_{vp} is given the highest priority while selecting the path, when two or more paths has the same A_{bw} values. Packet loss is much more complicated in MANETs, because wireless links are subject to transmission errors and the network topology changes dynamically. A packet may lose due to transmission errors, no route to the destination, broken links, congestions etc. Packet loss due to transmission errors is affected by the physical condition of the channel, the terrain where networks are deployed, etc., which is beyond the scope of this research and is not discussed. They cannot be eliminated or reduced by improving the routing protocols. Several solutions are made for the packet loss due to broken links and congestions.

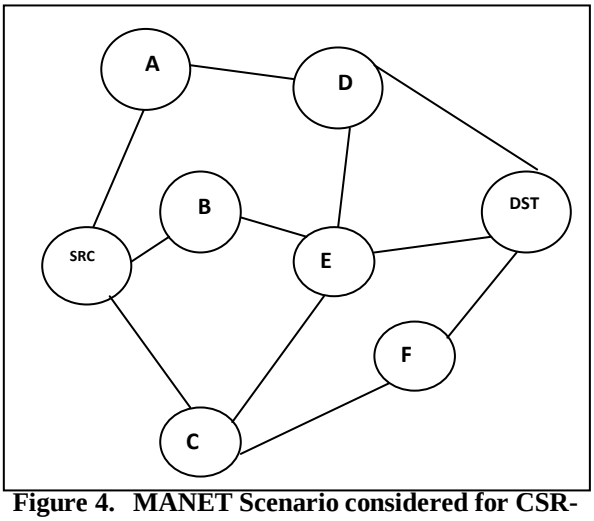

Figure 4. MANET Scenario considered for CSR-MAN

CSR-MAN proposes a new technique for securing the AODV by sharing the information from the PHY and MAC layer to the Routing layer and thereby selecting the best available and secure path. Table 8 describes the packet loss scenarios representing the number of packet sent, received and calculating the loss %, by the nodes under no attacks. It is made an assumption that the MANET is under malicious-free environment.

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. Table 1 describes the parameters used in our simulation. Figure 5 describes the end-to-end delay in our proposed solution. As the speed increases, the average delay of AODV increases when compared with the other two routing solutions. But in overall, CSR-MAN has less average delay when compared with AODV and SAODV. The average numbers of collected statistics are used to calculate the metrics, and then evaluate the performance of the three routing protocols namely AODV, SAODV and CSR-MAN. The following attacks and their impacts of the attacks upon these metrics are studied.

Table 1: Simulation Parameters

Simulator	NS2
Channel Type	Channel/Wireless Channel
Radio-propagation model	Propagation/TwoRayGround
Network Interface type	Phy/WirelessPhy
MAC type	Mac/802_11
Interface Queue Type	Queue/DropTail/PriQueue
Antenna Model	Antenna/OmniAntenna
Link Layer Type	LL
Routing Protocol	AODV
Simulation Area	500 * 400

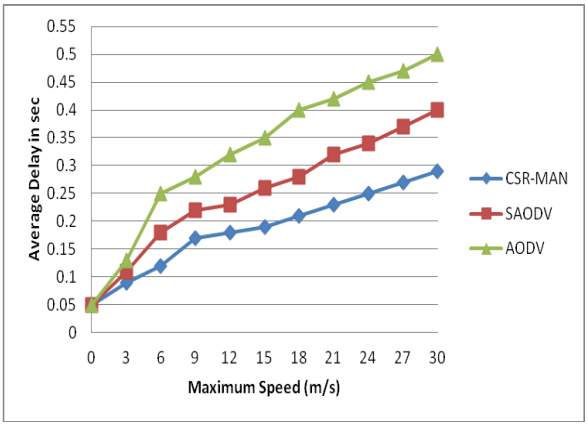

Figure 5. End-to-End delay

Extensive simulations are conducted to analyze the performance of the proposed solution in both normal and malicious conditions and compare it with SAODV (Secure ad-hoc on demand distance vector) and AODV routing protocols using NS-2. 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.

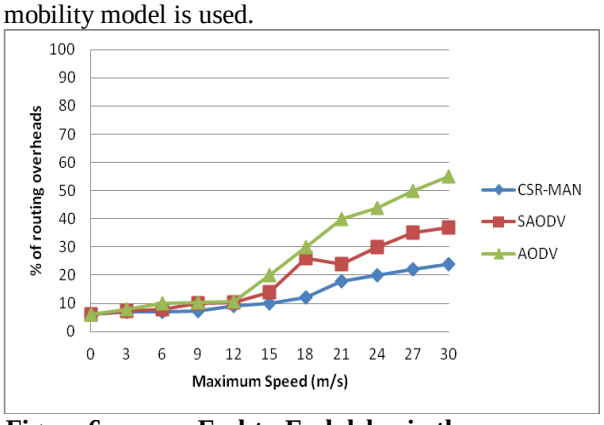

Figure 6. End-to-End delay in the presence of malicious node.

The average end-to-end delay in malicious environment for a network of 60 nodes is shown in Figure 6. Smallest end-to-end delay is observed in case of proposed solution. The end-to-end delay is increased quickly with increasing node mobility in AODV due to lack of alternate path. When an active route is broken, AODV initiates route discovery procedure again. SAODV has slight more end-to-end delay as compared to proposed solution due to involvement of cryptographic operations in route discovery.

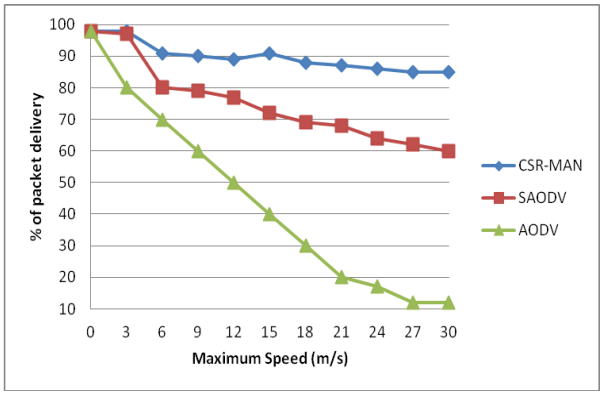

Figure 7. Packet delivery ratio in mobility in malicious environment

For each scenario, with the same type of attack and the same number of malicious nodes, simulations are run to collect the statistics. The simulations are diversified by changing the pause time value of the mobility model from 0 to 100 seconds. The average numbers of collected statistics are used to calculate the metrics, and then evaluate the performance of the three routing protocols namely AODV, SAODV and CSR-MAN. The following attacks and their impacts of the attacks upon these metrics are studied.

Extensive simulations are conducted to analyze the performance of the proposed solution (CSR-MAN) in both normal and malicious conditions and compare it with SAODV (Secure ad-hoc on demand distance vector) and AODV routing protocols using NS-2.

Figure 7 shows Packet delivery ratio in mobility in malicious environment. Initially all the three methods have the same delivery of packet rate. As the speed increases SAODV is better suited when compared with the AODV due to cryptographic methods used in providing security to the AODV. As the time increases further, CSR-MAN performs well, which is increased by over 70% compared with the normal AODV under malicious environment.

V. 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. The existing mechanism like SAODV is able to secure the protocol with its signature extensions. But the overhead of cryptographic computation still persist in the SAODV mechanisms. CSR-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 at the network layer, the route is chosen with the most secure and optimal routing.

The performance of the CSR-MAN is analysed in both the malicious nodes and non-malicious scenarios. The evaluations have showed that CSR-MAN is better choice in highly mobile and

malicious network environment. In black hole attack, some serious performance degradation has been observed in AODV protocol. Although SAODV is secure in nature but it is not resilient to packet dropping attacks. CSR-MAN is not only secure, but also ensures and selects the most optima path having enough energy and bandwidth. Researchers currently focus on developing new prevention, detection and response mechanisms for MANETs. To propose security solutions well-suited to this robust environment, it is recommended to the researchers to investigate possible security attacks and analyse the risks to the MANETs in a sophisticated manner.

Securing MANETs with help of cross-layer information exchange from the application layer towards the lower layers with the minimum overhead and finding the malicious activity as well as detecting and be eliminate at each layer which can lead to strong, secure and optimal routing can be considered as the future work.

To conclude, MANET security is a complex and challenging topic.

REFERENCES

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

[2] N.H Saeed, M.F Abbod, H.S Al-Raweshidy, "*Modeling MANET Utilizing Artificial intelligence*", Second UKSIM European Symposium on Computer Modeling and Simulation, EMS '08, Page(s):117–122, 8–10 Sept.2008.

[3] E.M. Belding-Royer and C.-K. Toh. *A review of current routing protocols for ad-hoc mobile wireless networks*. IEEE Personal Communications Magazine, pages 46–55, April 1999.

[4] D. Johnson, D. Maltz, Y.-C. Hu, and J. Jetcheva. *The dynamic source routing protocol for mobile ad hoc networks*. IEEE Internet Draft, March 2001. draft-ietf-manet-dsr-05.txt.

[5] S. Murthy and J.J. Garcia-Lunca-Aceves, "*An efficient routing protocol for wireless networks*". *ACM Mobile Networks and Applications Journal*, pages 183–197, Oct. 1996.

[6] V. Park and M. Corson, "*A highly adaptive distributed routing algorithm for mobile wireless networks*". In Proc. INFOCOMM, April 1997.

[7] C. E. Perkins and P. Bhagwat. "*Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers"*. Computer Communications Review, pages 234–244, Oct. 1994.

[8] C. E. Perkins and E. M. Royer, "*Ad hoc on-demand distance vector routing*". In IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.

[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.

[10] A. J. Goldsmith and S. B. Wicker, "*Design Challenges for Energy-Constraint Ad-Hoc Wireless Networks*", IEEE Wireless Comm., Vol. 9, No. 4, pp. 8-27, 2002.

[11] C. E. Perkins, E. M. Belding-Royer, and S. Das, "*Ad hoc On-Demand Distance Vector (AODV) Routing*", RFC 3561, July2003.

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

[13] Y.Zhang and T.A. Gulliver, "*Quality of Service for Ad-hoc On-demand Distance Vector Routing*". In proc. of IEEE International Conf. on Wireless Mobile Computing, Networking and Communications, vol 3, pp 192-193, 2005.

[14] R.S.Chang and S.J.Leu, "*Long-lived Path Routing with Received Signal strength for Ad-hoc Networks*". In proc. of 1st International Symposium on Wireless Pervasive Computing, 2006.

[15] G.Quddus et al., "*Finding A Stable Route Through AODV by Using Route Fragility Coefficient as Metric*". In proc. of International Conf. On Networking and Services, pp 107- 113, 2006.

[16] M.Idrees et al., "*Enhancement in AODV Routing Using Mobility Agents*", in proc. of IEEE.