Journal of Computer Science 7 (12): 1813-1818, 2011
ISSN 1549-3636


# Secure Enhanced Authenticated Routing Protocol for Mobile Ad Hoc Networks

[1]M.Rajesh Babu and [2]S.Selvan
[1]Department of Computer Science and Engineering,
PSG College of Technology, Coimbatore
[2]Principal, Alpha College of Engineering, Chennai, India

**Abstract: Problem statement:** This study propose an improvement of Ad Hoc on Demand Distance Vector (AODV) Routing protocol in order to include some of the aspects of ad hoc networks such as load balancing, congestion avoidance and avoidance of link breakage. **Approach:** The most important problem nowadays is link breakage which mainly occurs due to excessive load and congestion in the network. Each node contains a buffer in order to detect the congestion in the network. Thus it selects a route from source to destination to avoid congestion and balance the load. The threshold value is initially set to a pre-determined value. Once the buffer crosses the threshold value, then packet forwarding is carried out via alternate path. **Results:** As a result, the proposed protocol Secure Enhanced Authenticated Routing Protocol (SEARP) avoids congestion and balances the load to avoid link failure. **Conclusion:** By detailed simulation studies, we show that even in high mobility scenario, SEARP achieves better packet delivery ratio with reduced delay and overhead compared to AODV protocol.

**Key words:** Ad Hoc Networks, Load Balancing, wireless mobile nodes, link breakage, packet drop, secure enhanced authenticated routing protocol, Constant Bit Rate (CBR)

## INTRODUCTION

Ad hoc network is a collection of wireless mobile nodes. In ad hoc networks, there is no concept of centralized administration to manage some tasks such as security and routing; therefore mobile nodes must collaborate among themselves to accomplish these services. In addition, congestion forms the major reason for links to break. The load has to be balanced equally in order to avoid link breakage. The excessive load on the nodes causes the buffer to overflow which further leads to packet drop. This leads to packet delay and affects the packet delivery ratio. Load balancing also avoids congestion in the network. Thus any developed protocol must take all the above mentioned aspects of ad hoc networks into consideration to develop an efficient and effective routing or security protocol. In this study, we propose a Secure Enhanced Authenticated routing protocol (SEARP) for mobile ad hoc networks to avoid link failure using load balancing and congestion avoidance. The proposed protocol involves:

- Efficient security against route discovery attacks is provided using hop-by-hop signatures
- The load is balanced by determining the packet size
- When buffer crosses a certain threshold value, packets are forwarded via alternate path by which congestion is avoided

**Related study:** Ad hoc on demand Multipath Distance Vector is an extension to the AODV protocol for computing multiple loop-free and link-disjoint paths. The link failure of the route and mobility of the nodes are preemptively detected. Congestion which is the major reason for the link failure is avoided by Tan and Bose (2005), Idrees *et al.*, 2005 and Marina and Das (2001). Enhanced load balanced AODV routing protocol was proposed by Ahmad and Jabeen, 2011 to balance the load for AODV that improves overall network life, throughput and reduce average end-to-end delay. The mobile agent based congestion control AODV routing protocol (Hong *et al*., 2008) mainly focuses on congestion avoidance. Certain mobile agents are set which selects the less-loaded neighbor node as its next hop and the routing table is updated according to the congestion status of the node. Ad hoc on demand Distance Vector protocol (Perkins and Royer, 1999)

**Corresponding Author:** M. Rajesh Babu, Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, India Tel: 91-9843128310

finds routes on-demand and makes use of hop-by-hop technique to maintain routing table entries at intermediate nodes. In (Rajabzadeh *et al*., 2008), a probabilistic multi-path routing algorithm has been proposed and factors such as signal strength is being incorporated into the route metrics, which predicts link breakage before they actually occur in addition to signal strength and shortest path metrics. CA-AODV (Ramesh and Manjula, 2008) has proposed to ensure the availability of primary route as well as alternative routes to reduce route overhead. A Modified Routing Algorithm for reducing Congestion in Wireless Sensor Networks (Sengottaiyan *et al*., 2009) has proposed a conzone and it uses differentiated routing which reduces the traffic in the network to provide better service to high priority data. In DLAR (Lee and Gerla, 2001), the destination node sends the load information attached in the RREP packet to the source node. The primary route was taken as least congested route and load is balanced via primary route. Finally we summarize our findings and their importance.

## MATERIALS AND METHODS

In this study, we propose Secure Enhanced Authenticated routing protocol (SEARP) to avoid link breakage. It makes use of packet size and buffer size to detect the congestion in a particular node. The proposed protocol is very effective, as it also detects the malicious nodes quickly and it provides security for packet transfer.

In this proposed protocol, before the source node transfers the packets to destination, it should generate a temporary key pair. Using one-way hash function, the secret key list SS and public key by hashing the element of SS are the contents of temporary key pair. After key generation, the sender sends the public key to the appropriate destinations.

The source builds the verification information using SS list and it is included along with the route request. Once the intermediate node receives the request, it will first check for the verification information of the source using its PS. If the information is correct, the packet will be forwarded to the next node else discarded. Finally, when the route request reaches the destination node, the validity of the verification of source is checked by the destination node. If any information is found to be incorrect, the destination node discards the packet.

In order to improve the reliability of the route request packet, a MAC based authentication code is used. With the help of MAC value, the destination node can be easily identified if any changes are done to route request packet by the intermediate node. The destination node discards the packet if it is found to be changed. If all the verification is correct, the destination node sends the reply packet in the same way. In communication-related tasks, link breakage occurs due to overload, congestion. Therefore, buffer size has been set in each node to detect the congestion. Depending upon the buffer size, the packets are received by the node to transfer it to the destination.

**Route discovery process:** In the proposed protocol, once a node S wants to send a packet to a destination node D, it initiates the route discovery process by constructing a route request RREQ packet. It contains the source and destination IDs and a request ID, which is generated and a MAC computed over the request ID with a key randomly shared by the sender and the destination. When an intermediate node receives the RREQ packet for the first time, it appends its ID to the list of node IDs and signs it with a key which is shared with the destination. It then forwards the RREQ to its neighbors.

Let N1, N2….Nm-1 be the nodes, between the source S and the destination D. The route request process is illustrated below:

$$S \xrightarrow{\text{RREQ: } \left[S, D, MAC\left(Rid\right)\right]} N_1$$

$$N_1 \xrightarrow{\text{RREQ: } \left[S, D, MAC\left(Rid\right), \left(N_1\right), sign_{N1}\right]} N_2$$

$$N_{m-1} \xrightarrow{\text{RREQ: } [S, D, MAC\left(Rid\right), \left(N_1, N_2, N_{m-1}\right), \left(sign_{N1}, sign_{N2} \ldots sign_{Nm-1}\right)]} D$$

When the destination receives the accumulated RREQ message, it first verifies the sender's request id by recomputing the sender's MAC value, with its shared key. It then verifies the digital signature of each intermediate node. If all these verifications are successful, then the destination generates a route reply message RREP. If the verifications fail, then the RREQ is discarded by the destination. It again constructs a MAC on the request id with the key shared by the sender and the destination. The RREP contains the source and destination ids, the MAC value of the request id, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route.

When the intermediate node receives the RREP packet, it checks whether its id is in the list of ids stored by the RREP. It also checks for the ids of its neighbors in the list. The intermediate node then verifies whether 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 receives the RREP packet, it 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 source accepts the route. The source also verifies the request id that it sent along with RREQ packet. If it receives back the same request id from the destination, it means that there is no replay attack. If the source does not get the RREP packet for a time period of t seconds, it will be considered as route breakage or failure. Then the route discovery process is initiated by the source again.

The route reply process is illustrated below:

$$D \xrightarrow{\text{RREP: [S, D, MAC}(\text{Rid}), (N_1, N_2, \ldots N_{m-1}), (\text{sign}_D)]} Nm-1$$

$$N2_1 \xrightarrow{\text{RREP: [S, D, MAC}(\text{Rid}), (N_1, N_2, \ldots N_{m-1}), (\text{sign}_D, \text{sign}_{Nm-1}, \ldots \text{sign}_{N2})]} N1$$

$$N1 \xrightarrow{\text{RREP: [S, D, MAC}(\text{Rid}), (N_1, N_2, \ldots N_{m-1}), (\text{sign}_D, \text{sign}_{Nm-1}, \ldots \text{sign}_{N2}, \text{sign}_{N1})]} S$$

**Load balancing:** Load balancing is a methodology to distribute workload across multiple network links to achieve optimal resource utilization, maximize throughput, minimize response time and avoid overload. This is achieved by determining the maximum packet size to be forwarded in a single route. After route discovery process, the routes are maintained in the routing table. When a source node wants to forward the packet to destination node, it selects a least hop count route to forward the packet. Based on the size, the packets are forwarded. The packet size value is pre-determined to 512Mb. When the packet size is found to be less than the pre-determined value, then the packet is forwarded as a single packet. If the size of the packet is found to be larger, then the packet is segmented and sent through multiple less hop count routes.

The algorithm works in the following way:

Step 1: If packet size is less than or equal to 512Mb then
Step 2: Forward it as single packet
Step 3: Else, packet is segmented into 200Mb and sent via multiple less hop count path

This process balances the load equally by which frequent link failure has been avoided. But link failure can also occur due to congestion in the network. So we use congestion avoidance method to avoid congestion.

**Congestion avoidance:** Congestion occurs when a link or node is carrying so much data which reduces the quality of service. Congestion mainly results in packet loss, queuing delay and breakage of links. So link breakage can be avoided by congestion avoidance with verification of buffer size before forwarding the data packet. After packet size verification, the source node forwards the packet to the intermediate node. Each node consists of buffer and threshold value. The buffer represents the total number of packets present in the node. The buffer size frequently changes depending upon the number of packets sent or received in the network.

Each buffer consists of a threshold value which is set to 100%. Threshold value means the maximum number of packets that a queue will contain. The buffer size is set to 95% and the remaining 5% is left free in order to avoid overhead. When the source node forwards the data packet to its next intermediate node, intermediate node checks its buffer size. When buffer size is less than 95% of threshold value, the intermediate node receives and stores the data packet. It then forwards the data packet to its next node. When buffer size reaches 95% of threshold value, then load is balanced via alternate paths. Thus this process results in avoidance of congestion.

The algorithm works in the following way:

```
if (buffer_size < 95% of the threshold)
{   store the data packet
    forward it to the next hop
}    else
{    return back the data packet to the sender
     sender forwards the data packet to alternate
node}
```

Thus the algorithm avoids the congestion and balances the load by which link failure is avoided. The implementation of this novel approach avoids frequent link failure in ad hoc networks. The performance of the protocol has been evaluated and compared using Network Simulator (ns-2).

**Performance evaluation: Simulation model and parameters:**We investigated the performance by using the NS-2 (2.33) simulator, which is considered to be the most powerful and effective tool to test the performance of network protocols for both conventional and wireless networks by giving all possibilities to test all possible scenarios. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. We have compared the original version of AODV with our proposed version to prove the utility of our improvement.

In our simulation, 100 mobile nodes move in a 1000×1000 meter square region for 50 sec 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 minimal speed is 5 m $sec^{1}$ and maximal speed is 10 m $sec^{1}$. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in the following Table 1.

**Performance metrics:** We evaluate 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 SEARP with the AODV protocol in presence of malicious node environment.

## RESULTS AND DISCUSSION

Based on Malicious nodes: In our first experiment, we vary the no. of misbehaving nodes as 5, 10, 15, 20 and 25. Figure 1 shows the results of the delivery ratio for the misbehaving nodes 5, 10, 15, 20, 25 for 100 nodes. From the results, it is clear that SEARP scheme achieves more delivery ratio than the AODV, since it has both reliability and security features. Figure 2 shows the average delay for the misbehaving nodes 5, 10, 15, 20, 25 for 100 nodes. From the results, it is clear that SEARP scheme has lower delay than the AODV because of authentication routines. Figure 3 shows the results of routing overhead for the misbehaving nodes 5, 10, 15, 20, 25 for 100 nodes. From the results, it is clear that SEARP scheme has less routing overhead than the AODV, since it involves route re-discovery routines.

**Based on pause time:** In our second experiment, we vary the pause time as 40, 50, 60, 70 and 80 with 5 attackers for 100 nodes. Figure 4 shows the results of Delivery Ratio of the packet. From the results, it is clear that SEARP scheme has the better delivery ratio than AODV, since it has both reliability and security features. Figure 5 shows the results of average end-to-end delay. From the results, it is clear that SEARP scheme has slightly lower delay AODV because of authentication routines. Figure 6 shows the results of routing overhead. From the results, it is clear that SEARP scheme is slightly less routing overhead than AODV since it involves route re-discovery routines.

Table 1: Simulation settings and parameters

| No. of nodes | 100 |
|---|---|
| Area size | 1000×1000 |
| Mac | 802.11 |
| Radio range | 250 m |
| Simulation time | 50 sec |
| Traffic source | CBR |
| Packet size | 512 |
| Speed | 5 m $sec^{1}$ t 10 m $sec^{1}$ |
| Misbehaving nodes | 5, 10, 15, 20, 25 |
| Pause time | 40, 50 60, 70, 80 |

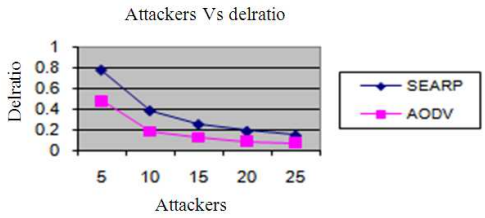


Fig. 1: Attackers Vs delivery ratio

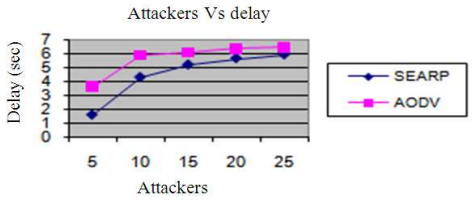


Fig. 2: Attackers Vs delay

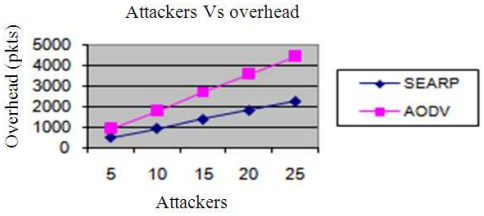


Fig. 3: Attackers Vs overhead

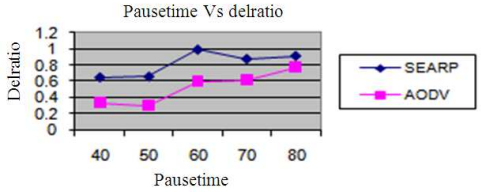


Fig. 4: Pause time Vs delivery ratio

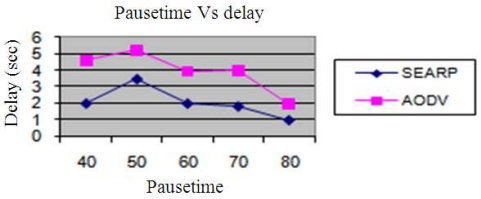


Fig. 5: Pause time Vs delay

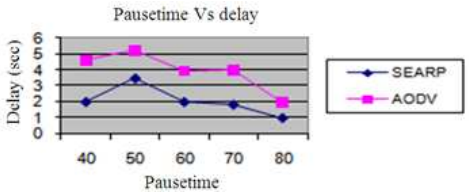


Fig. 6: Pause time Vs overhead

## CONCLUSION

In mobile ad hoc networks, an attacker can easily disrupt the functioning of the network by attacking the underlying routing protocol. Though several secured routing protocols have been proposed so far, all of them have certain disadvantages. This study has presented the design and evaluation of SEARP (Secure Enhanced Authenticated routing protocol), a new ad hoc network routing protocol which avoids link failure. It balances the load and avoids congestion in the network by choosing non-congested routes to send data packets. When congestion occurs in the node, data packets are transferred through alternate path. Thus it avoids congestion and balances the load to avoid link failure.

## REFERENCES

Ahmad, I. and H. Jabeen, 2011. Enhanced load balanced AODV routing protocol. Int. J. Comput. Sci. Inform. Security, 9: 98-101.

Hong, L., D. Chu, M. Wang and S. Li, 2008. Mobile Agent based congestion control AODV routing protocol. Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, Oct. 12-14, IEEE Xplore Press, Dalianl, pp: 1-4. DOI: 10.1109/WiCom.2008.612

Idrees, M., M.M., Yousuff, S.W. Jaffry, M.A. Parsha and S.A. Hussain, 2005. Enhancements in AODV routing using mobility aware agents. Proceedings of the IEEE Symposium on Emerging Technologies, Sep. 17-18, IEEE Xplore Press, Pakistan, pp: 98-102. DOI: 10.1109/ICET.2005.1558862

Lee, S.J. and M. Gerla, 2001. Dynamic load-aware routing in ad hoc networks. Proceedings of the IEEE International Conference on Communications, June 11-14, IEEE Xplore Press, Helsinki, Finland, pp: 3206-3210. DOI: 10.1109/ICC.2001.937263

Marina, M.K. and S.R. Das, 2001. On-Demand multipath distance vector routing in ad hoc networks. Proceedings of the International Conference on Network Protocols, Nov. 11-14, IEEE Xplore Press, USA, pp: 14-23. DOI: 10.1109/ICNP.2001.992756

Perkins, E.C. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans, LA , USA., pp: 90-100. DOI: 10.1109/MCSA.1999.749281

Rajabzadeh, M., F. Adibniya and M. Ghasemzadeh, 2008. MA-DSR; Multi agent based adaptive DSR protocol with intelligent behavior in realistic environments. Proceedings of the International Symposium on Telecommunication., Aug. 27-28, IEEE Xplore Press, Tehran, pp: 306-311. DOI: 10.1109/ISTEL.2008.4651319

Ramesh, B. and D. Manjula, 2008. CA-AODV: Congestion adaptive AODV routing protocol for streaming video in mobile ad hoc networks. Int. J. Commun. Network Syst. Sci., 1: 322-328.

Sengottaiyan, N., R. Somasundaram and S. Arumugam, 2009. A modified routing algorithm for reducing congestion in wireless sensor networks. Eur. J. Sci. Res.., 35: 529-536.

Tan, C.W. and S.K. Bose, 2005. Modifying AODV for efficient power-aware routing in MANETs. Tencon IEEE region, 1-6. DOI: 10.1109/TENCON.2005.300970