An authenticated encrypted routing protocol against attacks in mobile ad-hoc networks

C.C. Suma [1], H.L. Gururaj[2], B. Ramesh[3]
[1] PG scholar, Dept of CS&E, Malnad College of Engineering, Hassan, India
[2]Assistant Professor, Dept of CS&E, Malnad College of Engineering, Hassan, India
[3] Professor, Dept of CS&E, Malnad College of Engineering, Hassan, India
[1]suma.yadav20@gmail.com, [2] Gururaj1711@gmail.com, sanchara@gamil.com[3]

Abstract

Mobile Ad hoc Network is stated as a cluster that contains Digital data terminals and they are furnished with the wireless transceivers which are able to communicate with each other with no need of any fixed architecture or concentrated authority. Security is one of the major issues in MANETs because of vast applications such as Military Battlefields, emergency and rescue operations[10]. In order to provide anonymous communications and to identify the malicious nodes in MANETs, many authors have proposed different secure routing protocols but each protocol have their own advantages and disadvantages. In MANTE's each and every node in the communicating network functions like router and transmits the packets among the networking nodes for the purpose of communication[11]. Sometimes nodes may be attacked by the malicious nodes or the legitimate node will be caught by foemen there by controlling and preventing the nodes to perform the assigned task or nodes may be corrupted due to loss of energy. So, due to these drawbacks securing the network under the presence of adversaries is an important thing. The existing protocols were designed with keeping anonymity and the identification of vicious nodes in the network as the main goal. For providing better security, the anonymity factors such as Unidentifiability and Unlinkability must be fully satisfied[1]. Many anonymous routing schemes that concentrate on achieving anonymity are proposed in the past decade and they provides the security at different levels and also provides the privacy protection that is of different cost. In this paper we consider a protocol called Authenticated Secure Routing Protocol proposed which provides both security & anonymity. Anonymity is achieved in this protocol using Group signature. Over all by using this protocol performance in terms of throughput as well as the packet dropping rate is good compared to the other living protocols.

IndexTerms: ***Anonymity, Authenticated routing,Mobile-ad-hoc networks(MANETs),Group signature.***

I. Introduction

MANET can be defined as a network that contains self-configurable mobile nodes that are connected by wireless links with no access point. In MANETs, each mobile node functions as a router and forwards the routing packet from one node to another for the purpose of communication. Every mobile node is autonomous in nature and they have the ability to move from here to there within the communicating network. So, MANETs have frequently changing dynamic topology and the breaking of communication link is common in the network. MANETs have wide varieties of applications, namely Wireless Sensor Network, Military Battlefields [3], Device Networks, Tactical networks and many. Some challenges as well as the design issues are there to overcome regardless of attractive applications of MANETs. Here exist many security vulnerabilities that are related to security in MANETs.

The example for MANETs that consists of wireless mobile nodes can be seen through an example shown in the below Figure 1.1.Whenever a sender node wants to transmit the information to receiver node which is not reachable from its transmission range[2], then the sender node will initiate the routing process. The Route discovery process identifies the optimum route from sender to the receiver node. Here the intermediate nodes play an important role and they have the responsibility to forward the packets from one node to another node within communication range.

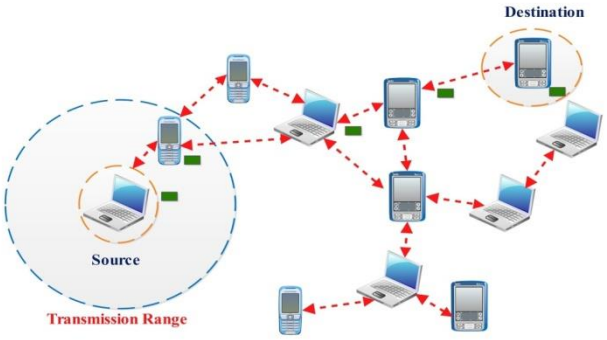

Figure 1.1: Infrastructure less network

II. Related work

Much work has been done in anonymous routing and provide short appraise on the living protocols.

The ad-hoc on-demand distance vector (AODV) routing protocol is based on DSDV and DSR algorithms [4].it uses the periodic beaconing and sequence numbering procedure of DSDV and similar route discovery procedure as I DSR. However there are two major differences between DSR and AODV. An important feature of AODV protocol [5] is the maintain ace of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired not used recently.

The propose of a novel anonymous on-demand routing protocol, called MASK, which can concurrently accomplish anonymous MAC-layer and network-layer communications. The newness of this protocol deceit in the use of active pseudonyms rather than static MAC and network addresses. It offers sender and receiver anonymity as well as sender-receiver affiliation anonymity [6]. Specifically, adversaries might monitor a packet transmission, they cannot establish actual network IDs of its sender and receiver, nor can they choose if (or when) any 2 nodes in the network are communicating. In addition, It ensure node unlocatability and intractability, meaning that, although adversaries might know some real network IDs and/or group memberships, they be unable to decide whom and where the corresponding nodes are inside the network. Moreover, it ensures end-to-end flow intractability [8], Means those adversaries cannot trace a packet onward to its final destination or backward to its original source, nor can they recognize packets belonging to a same continuing communication flow.

The DSR protocol allows nodes to vigorously discover source path crossways numerous network hopes to any destination in the ad-hoc network. Every data packet sent then carries in its header the accomplished, ordered list of nodes all the way through which the packet must move, achieved packet routing to be trivially loop-free[7], and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded .by including this source route in the header of each data packet other nodes forwarding or over caption any of these packets may also with no trouble cache this routing information for further use.

III. Methodology

3.1 Problem Statement

Many researchers and the many users for the mobile ad hoc network have been increasing drastically in the recent years. Providing security for the communicating network is an intense concept in MANETs. Many advance techniques and applications are built in the MANET field, so it is necessary to make available efficient and protected communication in the adversarial surroundings. The more is the network security and performance; more will be the advantages from it.

The protocol considered in this project aims to achieve the goals of Anonymity that are not satisfied in other existing protocols. Some of the existing protocols are not capable to authenticate packets so adversaries find one or the other way to track the information in the communicating network [9]. By considering all these issues the

protocol implemented in this project is aiming to give anonymous communications and improved performance in terms of throughput and packet loss ratio as compare to other existing protocols.

3.2 Objective

The aim of this paper is to achieving the anonymity goals and to protect against attacks under the presence of adversaries. It also aims to provide improved performance in terms of throughput and the packet loss rate as compare to existing protocols. Source node and the destination node identities cannot be revealed to any intermediate nodes or the adversary nodes in the network. Route anonymity: Route identities such as the path from source node to destination node cannot be recognized by any intermediate node or the adversary nodes.

3.3 Protocoldesign

3.3.1 Network topology

Consider the below network topology as shown in figure 3.3.1 which consisting of five-nodes for illustrating the proposed protocol. In the below topology S is the source node which needs to send data to the destination node D, so S initiates the route discovery process for discovering path to D **.**

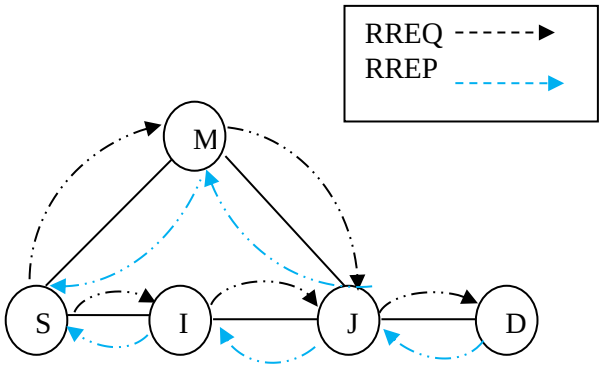

Figure 3.3.1 Network topology

3.3.2 Anonymous Route Request

1) Source node: Whenever the sender node S wants communicate and send some information to the destination node then it will look up into its routing table for checking whether it has the available path to the intended destination. If it doesn't have the active way to the destination then it'll initiate the way discovery method. Supply node at the start is aware of the knowledge regarding D, as well as this anonym, public key, and destine. The destine 'dest'is a binary string that indicates the node as "this is the destination" and may be familiar by D [5]. If there's no session key then it'll generate a new replacement period key K_{SD} for the safety organization among the source & destination node. Subsequently it'll update its destination table as shown within the below table 3.3.2.1

Table 3.3.2.1: Destination table of source node S

Des	Des.str	Des.Pub_key	Session key
N_D	Des	K_{D+}	K_{SD}

Then sending RREQ, source node S establishes an original entrance in its routing table as shown in the table 3.3.2.2.

Table 3.3.2.2: Routing table of source node S

Req	Des	Ver_Mes	Next node	state
N_{sq}	N_D	V_D	N/A	awaiting

2) Transitional node: RREQ packet beginning S is floated in **T**. The intermediate node I encounters the RREQ packet as shown within the Figure 3.3.2.3 Every intermediate node has the neighborhood relationship with each intermediate node within the network, that the node I has the neighborhood relationship with S and and

it aware of wherever the RREQ packet comes from. The table 3.3.2.3 shows the entries that are kept in I's neighborhood table of node S.

Table 3.3.2.3: Neighborhood table of source node S

Neighbour_Nym	Session_Key
N_S	K_{SI}
N_J	K_{IJ}

Table 3.3.2.4: Routing table of transitional nodes

Req_Nym	Dest_Nym	Ver_Msg	Next_hop	State
N_{sq}	N/A	V_D	N/A	Routing

3) Destination Node: When the destination node D receives RREQ packet then it'll validates the packet equally to the intermediate nodes I or J. Since D will decode the part of V_D, it realizes that it is the destination of the RREQ. D will acquire the session key K_{SD}, the validation nonce N_v, and therefore the validation key K_v. Then, shown in table 3.3.2.5 D is prepared to bring together an associate RREP packet to reply to the S's route request.

Table 3. 3.2.5 Routing table

Req.Nym	Dest.Nym	Ver.msg	Next_hop	status
N_{sq}	N/A	VSD	N/D	Active

3.3.3 Sending RREQ

It takes packets made by source node as input and logically processed it and verifies the RREQ packet and fat last destination node receives the RREQ packet. RREQ packet made by the source node

The RREQ packet is transmitted within the network per procedure shown in the figure 3.3.3.1

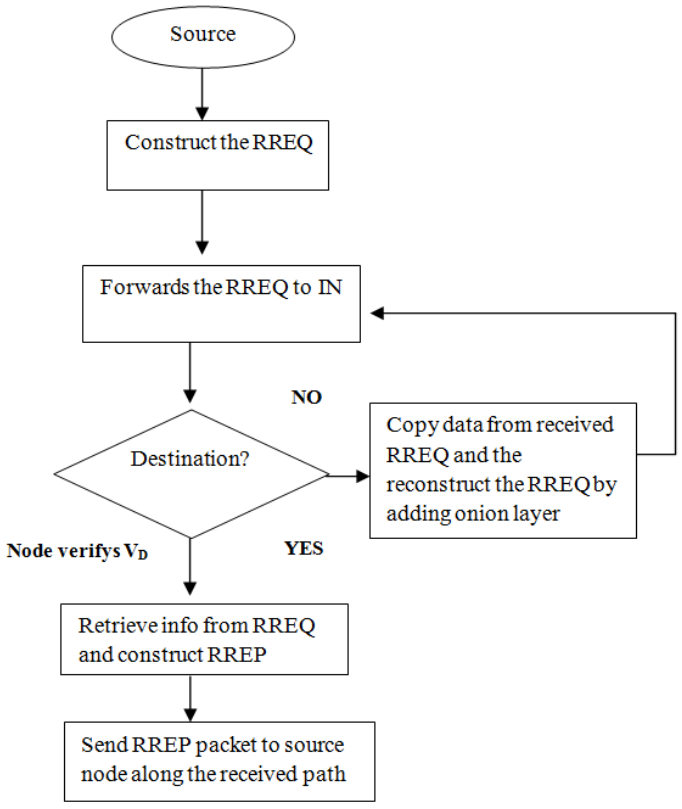

Figure: 3.3.3.1 Flow chart for sending RREQ

3.3.4 Sending RREP

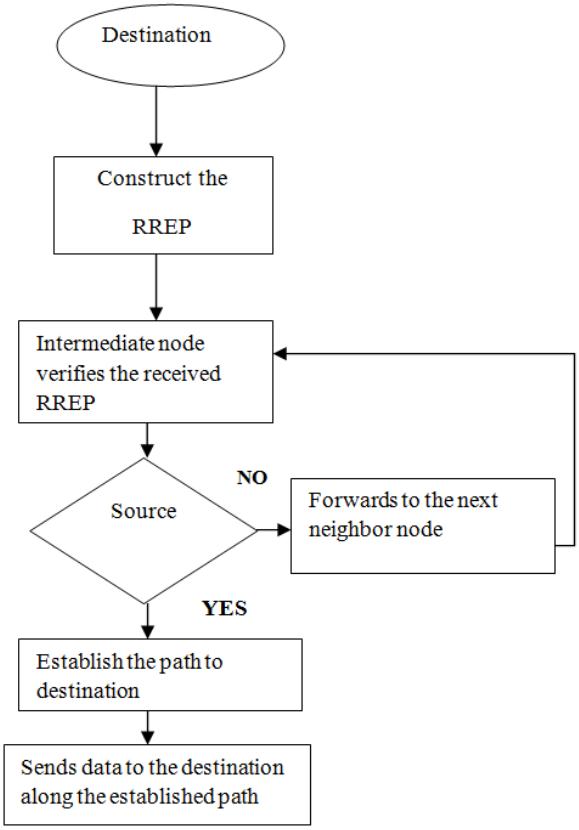

Figure 3.3.4.1: Flow chart for sending RREP

The RREP packet B transmitted in the network according to the procedure shown in fig 3.3.4.1. It takes packets constructed by destination node as input and logically processed it decrypting the outer onion part in the RREP packet nodes will forward the RREP to their neighbor nodes and RREP packet reaches the source node.

IV. Result analysis

The proposed AASR protocol has been implemented by the Network Simulator2 (NS2). It is mainly used to implement the routing protocols in the networking explore. The main focal point of our analysis is security and privacy under malicious nodes. Several performance parameters are used in the valuation of routing protocols. They represent different characteristics of overall network performance. Here 2 metrics are evaluated and used in comparisons to study their outcome on the overall network performance. These metrics are packet loss ratio and Average Throughput.

Packet loss ratio

It is stated as the rate between the numbers of packets lost to number of packets lost and the number of packets of received. The figure 4.1 shows the packet loss ratio comparison under malicious nodes. Compared with existing protocols AASR provides lower packet loss ratio in different mobile scenarios in the presence of adversarial attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio.

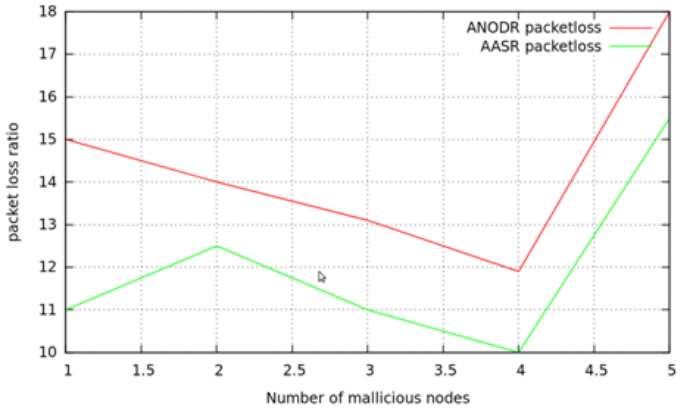

Fig 4.1 Packet loss ratio comparison under malicious nodes

Throughput

It is stated as the total number of delivered data packets divided by the total duration of simulation time. The figure 4.2 shows the comparison of Throughput between the existing and the proposed protocol. It can be observed that throughput of the proposed protocol is better compare to the existing protocol

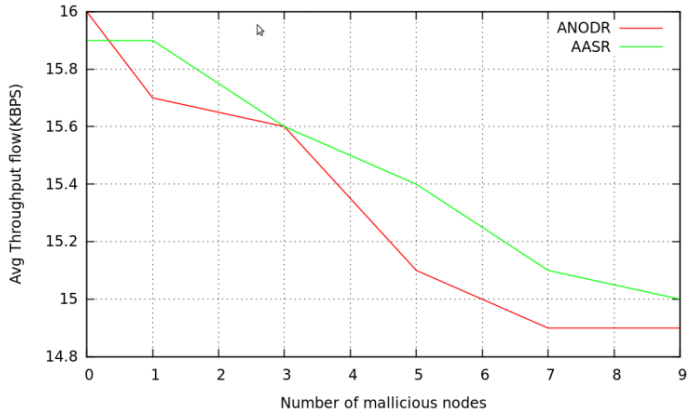

Fig 4.2 Avg Throughput comparisons under malicious nodes

V. Conclusion

The AASR protocol introduces the efficient way to anonymize the entire wireless communication in presence of adversaries. The protocol identifies the malicious node effectively and aims to provide security for finding path, routing and data transmission. From the simulation and analysis results, the packet loss ratio of the proposed system is efficient than the existing system and Throughput of the proposed system is better compare to existing anonymous protocols. So, from these evaluations the protocol is best for higher Packet Delivery Ratio consideration and it efficiently identifies the malicious nodes in presence of Adversaries, limited transmission power and partial dropping.

In future work, routing overhead can be reduced and the Throughput of the protocol can be increased using trust based routing. Another future aim is to consider the Average Routing overhead for the performance evaluation along with the previously considered parameters.

References

[1] D,R. Raimes, R.win, B. Mullins, and S. Brimaila, “Towards a taxonomy of wired and wireless anonymous networks,” in *Proc. IEEE ICC*, Jun. 2009, pp. 1–8.

[2] C. kerkins, E. Velding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” IETF RFC 3561, Jul. 2003. Available: www.ietf.org/rfc/rfc3561.txt

[3] D.J.son, Y. Hu, and D. Baltz, “The Dynamic Source Routing Protocol (DSR) for MobileAdHocNetworks for IPv4,” IETFRFC4728, Feb. 2007. [Online]. Available: www.ietf.org/rfc/rfc4728.txt

[4] J. Jong and X. Kong, “ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks,” 2003, pp. 291–302.

[5] J. Jong, Y. Kong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[6] A. koukerche, K. El-Khatib, Xu, and Korba, "SDAR: A secure distributed anonymous routing protocol for wireless and mobile adhoc networks," in *Proc. IEEE Int. Conf. LCN*, Nov. 2004, pp. 618–624.

[7] R.Song, L. \Korba, and G. Yee, "AnonDSR: Efficient anonymous dynamic source routing for mobile ad hoc networks," in *Proc. ACM Workshop SASN*, Nov. 2005, pp 33–42

[8] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Mar. 2005, vol. 3, pp. 1940–1951.

[9] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2376–2386, Sep. 2006.

[10] K.E. Deafawy and G. Tsudik,"privacy-preserving location-based ondemandd routing in MANETs"IEEE J.sel.Area communication based vol 29,no.10.pp.1926-1934,Dec.2011.

[11] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE transactions on vehicular technology, vol. 63, no. 9, November 2014.