E-SHARP: Enhanced Secured Hierarchical Anonymous Routing Protocol for MANETs

Sheikh Abdul Wajid
Research Scholar
Department of CSE,SDDIET
Golpora, Barwala, Haryana

Kiran Gupta
Assistant professor
Department of CSE, SDDIET
Golpora, Barwala, Haryana

ABSTRACT
MANETs are a type of wireless networks, typical choice for communication and data sharing. As the application field for MANETs widens so does the need for secure data transmission. Due to limitations posed by wireless and decentralized nature of MANETs the routing protocols proposed for MANETs are vulnerable to different types of attacks. Hence anonymous routing protocols are proposed that provides security and anonymity for secure communications. In this paper we are working on a protocol called E-SHARP which basically secures the data communication between the nodes, where the network is divided into clusters. The problem with underlying protocol SHARP is that it does take in to account the malicious node activity which is done by the nodes within the cluster. The Sharp protocol is improved in this work by adding the concept of helper nodes in the protocol which confirms the data routed internally by nodes is malicious or not by confirming with help of helper node. The proposed techniques evaluated using simulation. Our study shows that it is possible to guarantee a desired level of anonymity with intra and inter cluster data security.

General Terms
Routing, Security in MANETs, Clustering

Keywords
RSA, SHARP, E-SHARP, Anonymity, MANETs

1. INTRODUCTION
A mobile ad hoc network consists of group of nodes that communicate with each other without any membership criteria .The nodes are self organizing and network is decentralized in nature. MANETs are infrastructure-less type of wireless networks, they are not based on any predefined access points. The nodes in the network act either as source, destination or intermediate forwarders. Since, increasing use of MANETs for widespread applications especially for sharing sensitive information require data to be routed safely from one node to other. To provide secure communication in MANETs we require anonymous routing protocols that provides anonymity of source, destination and the path from source to destination. If the anonymity is not provided then there are more chances of attacks and in such a case it becomes much easier for the intruder to compromise the network and perform the traffic analysis. Anonymity means to hide the real identity of real source, destination and that of route. Hiding the route identity involves that in no case any intruder should be able to trace back the path of data packet to its previous node or to the source. The different routing protocols for MANETs are vulnerable to various attacks both from internal and external intruders. The standard routing protocols proposed for data communication does not provide any security features. Advancements in MANETs have made it necessity to provide secure routing protocols for sharing sensitive data and secure communication. So there is need for anonymous routing protocols that provide essential security features. One such anonymous routing protocol proposed is E-SHARP that provides secure communication in MANETs. The contribution of the proposed protocol is as follows:

- SHARP is taken as underlying protocol which itself takes AODV [5] as standard routing protocol. We add additional features to SHARP to achieve the desired level of anonymity. For multi hop communication the intermediate nodes are selected based on distance between intermediate node and the destination.
- The whole network is partitioned into clusters based on coordinates and their range such that one hop neighbours are grouped as one cluster. Inter and intra cluster security is implemented. The data is routed outside cluster in encrypted form using RSA encryption algorithm.

2. RELATED WORK
MANETs are open choice for communication for wide areas of application including disaster areas and battle fields for military applications where fixed infrastructure is not viable. The military and battle field applications require secure communication. For this purpose anonymous routing protocols are used in MANETs. Anonymity provides privacy to source, destination and to routes. The openness and distributed nature of MANETs does not restrict the membership of nodes. So the intruder can easily attack the network. Many anonymous routing protocols proposed so far are not able to provide complete anonymity altogether. Most of routing protocols use geographical routing protocols as underlying routing protocol and are location based [6][9-12]. Various anonymous routing protocols proposed are as:

Secured hierarchical anonymous routing protocol (SHARP) an anonymous cluster based routing protocol. Here, the nodes are grouped based on the distance and location of nodes. The node and its one hop neighbors are grouped together. Each group maintains a Group identifier all the inter group communications are based and are encrypted by RSA encryption. Outside of cluster there is no identity of actual source and destination. Hence, SHARP provides source, destination and route anonymity [1]. An anonymous energy efficient routing protocol that partitions the network in zones and then chooses random relay nodes that act as intermediate nodes to forward data packets EARP. There is random selection of nodes that always leads to the formation of un-detectable route. EARP has methods to counter Sybil and timing attacks .the underling protocol of EARP is Energy Aware Greedy Perimeter Stateless Routing Protocol [2]. DD-SHARP based on two underlying protocols, Anonymous location-based and efficient routing protocol (ALERT [4]) and Greedy Perimeter Stateless Routing protocol (GPSR) has been proposed. ALERT [4] is based on bursty traffic and node

to node hop encryption. GPSR follows greedy method to forward packets using the one hop neighbors information. Simulation results have shown that efficiency of proposed protocol DD-SHARP has improved [3]. A variant of ALERT has been proposed as S-ALERT [13] that implements suspect detection algorithm to avoid any black hole problem. Anonymous Routing Protocol for Mobile Ad Hoc Networks (ARM) a secure routing protocol that during route discovery process generates datagram consists of destination ID, generated secreted and private key, TTL and pseudonym. RREQ is then broadcasted, intermediate nodes upon receiving this message generate a new link ID and append it to RREQ, each field is encrypted with public key of destination. During RREP datagram field is decrypted. Hence ARM provides complete anonymity for communication in MANETs [8]. The first anonymous routing protocol for MANETs proposed was ANODR. The communication is based on shared key between source and destination. Source generates trapdoor identifier encrypting a message with shared key. There is an onion encryption by the successive intermediate nodes. Each successive node adds its own public key. Destination is able to open the trapdoor and replies by generating a new link key that is encrypted with the public key of previous node [7]. In SHARP the communication between the clusters is secured by cryptography technique using RSA encrypted transmission of messages as proposed in [1]. The packet is identified by the cluster ID not the sender ID. Thus receiving node cannot know about the node from which data is coming it can only know about the cluster ID. Thus anonymity is preserved and the network is prevented from the external attacks. However, in the cases where the attacker has already compromised an internal node, maintaining anonymity becomes a very tedious task. In the cluster based data transmission approach in SHARP if the internal node has been compromised, the source node cannot know of it. The transmission of the data within the cluster can be impacted. The malicious internal attacker upon receiving the data will drop the packets consequently breaching the security. So while external attacks are taken care of by maintaining the anonymity and using the cryptographic approach, the internal attacks need to be given focus. In this work we tend to prevent the network from the internal attacks.

3. PROPOSED MODEL

The proposed protocol provides secure anonymous data routing between source and destination. The protocol considers partitioning of network into different clusters. Each cluster is made based on range of the nodes and the geometrical coordinates of the individual nodes such that a node and its single hop neighbor are put in one cluster. Each cluster maintains it unique identity by its group id and all the inter group communications are based on this id. When data needs to be routed between source to destination which are at multi-hop distance then the intermediate nodes are selected randomly for the path to remain dynamic and unpredictable. The random nodes selected act as forwarding nodes. There comes two types of communication one within the cluster and other between different clusters. For inter group communication data packets are encrypted using RSA. The encryption is done at group level so that even the last node may identify the destination. This reduces the time delay as incurred if otherwise encryption done at node level. This ensures inter cluster anonymity. For intra group communication the use of helper nodes identifies the malicious node if present. Helper nodes are randomly selected and is the only node in the cluster that knows the ID of source. When data is to be sent by a source it first selects random helper node the Id of helper node is then broadcasted to the nodes of neighboring cluster. Then the source randomly selects a intermediate node within the cluster other than helper node and data is encrypted before data is send outside the cluster .The destination upon receiving the data communicates with helper node in source cluster, which then forwards the information about data to source that verifies about the data packets forwarded by the intermediate node. Hence, provides intra group security.

4. METHODOLOGY

1. First the network will be divided into clusters.
2. When the source node has some data to forward to destination, it will choose random node which will be referred to as helper node. The ID of the helper node will be visible to the nodes outside the cluster of the source node. The helper node will be used to check the proper flow of the data between the nodes within the cluster. The data will be sent out of the cluster using RSA cryptography so that anonymity of the sender can be maintained.
3. From its one hop neighbour nodes, the source node will choose a random node and will inform it by sending the hello message of its election as the helper node. The helper node must forward its ID to the any random node in the next cluster which upon receiving this ID will broadcast it to all the members in the cluster.
4. So before the data transmission starts, the helper node ID will be available to the every member of the next cluster.
5. In second step, the source will choose another node randomly from its one hop neighbours to send the data. The helper node chosen by the source node will not be used for the purpose of the data forwarding.
6. The source node will send few packets to the relay node. For example if source node has to send 100 packets to destination node, then first it will send the 10 packets to the relay node so that its malicious nature can be checked.
7. If this relay node is packet dropping node then it will not forward the data properly to the next cluster. It can drop few of the packets, it can drop all the packets also.
8. After the relay node has sent first block of data to the node in the next cluster, then the node which has received the packets in the next cluster must inform the helper node about number of packets received by it.
9. The helper node will inform the source node about the received information. The source node will check if the relay node has forwarded data properly or not.
10. Case 1: If the data received in the next cluster is significantly less than what is sent by the source node, then the source node will choose another random relay node from its one hop neighbours to forward the data.
11. Case 2: If the relay node has properly forwarded the data, then the source node will keep on sending the remaining data to the same relay node.
12. Case 3: If the helper node itself is malicious node and does not inform the source node about the required information then after waiting for a particular amount of time (when the source node has sent the first block of data and has not received any information from the helper node) the source node will put the helper node in

the malicious node list and will choose another helper node. The process will again start from step3.

13. Same procedure will be followed by the node in the other clusters until data reaches the destination node.

5. RESULTS

In this paper we have simulated E-SHARP protocol in MATLAB with the concept of helper nodes. Initially we deploy 504 nodes partitioned in 9 clusters. The implementation of helper nodes inside clusters enhances the chances of catching the malicious nodes when selecting an intermediate node within cluster. We evaluate packet delivery ratio, drop ratio and throughput for both the proposed system and the existing system. The experimental show that the packet delivery ratio for proposed system is more than existing system since the malicious nodes are indentified prior to selecting path for data sending from source to destination. Hence, the drop ratio for proposed system is much less than existing system. Finally, throughput is calculated and the results show that it is more for E-SHARP.

1) Packet delivery ratio

$$PDR = \frac{Packets\ \ delivered}{packeys\ \ sent}$$

2) Drop ratio

$$D = 1 - PDR$$

3) Throughput

$$TH = (initial\ energy - energy\ consumed)/packets\ generated$$

A) Plot for Packet Delivery Ratio Vs Rounds

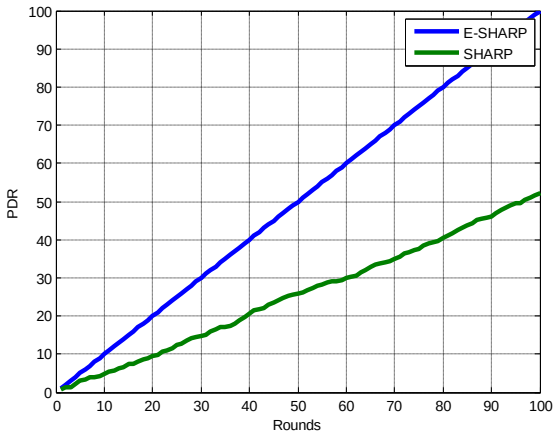

Fig 1: PDR Comparison

B) Plot of Throughput

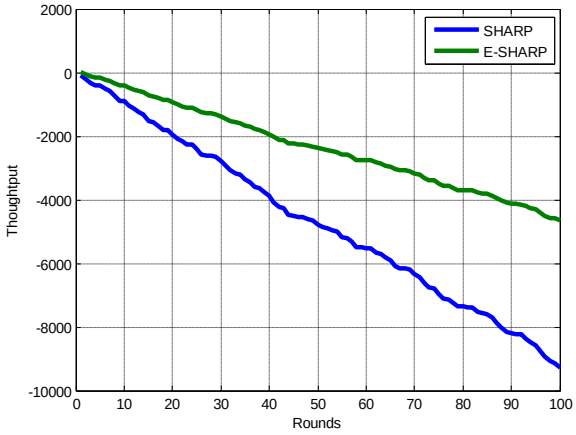

Fig 2: Throughput comparison

C) Calculation of Drop Ratio

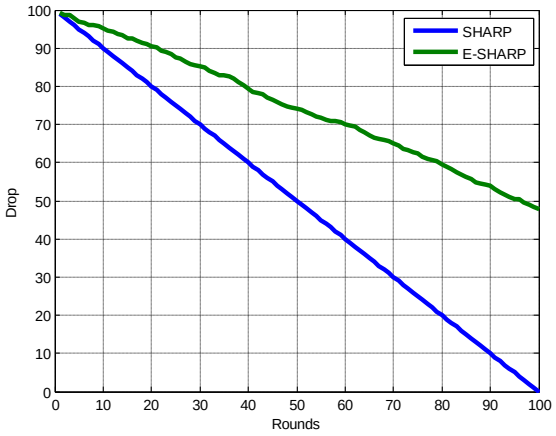

Fig 3: Drop Comparison

6. CONCLUSION AND FUTURE SCOPE

The proposed protocol will provide much greater anonymity for secure communication. Experimental results show that packet delivery ratio is more in E-SHARP also it assumes less drop ratio. The protocol achieves security at two levels. For inter cluster communication the data is encrypted by RSA method and For intra cluster security helper node inside the cluster enhances the chances of catching the malicious node in the internal communication of the network clusters. The helper nodes are selected on the bases of the random selection process. The route selection process starts from the source node which selects the helper node. There can be enhancement in the encrypting technique which will involve less routing overhead. Also techniques can be incorporated that can ease in detecting other types of attacks like eavesdropping.

7. REFERENCES

[1] Remya S., Lakshmi KS. 2015 SHARP : Secured Hierarchical Anonymous Routing Protocol for MANETs" , International Conference on Computer Communication and Informatics, IEEE

[2] S. Kalai Selvi, Ganeshkumar 2014 EARP: Energy-aware Anonymous Routing protocol in MANETs, International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), IEEE.

[3] Imran,S., Karthick,RV., Visu,P. 2015 DD-SARP: Dynamic data secure Anonymous Routing Protocol for MANETs in attacking environments, International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), IEEE

[4] Khasnikar,AK. 2015 Anonymity protection using ALERT in MANET, International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), IEEE.

[5] Manel Guerrero Zapata 2002 Secure ad hoc on-demand distance vector routing.(SecAODV) ACM SIGMOBILE Mobile Computing and Communications Review.

[6] Defrawy,KE., Tsudik,G. 2007 ALARM: Anonymous Location- Aided Routing in Suspicious MANETs, Proc. IEEE Intl Conf. Network Protocols (ICNP).

[7] Hong, JKAX. 2003 ANODR: Anonymous On Demand Routing with Untraceable routes for Mobile Ad-hoc Networks. In: 4th ACM International Symposium on Mobile Ad hoc Networking and Computing, MOBIHOC.

[8] Seys, S., Preneel, B. 2009 ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks. International Journal of Wireless and Mobile Computing.

[9] Karim El Defrawy, Tsudik,G. 2011 Privacy-Preserving Location-Based On-Demand Routing in MANETs, IEEE Journal on selected areas in communications, December.

[10] Wu,X., Liu,J., Hong,X., and Bertino,E. 2008 Anonymous Geo- Forwarding in MANETs through Location Cloaking, IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309.

[11] Xiaoqing Li, Hui Li, Jianfeng Ma and Weidong Zhang 2009 An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks, Fifth International Conference on Information Assurance and Security.

[12] Lanjun Dang, Jie Xu and Hui Li 2010 DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks, IEEE Asia-Pacific Services Computing Conference.