2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

Preventing DOS & MITM Attacks in "Anonymous Location Based Efficient Routing Protocol" in MANET

Priyanka Patil
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
Email: patilpp6990@gmail.com

Nilesh Marathe
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
Email: nilesh.marathe@rait.ac.in

Vimla Jethani
Dept. of Computer Engineering
Ramrao Adik Inst. of Technology
Nerul, Navi Mumbai, India
Email: vimlajethani@gmail.com

***Abstract*—Mobile Ad Hoc Networks (MANETs) gained lot of importance due to fast growth of the businesses and used in different applications such as military, entertainment, commerce, emergency services etc. Because of openness and decentralization feature of the MANET, nodes of the MANET can be vulnerable to malicious entities. Hence, anonymity becomes one of the important aspects in MANET. In last few years, a lot of research has been carried out by different researcher to prevent the anonymity of the MANET. Different routing protocols have been evolved such as GSPR, AO2P, ALARM, PRISM and ASR to secure the anonymity of the MANET. But all of these protocols have some limitations regarding providing complete anonymity of source, destination or routes and also involving high cost. To overcome above issues ALERT protocol is evolved which is distinguished by its low cost and anonymity protection for sources, destinations, and routes. But ALERT protocol is not providing security against the active attacks, so in the proposed work we have decided to make the strategy to prevent the DoS and Man in the middle attacks on ALERT by using Hash function with SHA-1 algorithm.**

Keywords—Mobile ad hoc networks, Vulnerability, Anonymity, ALERT.

I. INTRODUCTION

The rapid growing businesses in today's world, understands the advantages of the new technologies of computer networking. The wireless communication helps big firms for their better growth. A mobile ad hoc network (MANET) is a self-motivated distributed system of wireless nodes that move independently of each other. It consists of large number of mobile nodes where each node moves independent of its location as topology of the collection changes dynamically. The nodes in the network can join or leave the network at any time. This network is temporary and infrastructure-less network. In MANET security is the most significant aspect for the protected communication. The malicious entities in the network can attacks on the nodes in the MANET and collect important information from the network. Because of this high security is important in MANET. The anonymous routing protocols are developed in order to secure the network by disclosing the information about the identities as well as location of the source and destinations. Also it provides the security against the routing path. MANET is applicable in military battle field, sensor networks, commercial sectors, medical sectors.

978-1-4673-9916-6/16/$31.00 ©2016 IEEE

Currently, the MANET is not having faultless security strategy. It is most significant to offer secure communication between parties in the MANET and the secure solution which should be dynamic and also free from various attacks. There are various protocols evolved in MANET which provide anonymity. The different protocols like AO2P, ALARM, and ZAP etc. have been evolved for secure routing. But, this protocol generates extensive cost in providing the anonymity. Because of such condition, it has been needed to develop a protocol which should be cost effective and high anonymity.

The rest of the paper is organized as follows: types of routing protocols, vulnerabilities, attacks and the related works with existing routing protocols are discussed as literature review in section 2; section 3 discusses the ALERT protocol; proposed solution is discussed in section 4 and section 5 discusses the conclusion.

II. LITURATURE REVIEW

A. Types of Routing Protocols

Due to infrastructure-less of network MANET faces challenge of routing. Routing in MANET is to search and maintain routes between nodes in a dynamic topology with probably unidirectional links, using minimum number of nodes. There are three types of routing protocol of MANETs as shown in Fig.1 [1]. First is Proactive protocol (Table driven) that maintains fresh lists of destinations and their routes by intermittently allocating routing tables throughout the network. This protocol is not good for highly mobile nodes because it can take large amount of bandwidth to share data with other node due to distance vector routing. Another disadvantage is that table size becomes big and high memory required in case of about big networks. On Demand or reactive routing protocols intend to overcome the drawback in the proactive protocols by maintaining the only routes which are active at that moment. It means routes are maintained for the nodes which are active currently and sending data packets

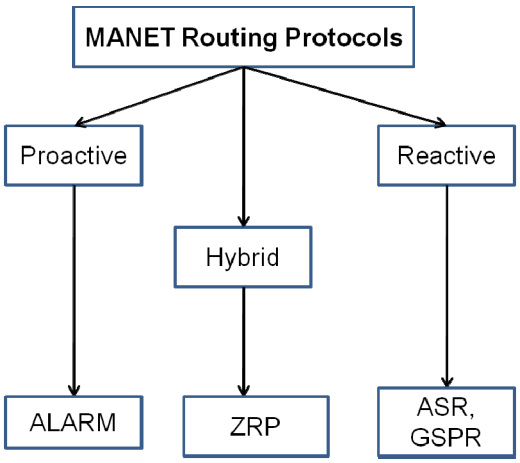

Fig. 1 MANET Routing Protocols.

from source to destination. Third Hybrid gives the advantages of both the above protocols by providing initial routing by proactively and further routing reactively for active nodes.

B. Vulnerabilities in MANET

Vulnerability is a flaw in security system. Some of the vulnerabilities are as follows [2]:-

1. Absence of infra-structure: MANET does not have a centralized monitor server. Due to lack of management detection of attacks is difficult.
2. Scalability: Due to mobility of nodes, the network size also continuously varies. So it is a main problem regarding security. So, to avoid this problem, security system should capable of handling a big network as well as small ones.
3. Cooperativeness: Routing protocols always consider that nodes are supportive and non-hazardous.
4. Dynamic topology: Due to dynamic behavior of the nodes in the network, it trust relationship gets disturbed between the nodes. Some nodes are found as compromised nodes, this condition may also lead to disturbing the trust relationship.
5. Bandwidth constraint: Link exist with changeable low capacity than wireless network which are more susceptible to outside noise, intervention and signal reduction effects.
6. No predefined Boundary: Due to no predefined boundary nodes are allowed to join or leave the network. Because of this adversary can able to communicate with nodes as soon as it comes in the range of adversary node

C. Attacks in MANET

Due to such vulnerable nature of the MANET, the chances of the attacker to perform the attack on the network increases. There are two types of attacks; external and internal attacks. In case of internal attack, attacker performs attack directly on the node and may provide wrong routing information to other nodes. In External attacks, attacker is from outside of the network. In his attack normal communication cannot be done by users in the network. The types of external attacks are as follows [3];

a) Passive attacks:

This type of attacks will not cause any problem within the network or to routing protocol. It tries to accumulate key data from the network by illegal listening.

b) Active attacks:

Active attacks may cause by outside sources which not belong to the network or may cause by internal malicious nodes which are in the network. The internal attacks are hazardous than external attacks because it provides unauthorized entry to network. It helps attacker to create jamming in the network and try to modify the network. Malicious nodes act with other nodes as they have nearest path to destination. Some common types of attacks in MANET protocols are as follows;

i. Denial-of-services (DoS): In this attack, attackers denied access of the service to real users. This attack can be internal or external.
ii. Eavesdropping: This is a passive attack where attacker or malicious node observes and draws the confidential information like location, public key, private key, password etc.
iii. Black hole attack: Malicious nodes act with other nodes as they have nearest path to destination.
iv. Man-in-the-middle attack: Malicious node puts itself between source and destination and captures all packets and modifies them.

D. Anonymity in MANET

Anonymity does not disclose the node information such as identity to attackers. The anonymous [4] protocol should protect the relationship between source and destination; the location and identities of the sender, receiver and the intermediate nodes. It should help in such way that adversaries will not able to trace a massage to its sender or receiver. The nodes need to validate each other without knowing their real identity [5].

E. Related Work

Geographical secure path routing protocol (GSPR) [6] secure location based services under vehicular ad-hoc networks(VANET).This protocol preserves privacy by geographically routing messages through unidentified nodes to destination locations. GSPR uses cryptographic one-way hash functions. Results shown that, the proposed protocol ignored the malicious nodes by increasing routing path length. This protocol is also able to maintain a low loss rate even when the large numbers of nodes are malicious.

The PRISM protocol [7] is a reactive routing protocol. In this protocol, the node tracing is prevented from internal and external adversaries by using supports anonymous reactive routing within suspicious location based MANETs. The PRISM prevents node tracking, reliability of routing massage.

An ALARM [8] is topology based proactive routing protocol. Each node develops the map of the route which will not get disclosed, because here each node communicates with authenticated neighbors.

In AO2P [9] receiver contention scheme is used for deciding the next hop with minimum information. In this scheme when source sends request to neighbors, then if any one of neighbor receives that request it argue for its next hop in routing. At the receiver side, receiving nodes are categorized into number of types. The node which will be nearer to destination by position that will be get higher priority. Then after route establishment, pseudo identifier having temporary identity is used for data transfer. Anonymity for a destination depends on the complexity of corresponding a geographic position to a real node identity.

In paper [10], author proposed a novel packet coding techniques that combine multicast and onion-based packet encryption. Proposed technique provides both global and local anonymity solutions. To reduce traceability author separates the packets, and their headers, change at each hop. Influence the wireless or open nature of the radio channel to add supporting works to create those mechanisms further capable in hiding communications in network.

Anonymous Secure Routing (ASR) protocol [11] provides the protection of discovered routes from passive attacks and active attacks.

The protocols discussed in the above sections are having several limitations. Some protocols like GSPR, ASR, PRISM, and AO2P not able to provide anonymity against. Most of the protocols are uses encryption based on the public key. Hence this protocol provides anonymity with high cost. So, it has become necessary to develop protocol which can give full anonymity with low cost.

III. "ALERT-ANONYMOUS LOCATION BASED EFFICIENT ROUTING PROTOCOL"

"ALERT" protocol provides anonymity to for sources, destination, and route. Also the cost involved is low. In ALERT, network field is randomly gets divided into zones, which may be vertical or horizontal as shown in Fig. 2 and 3 [12].

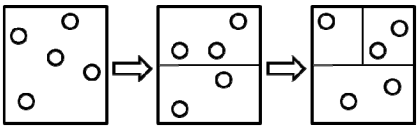

Fig. 2.HorizontalPartitioning [12]

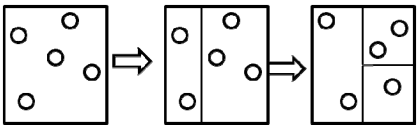

Fig. 3.VerticalPartitioning [12]

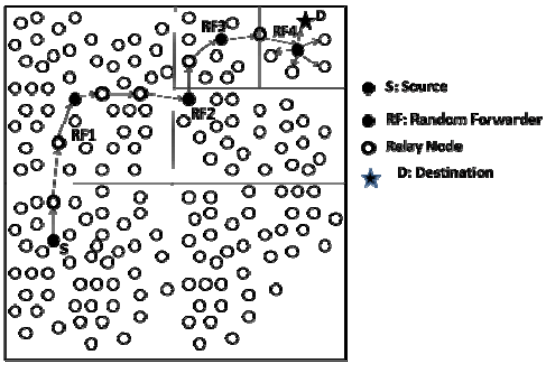

Fig. 4 Routing among zones [13].

The partitioning is carried out in each step of routing, where source or intermediate forwarder try to separate itself from destination zone. In the next step, it selects node of the other zone randomly as the next replay node. Then the data is passed to relay node with GPSR algorithm. In destination zone the data is broadcasted to k node by providing anonymity to the destination. . It gives untraceable anonymous route by randomly selecting the nodes in zones which as shown in Fig. 4[13].

A. Dynamic Pseudonym

Instead of using its real MAC address ALERT uses dynamic pseudonym as its node identity. So attacker can-not copy node's reality. For avoiding pseudonym collision, hash function like SHA-1 used. Here hashing is performed for real MAC address and current time stamp of node. Additionally to avoid re calculation of pseudonyms by adversary, timestamp must be predefined. In addition, by creating more complications to calculate timestamp for an attacker, ALERT uses randomness of timestamps. As a result, the pseudonyms cannot be simply regenerated. To foil adversaries from associating the pseudonyms each node pseudonym expires after definite instance of time.

If pseudonyms are changed excessively again and again, the routing may get disturbed. Furthermore if pseudonyms are changed rarely, the adversaries can find out respective pseudonyms of node. As a result pseudonym modification should be regularly and suitably determined. If pseudonyms change occurs periodically, then it updates its new position and pseudonym to its neighbors. At the same time, each node records the routing table so as to keep its neighbors' pseudonyms related with their locations.

ALERT uses cryptography to hide the packet content. Data is transmitted by using symmetric key encryption. There is only one secrete or symmetric key between source and destination. When source sends data to destination the data is encrypted by destinations public key and decrypted by its own key. Thus, the packets communicated between source and destination may be effectively and safely defend using symmetric key [14].

B. Source, Destination & Route Anonymity

ALERT makes stronger privacy preservation for source (S) and destination (D) by the unlink-ability of the communication endpoints and the transferred data. Namely, S and D cannot be related by the packets in their communications by attackers. ALERT includes the "notify and go" method to avoid an intruder by identifying exactly which node surrounded by source has sent out the packets. As well ALERT provides k-anonymity to destinations by hiding destination node D along with the k receivers in destination zone ZD. So, an eavesdropper can find in order to destination zone, but it can-not find out exact destination node position from the packets and nodes in path. ALERT provide route anonymity by its randomly relay node selection, which prevents an attacker by grabbing packets or revealing susceptible nodes [14].

C. Prevention of Attacks

1) Timing Attacks:

Here, an attacker can observe the packets transmitted among S and D during packet departure and arrival times. After this surveillance, the attacker can find out S and D. ALERT uses the "notify and go" method in source zone. At the destination zone the broadcasting is used. Because of such arrangement, intruder can-not find out source and destination. Moreover, the routing path between a given S-D and the time stamp changes frequently. As a result intruder again gets into trouble to find out source and destination [14].

2) Counter Intersection Attacks:

In this scheme, attacker observes the active users constantly at a specified time. This can help the attacker to find out the position of source and destination. Even though ALERT has k-anonymity approach to hide information of destination node, attacker can find out destination by continual watching node movement and long communication. Because in long communication destination node remain active all time. This is the intersection attack. To avoid intersection, the ALERT confuses the attacker and making it infrequently fail to monitor destinations reception of packets. Here multicasting is used instead of direct broadcasting. As soon as packet 1 reaches to destination zone, random forwarder multicasts packet to some of the nodes in destination zone. These nodes hold the packet 1 until packet 2 reaches to destination zone. Then the nodes which had the packet 1 perform one hop broadcasting in order to hide destination. Hence intersection attack is prevented [14].

D. Drawbacks of ALERT

ALERT is not providing security against the active attacks. It uses dynamic pseudonym and hashing of real MAC address of node and timestamp. If pseudonyms are changed constantly, the routing may get disturbed; and if pseudonyms are changed rarely, the adversaries may succeed to find out attacks, also to create a new pseudonym in short time is hard task, so that makes ALERT inefficient. ALERT uses symmetric key cryptography AES (Advanced Encryption Standard) algorithm where shared key can be decrypted by strong attacker nodes, so it cannot prevent from active attacks such as DoS attack and Man in the middle attack.

IV. PROBLEM STATEMENT

ALERT is not providing security against all the active attacks. So in the present we have decided to improve the ALERT protocol by making the strategy to avoid the Denial of Service attack and Man in the middle attack in MANET.

V. PROPOSED SOLUTION

To prevent from DoS and Man in the middle attack in ALERT protocol in MANET our strategy is as follows;

Our proposed solution will be based on the single path strategy. The routing path will be decided before sending data packets. Once a route is found, pseudo numbers of position of nodes are generated which used for the nodes data packet along the route. Each node in the path only knows the pseudo numbers from its previous hop and next hop. Data packet will contain Hash value of message, previous hop and next hop. Then during routing our scheme checks for if (previous hop that node = next hop of other node).If it is same, it will accept packet; otherwise discard that packet. Hence DoS attack will be prevented in ALERT.

To prevent ALERT from Man in the Middle Attack Our scheme uses ACK for successful delivery of packets. When attacker node tries to modify/alter data packet; hash value given at Source side is checked at destination. If data packet's hash value is different from its source side hash value, attack is detected. So it sends negative acknowledgment (NACK) to send packets again by finding malicious node in network & uses alternative path for routing.

For preventing ALERT protocol from these active attacks we are going to use Hash function with SHA-1 for only source and destination nodes scheme. The algorithm for proposed work will be as given in Fig. 5.

VI. CONCLUSION

In this paper we have discussed the benefits of the MANET in different application such as military and education etc. We have also looked in to the different routing protocols such as GSPR, AO2P, ALARM, PRISM, ASR which are helping to protect the MANET from different attacks. But all of these protocols have some limitations regarding providing complete anonymity of source, destination or routes and also involving high cost. ALERT is cheap and an efficient for secure communication. But, ALERT is not providing the security against active attacks and hence in this work we have proposed a solution to prevent DoS and Man in the middle attack in ALERT protocol using hash function and SHA-1 algorithm.

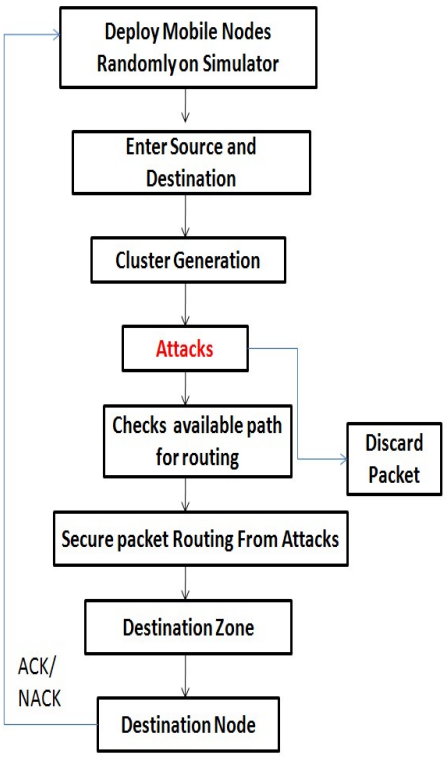

Fig. 5 Proposed System Flow

REFERENCES

[1] S. Kavitha and E. Bharathi, "Outsider Attack Prevention in Unobservable Secure On- Demand Routing Protocol for Mobile Ad Hoc Networks", In. International Journal of Engineering Research & Technology, Vol.2, Issue 9, e-ISSN 2278-0181, pp. September – 2013

[2] Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com "A Surveys of Attacks in MANET " Manjeet Singh1 Gaganpreet Kaur 2 Research Scholar (Deptt. of CSE) Assistant Professor (Deptt. of CSE) SGGSW University , Fatehgarh Sahib SGGSW University , Fatehgarh Sahib Punjab, India Punjab, India

[3] V .Madhumitha , Dr. S. Kirubakaran , "A Survey on Anonymous Routing Protocols in Mobile Ad hoc Networks", International Journal of Computer Science Trends and Technology (IJCST) , ISSN No. 2347-8578, Volume 1, pp. 34-36, November 2013

[4] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, Anonymity,Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31, technical report, 2005.

[5] Z. Zhi and Y.K. Choong, Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy, Proc. Third IntlWorkshop Mobile Distributed Computing (ICDCSW), pp. 646-651, DOI:10.1109/ICDCSW.2005.43, June 2005.

[6] K.E. Defrawy and G. Tsudik, PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs), Proc. IEEE International Conf. Network Protocols (ICNP), ISSN 1092-648, pp. 258-267, Oct. 2008.

[7] K.E. Defrawy and G. Tsudik, ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, Proc. IEEE International Conference Network Protocols (ICNP), Vol. 10, Issue 9, pp. 1345-1358, September 2011.

[8] X. Wu, AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol, IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/August- 2005.

[9] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[10] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, Anonymous Secure Routing in Mobile Ad-Hoc Networks, Proc. IEEE 29th Ann. International Conference Local Computer Networks (LCN), pp. 102-108, 2004.

[11] H. Snehlata and S. Pathan, " An Overview of Anonymous Routing ALERT Protocol", International Journal of Computer Science & Information Technology, , Vol. 5 Issue 2, p1607, 2014

[12] Lianyu Zhao ; Dept. of Electr. & Comput. Eng., Clemson Univ., Clemson, SC, USA; Haiying Shen ALERT: An Anonymous Location-Based Efficient Routing Protocol inMANETs, in Parallel Processing (ICPP), 2011 International Conference on , vol., no.,pp.703-712, 13-16 Sept. 2011.

[13] Haiying Shen, Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093, June, 2013