Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of Attacks in MANET

Trupti G. Mane*, Rajesh N. Phursule
Computer Engg Department, ICOER, Wagholi,
Pune, Maharashtra, India

Abstract— A mobile ad hoc network (MANET) is introduced as a self-configuring infrastructure-less network of mobile devices connected by wireless. MANETs each device is able to move individually in any direction, so they can change its links to other devices regularly, they change their locations. To hide node identities and/or routes from outside viewers in order to provide anonymity security Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols. Current anonymous routing protocols depend on either hop-by-hop encryption or terminated traffic; either generates high cost or cannot provide full anonymity security to data sources, destinations, and routes. We use an Anonymous Location-based Efficient Routing protocol (ALERT) to minimize the cost. ALERT hides the data sources/destinations among many sources/destinations to reinforce source and destination anonymity security. ALERT offers anonymity security to sources, destinations, and routes. ALERT has strategies to counter intersection and timing attacks. Proposed system achieves better route anonymity security and lower cost compared to other anonymous routing protocols. ALERT is not absolutely secured to all attacks. This paper is proposed to overcome the drawbacks of the ALERT. So that we can provide complete source, destination, and route anonymity protection.

Keywords— Ad-hoc Network, Data Anonymity, Location-Based Routing or Location-Based Services Routing Protocol, MANET, Secure Routing.

I. INTRODUCTION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some of protocols are unable to provide complete source, destination, and route anonymity protection. Due to Wide use of internet there is a need of some advanced technology which will boost up the wireless applications such as commerce, emergency services, military, education, and entertainment disaster relief, and mine site operation. We need secure and reliable communication is a necessary prerequisite for such applications. This is possible in MANETs by using ALERT [1]. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless, due to these features it make them an ideal choice for uses such as communication and information sharing. The primary challenge in building a MANET is providing each device to continuously maintain the information required to properly route traffic. Because of the open system and absence of centralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are open to malicious entities that aim to damage and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. In civil oriented applications, may not be a requirement of anonymity as it is critical in military applications.

Anonymous routing protocols are important in MANETs to arrange secure communications by hiding node characteristics and avoiding traffic analysis attacks from outside viewers. Currently, increasing use of multimedia applications enforces great requirement of routing efficiency. But, existing anonymous routing protocols generate a high cost, which improves the resource constraint problem in MANETs. ALERT has an approach to hide the data originator among a number of originators to support the anonymity protection of the source.

The black hole problem is one of the security attacks that occur in *mobile ad hoc networks* (MANETs). The traditional routing protocols of the Internet have been designed for routing the traffic between wired hosts connected to a static backbone; thus, they cannot be applied to ad hoc networks because the basic idea of such networks is mobility with dynamic topology.Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

II. LITERATURE SURVEY

Every device in a MANET is free to move independently in any direction so they change its links to other devices regularly. In MANETs, currently need is improved Anonymous routing schemes with low cost.

On-demand or reactive routing methods [2], [3], [4] and proactive routing methods [5] are the different categories by the different usage of topological information. Anonymous middleware working is also there between network layer and application layer [7]. A packet is encrypted in hop-by-hop encryption routing, in the transmission of two nodes en route, preventing adversaries from damaging or analyzing the packet contents to intersect the communication or identify of the two communicating nodes.

To prevent opponents from participating in the routing to ensure route anonymity, Hop-by-hop authentication can be used[2], [3], [4],[7]. In GSPR [3], nodes encode their location updates and direct location updates to the location server. But, GSPR does not offer route anonymity, the packets constantly follow the shortest paths using geographic routing, and the route can be detected by opponents in a long communication term.

Multicast, local broadcasting and flooding like this redundant traffic can be operated by Redundant traffic-based routing to obscure potential attackers. Very high overhead incurred by the redundant operations or packets, leading to high cost is a disadvantage of redundant traffic-based methods. Each node broadcasts its location information to its authenticated neighbours, so each node can build a map for later anonymous route discovery for this proactive routing used in ALARM. ALERT and GLS are different in the zone division scheme. ALERT divides a zone into two smaller rectangles, but GLS divides the entire square area into four sub squares, after that again divided part recursively divides into smaller squares. In ALERT zones are formed dynamically as a message is being forwarded, when selection of next forwarding node is completed. In GLS, the location servers are selected on the different hierarchies.

The black hole problem is one of the security attacks that occur in *mobile ad hoc networks* (MANETs). The traditional routing protocols of the Internet have been designed for routing the traffic between wired hosts connected to a static backbone; thus, they cannot be applied to ad hoc networks because the basic idea of such networks is mobility with dynamic topology.Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

III. PROPOSED WORK

ALERT is not absolutely secured to all attacks .In this Paper we are handling the drawbacks of the ALERT and analyse, predict attacks in MANET by using ALERT. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. When this route is established, now it's up to the node whether to drop all the packets or forward it to the unknown address. This attack is called a black hole as it swallows all objects; data packets. This paper proposes possible two techniques which can be used.

Algorithms: The proposed work which is as follows:-

- Route Requests (RREQ) are forwarded to Random Forwarder.
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
- When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP)
- Route Reply travels along the reverse path set-up when Route Request is forwarded
- Route Request (RREQ) includes the last known sequence number for the destination
- An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender
- Intermediate nodes that forward the RREP, also record the next hop to destination
- A routing table entry maintaining a reverse path is purged after a timeout interval
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry

Mathematical Model

Problem Statement:

Anonymous routing in a MANET including anonymity for data source and data receivers along with route anonymity.

Mathematical Module:

1] N is main set of communicating Nodes

$$N = \{N1, N2, N3\ldots\ldots.\}$$

2] LS is a main set of Location Servers.

$$LS = \{L1, L2, L3\ldots\ldots.\}$$

3] RF is the main set of data forwarders

$$RF = \{RF1, RF2, RF3\ldots\ldots.\}$$

4] RN is main set of Relay Nodes

$$RN = \{RN1, RN2, RN33\ldots\ldots\ldots\}$$

5] TD is the main set of Temporary Destinations

$$TD = \{td1, td2, td3\ldots\ldots..\}$$

6] P is the main set of Processes.

$$P = \{P1, P2, P3\ldots\ldots\}$$

1] P1 = {a1, a2, a3, a4} set of processes for preparation of network region

Where,

{a1=i|i is to generate the network region field}

{a2=j|j is to create and load the communicating nodes except location servers}

{a3=k|k is to create and load the location servers}

2] P2 = {a1, a2} set of processes for hierarchical partitioning of the network region

Where,

{a1=i|i is to determine number of partitions}

H is the number of partitions,we calculate it by using following equation where p is node density,G size of network field and k is number of nodes in destination zone or anonymity degree

$$H = log_2\left(\frac{\rho . G}{k}\right) \dots\dots\dots\dots (1)$$

{a2=j|j is to determine the destination zone size (Z_d)}

Z_d = zone destination size

G = size of network region

H = number of partitions

$$Z_d = G/2H$$

3] P3 = {a1, a2, a3, a4, a5} set of processes to determine next data forwarder

Where,

{a1=i|i is to calculate the two side lengths of the H^{th} portioned zone}

l_A = horizontal side length of the remaining network region

l_B = vertical side length of the remaining network region

H = Hth partitioned zone

a = horizontal side length of the new Hth partitioned zone

b = vertical side length of the new Hth partitioned zone

$$a = \frac{l_a}{\{2\left(\frac{H}{2}\right)\}}$$

$$b = \frac{l_b}{\{2\left(\frac{H}{2}\right)\}}$$

{a2=i|i is to determine whether new source is within destination zone}

{a3=j|j is to determine next type of partition and partition the remaining area}

{a4=k|k is to determine the next random forwarder using GPSR algorithm}

{a5=l|l is to send the data to next random forwarder using GPSR algorithm}

NP hard or NP complete:

Our project comes into the NP complete. Our project comes into NP complete because in particular time it will give the result. For the decision problem, so that it will give the solution for the problem within polynomial time. The set of all decision problems whose solution can be provided into polynomial time by using the given algorithm

Functional Dependencies:

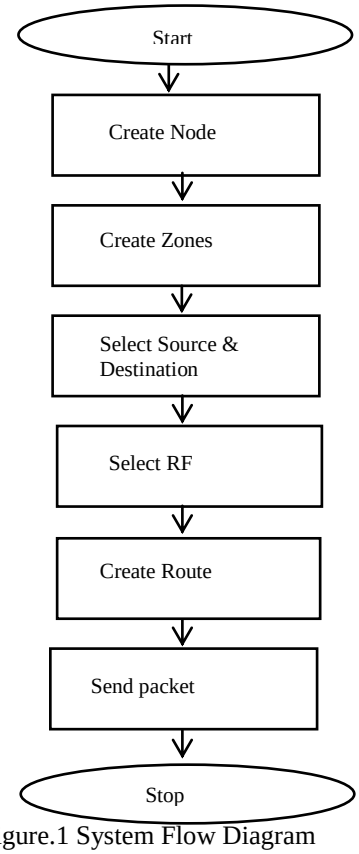

Figure.1 System Flow Diagram

Cryptographic algorithms:-
a. SHA-1: Generation of Dynamic Pseudonym
b. AES: Generation of Symmetric Key between Location Server and data sender (Source)
c. RSA: Generation of public key for every communicating node except the Location Servers
Input: {Zone position of the Destination, Message}
Output: {Degree of anonymity for destination}
Success: {Message successfully delivered to destination assuring anonymity protection for source, destination and route}
Failure: {If packet delivery speed i.e., data transmission speed is less than the moving speed of the destination node; in which case the destination moves out of destination zone}

IV. CONCLUSION AND FUTURE WORK

Due to the dependency on hop-by-hop encryption or redundant traffic of previous anonymous routing protocols, generate high cost. Some of the protocols are unable to provide complete anonymity protection to source, destination, and route. ALERT offers anonymity protection for sources, destinations, and routes with low cost as compared to other anonymous routing protocols.ALERT supports the anonymity protection of source and destination by hiding the data originator/receiver among a number of data originators/ receiver but. ALERT is not absolutely secured to all active attacks. This paper is proposed to overcome the drawbacks of the ALERT. So that we can provide complete source, destination, and route anonymity protection.This proposed system can avoid Black hole attack in MANET and provides more security in data transmission. Future work lies in reinforcing this system in an attempt to another active attacks.

REFERENCES

[1] HaiyingShen, and Lianyu Zhao, IEEE "ALERT: An Anonymous Location-BasedEfficient Routing Protocol in MANETs" 2013.
[2] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.
[3] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.
[4] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc.Ecurecomm and Workshops, 2006.
[5] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.
[6] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

