International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

SECURITY ASPECTS IN MOBILE ADHOC NETWORKS

Rajinder Singh
Research Scholar
DCRUST, Murthal, Haryana, India

ABSTRACT

Mobile Ad-hoc Network is the moving hub as opposed to any settled foundation, go about as a portable switch. These versatile switches are in charge of the system versatility. The historical backdrop of portable system start after the creation of 802.11 or Wifi they are basically utilized for associating among themselves and for uniting with the web through any altered foundation. Vehicles like auto, transports and trains furnished with switch goes about as settled Mobile Ad-hoc Network. Vehicles today comprises numerous installed gadgets like form in switches, electronic gadgets like Sensors Pdas fabricate in GPS, giving web association with it gives, data and infotainment to the clients. These developments in MANET helps the vehicle to correspond with one another, at the time of crisis like mischance, or throughout climatic progressions like snow fall, and at the time of barricade, this data will be educated to the adjacent vehicles. Presently days innovations climbing to give proficiency to MANET clients like giving enough storage room, as we all know the distributed computing is the cutting edge figuring standard numerous investigates are leading probes Mobile Ad-hoc Network to give the cloud benefit safely. This paper endeavors to propose and actualize the security based algorithmic approach in the Mobile adhoc systems.

Keywords : MANET, Network Security, Wormhole Attack, Secured Algorithm

INTRODUCTION

In case a mobile node wants to communicate with another mobile node which is too far from the source node, it should depend on relay node as bridge to communicate with destination. Relay node is nothing but another mobile node. In this case there arises a question of security. Apart from authentication, reliability and acceptance it should also aware of the address location and packet traffic digression.

In this manuscript we are going to concentrate on the various issues that affect the ad-hoc networks security mechanism and also we are going to concentrate on pros and cons of Mobile networks protocols. We are also concentrating on enhancing security and reliability to Mobile Ad-hoc Network (MANET).

Many researches were done before to provide security to MANET but none of the protocol shines in providing security and performance. There are many defects in the Mobile framework; this may cause unknown nodes to connect frequently without any proper routing. In order to prevent other nodes from trespassing we are going to concentrate on providing more security to Mobile Ad-hoc network.

Wormhole attack

Wormhole attack is also known as tunnelling attack, in this tunnelling attack the colluding attackers build tunnel between the two nodes for forwarding packets claiming that providing shortest path between the nodes and taking the full control of the nodes, which is invisible at the higher layers.

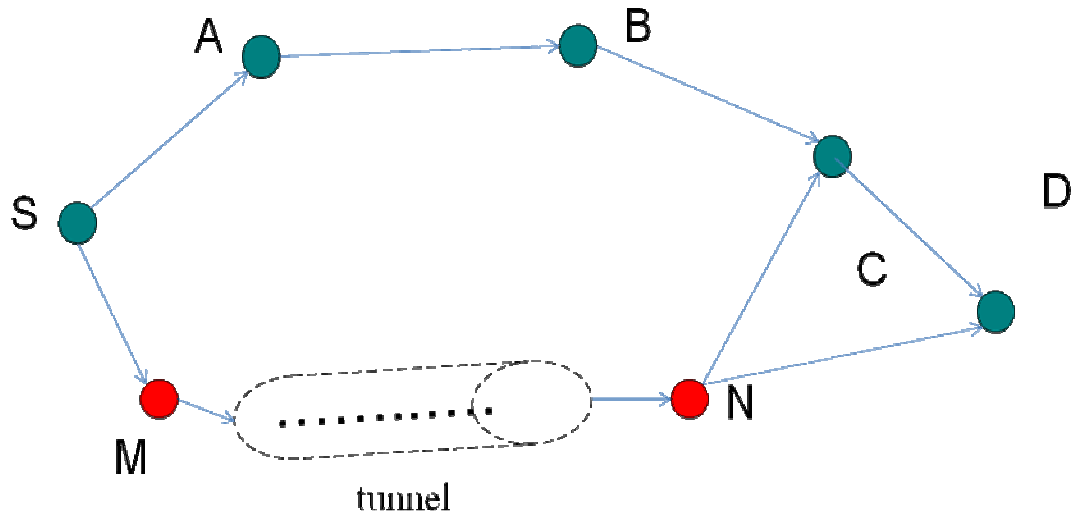

Figure 1 : Wormhole attack

Fig 1 represents the wormhole attack, where S and D nodes are the source and destination, A B and C are the connecting nodes providing path between source and destination. M and N are the malicious nodes, tunnelled by colluding attackers.

EXISTING TECHNIQUE FOR PREVENTING WORMHOLE ATTACK

In the previous techniques wormhole attack is prevented using the Location based Geo and Forwarding (LGF) Routing Protocol.

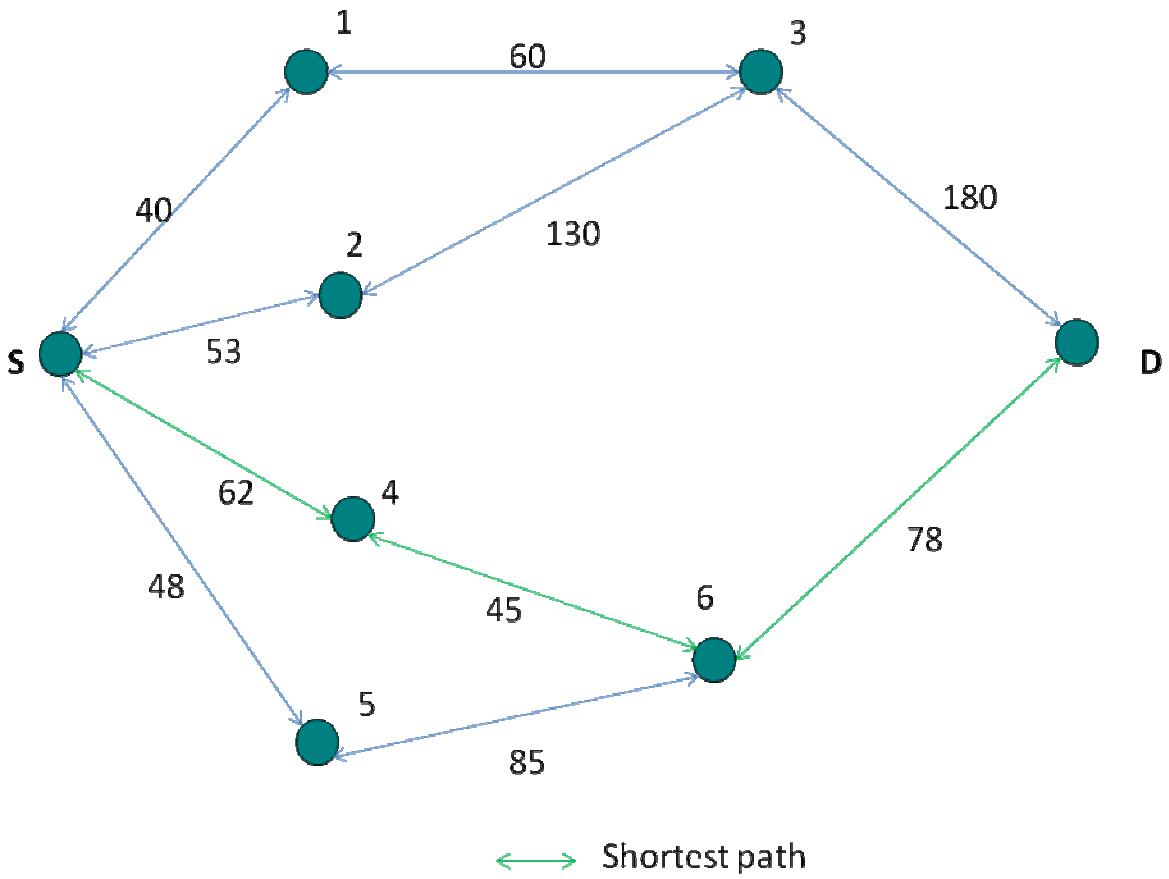

Figure 2 : LGF protocol implementation

However the preventive measures of wormhole attack with this LGF protocol was not solved clearly.

BLACK HOLE ATTACK

Black hole attack [8] is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path.

In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

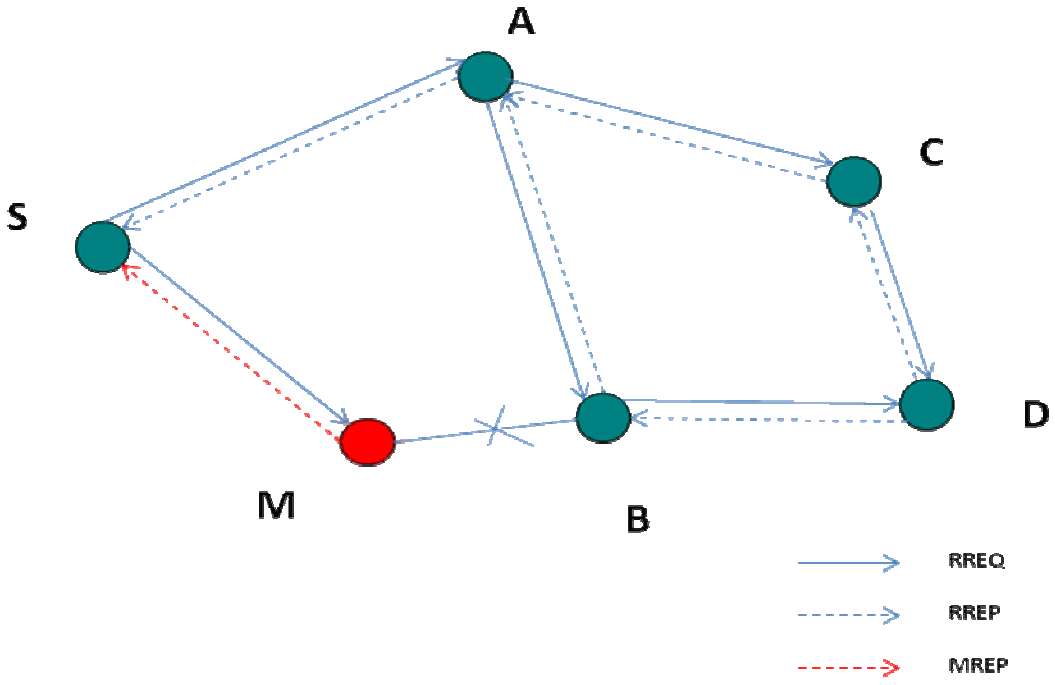

Figure 3 : Black hole attack

In the fig 3, S and D nodes are the source and destination nodes, A B C are the intermediate nodes and M is the malicious node. RREQ and RREP are the key terms for route request and route reply respectively. MREP is abbreviation for malicious reply.

PROPOSED ARCHITECTURE

WORM-HOLE ATTACK PREVENTION USING ALPHA NUMERIC REFLEX ROUTING ALGORITHM

ISSN (Online) : 2229-6166
Volume 4 Issue 3 September 2013

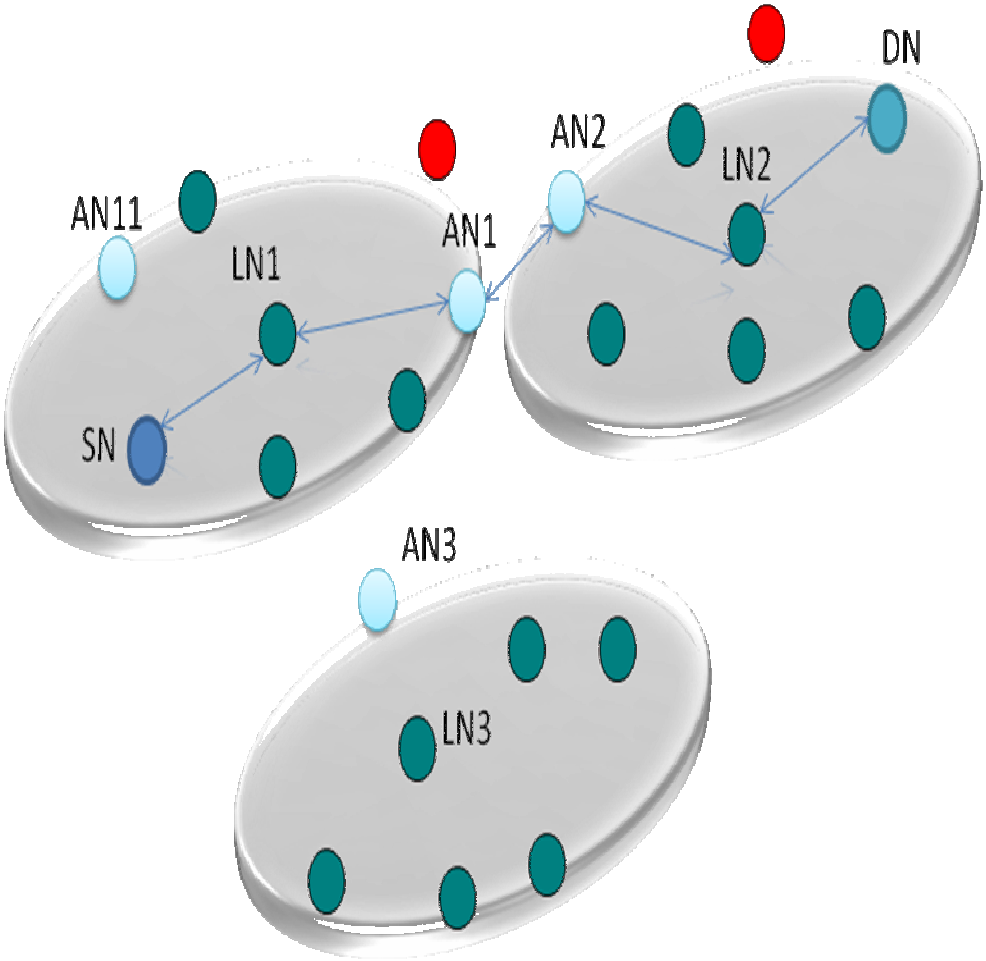

Figure 4 : Proposed Worm-hole prevention technique

In this technique, there won't be any possibilities for a malicious node to make tunnelling between the source and the destination nodes, as it is not included in the either of any groups. The packets are safe to reach the destination node efficiently.

INTELLIGENT MANET ARCHITECTURE

ISSN (Online) : 2229-6166
Volume 4 Issue 3 September 2013

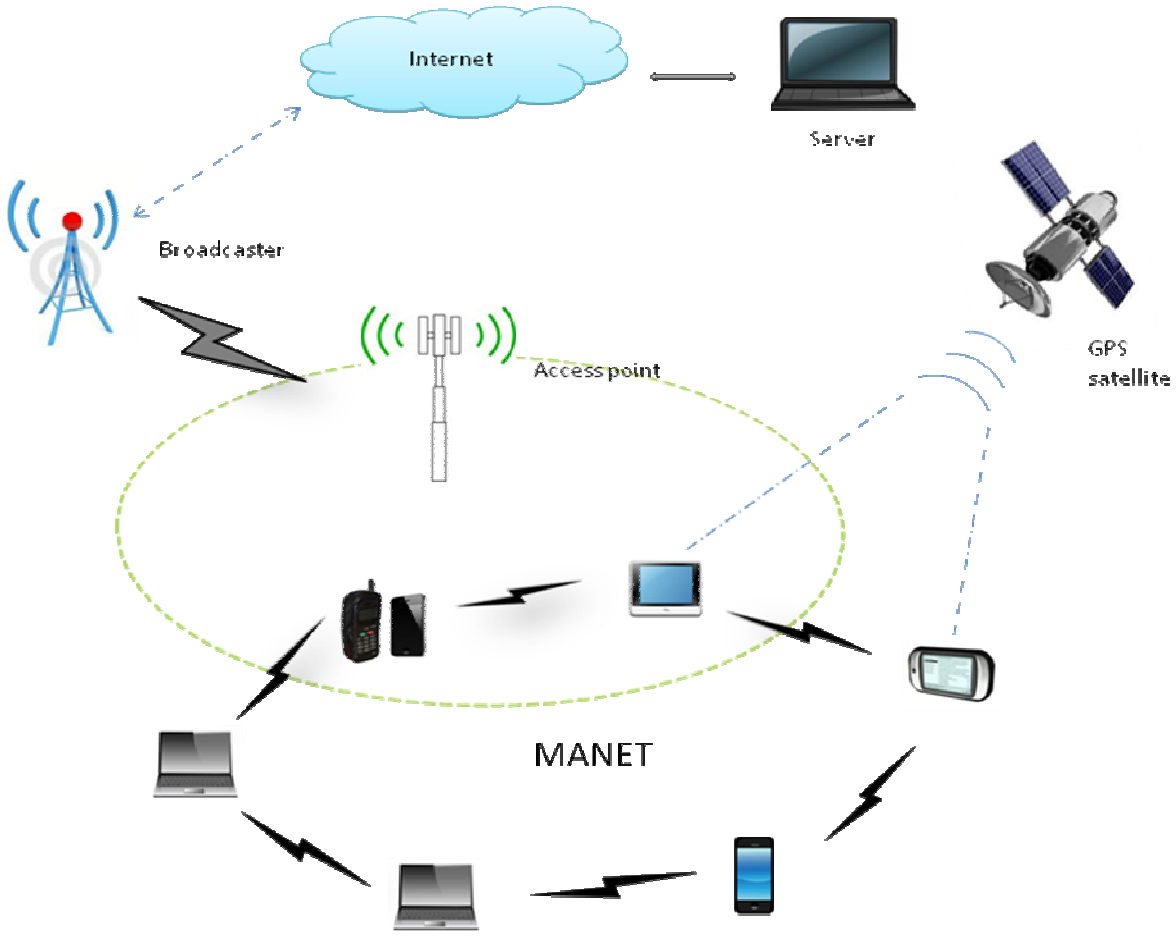

Figure 5 : Intelligent MANET architecture

INTELLIGENT MANET ALGORITHM

In this intelligent approach, nodes connected to this network is monitored by server agent, the server agent manages the details of the mobile nodes in a network like

- Behaviour of the node
- Speed of the node
- Direction of the node
- Position of the node

This technique prevents the malicious node from attacking other nodes

Step 1

The nodes participating in the networks to access service like internet registers its identity with the server agent, the server agent replies with unique ID to the requesting node.

Step 2

The source node request route with the current access point to the destination node the current access point forwards the route request to the server agent.

Step 3

The server agent verifies the source ID, then it accepts the route request from sender then it gathers the information of receiver using destination ID from the list.

Step 4

The server agent then broadcasts the route request message using destination ID, the registered adjacent nodes that are nearer to the destination node which are ready to provide the service replies with the acknowledgement message to the server agent.

Step 5

The server agent chooses the adjacent node with the longest life time (the ability of the nodes to stay connected with the destination node) using the details collected from the ID, Such as nodes position, direction of motion and speed of the node.

Step 6

Then the server agent provides route reply message for the source node, after this authentication process, source node starts sending data packets in a secure way.

Step 7

In case any node moves away from the network, immediately the server agent replaces it with some other nodes to maintain the continuity of connection.

Step 8

In this technique, the malicious node or selfish nodes are completely eliminated from the network, as the server agent takes full control of the ad-hoc network.

PACKET LOSS COMPARISONS

Scenarios	Time (in seconds)	Packet drop (in bits)
Existing system 1	**6.5**	**10581**
Existing system 2	**6.5**	**13221**
Proposed system 1	**6.5**	**4372**
Proposed system 2	**6.5**	**322**
Proposed system 3	**6.5**	**715**

Table 1 : Packet loss comparisons

PACKET LOSS COMPARISON GRAPH

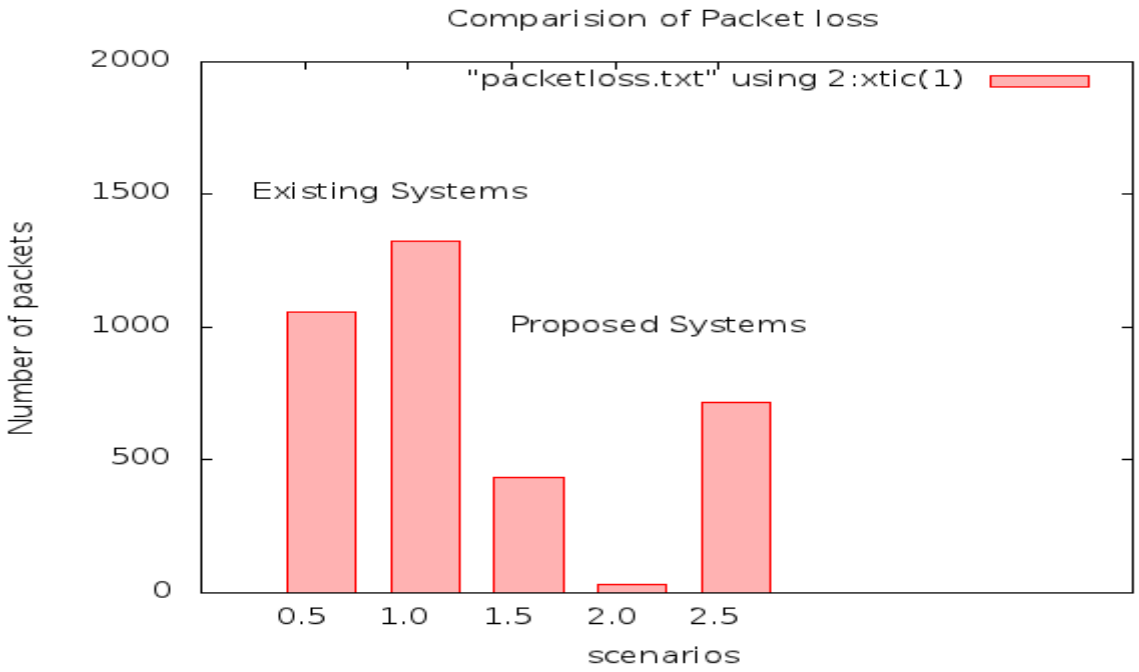

Figure 6: Packet loss comparison graph

CONCLUSION

Mobile adhoc networks are having lots of vulnerability and security issues from a long time. Various protocols and algorithmic approaches has been developed and implemented so far to avoid and remove the issues associated. This manuscript highlights various aspects of the mobile ad hoc network security issues

REFERENCES

[1] T.H Clausen, “Introduction to Mobile Ad-hoc Networks (MANET)s” , 2007.

[2] Che-Fn Yu, “Security safe guards for intelligent networks”, GTE laboratories incorporated, 40 sylvan road, Waltham, MA 02254.

[3] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, “WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks”, International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2008.

[4] Tuna Guven, Hui Zeng, Jason H. Li, Song Luo, Subir Das, Tony McAuley, Thomas Stuhrmann, Joe Sherrick, Christine Adelfio, Seth Spoenlein, Aristides Staikos, Mario Gerla, "A Multi-Layer Approach For Seamless Handoff In Ad Hoc Networks With Wireless Heterogenity", IEEE, Paper ID 900668.pdf.

[5] S. Prasad, Y.P.Singh, and C.S.Rai, " Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[6] Poonam Garg, "A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009