Performance analysis of black hole attacks in geographical routing MANET

H.J Shanthi[1], E.A Mary Anita[2]

1 Research Scholar, AMET University, Chennai
shanthi_harold@yahoo.co.in
2 Professor, S.A.Engineering College, Chennai

ABSTRACT

The MANET (Mobile Adhoc Network) is vulnerable to several types of attacks. The most commonly classified attack is black hole attack, which is carried by single or multiple attackers, advertising itself of having a short fresh route to transmit data.

The aim is to ensure security against the black hole attack and analyze the performance in geographical routing. The simple method is to send data as small blocks instead of entire data. The traffic is monitored independently in its neighborhood. The mechanism uses geographic information to detect variance in neighbor relations and node movements. We analyze the black hole attack in two popular location based protocol LAR and DREAM. It provides the stimulation study of black hole attack with the minimum attacker and also provides analysis on the parameters such as throughput, packet delivery and delay done with OMNET++ simulator. The simulation results show that packet loss increases and throughput decreases in the network with a black hole node in geographical routing. The proposed mechanism can be combined with existent routing protocols to defend against black hole attacks.

Keywords: MANET, Black hole, LAR, Geographical routing, OMNET++

1. Introduction

In Recent decade the wireless communication has gained the attention. Many researches are carried in self organizing networks with or without infrastructure. Mobile Adhoc Network (MANET) is a set of autonomous mobile nodes, communicate each other with no infrastructure. The MANETS are suitable for the emergency applications which have no infrastructure such as military, rescue, unmanned aerial vehicles (UAV) and mining operations.

There are many protocols in MANET which are designed to scale few nodes and provide poor results in larger mobile networks. Hence much attention is made on routing algorithms based on location.

These networks suffer from flooding, power and bandwidth, hence numbers of routing protocols are proposed for MANETs, which can be categorized into two different approaches: topology-based and position-based routing [1].

Topology-based routing protocols use information about the links. The information about the paths is maintained and routes are established based on the information of the links that stay alive in the network.

Position-based or geographic routing approaches are introduced to eliminate some of the important limitations of the topology-based protocols in MANETs. These routing protocols rely on having one piece of information and that is the nodes' physical location information. Thus, it is necessary for nodes to obtain their coordinates either by using a location service such as GPS or other types of positioning services [2]. By employing position information, geographic routing protocols do not necessarily establish and maintain routes, thereby eliminating cost of routing table construction and maintenance.

The network topologies in MANET are dynamic and unreliable. Security is more challenging due to its autonomous and lack of infrastructure support. This is another prime research area for MANET against several types of attack. A number of security techniques are developed and proposed, but still it difficult to ensure that network is free from malicious attack. The root causes of attacks can be divided in internal attack and external attack. The external attack is introduced but external illegal node. Internal attack is introduced by internal node or compromised node from its own network. This is a big threat which can disable the entire defense mechanism employed. The nature of this complicated nodes make more vulnerable to attack. The most predominantly they are liable to Black hole internal attack which is launched by single or group of nodes. MANET is highly subjected to vulnerability which requires secure communication. The proposed method presents a behavior based method to detect malicious node attack, which is based on Geographical routing. The geographical routing protocols make routing based on Global Positioning System (GPS) and location services.

The scope of this paper is to study the effects of Black hole attack in MANET using Location Based routing protocol i.e Location-Aided Routing (LAR) algorithm, the Distance Routing Effect Algorithm for Mobility (DREAM). Comparative analysis of Black Hole attack for both protocols is taken into account. The impact of

Black Hole attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols [16]. The performance indicators selected are throughput, end-to-end delay and network load. In the paper, we simulated black hole attacks in wireless ad-hoc networks and evaluated their effects on the network performance. Simulation is done in OMNET++ tool [13].

The rest of the paper is organized as follows: Section 2 describes related works done on Black hole attack and location based routing protocols, Section 3 describes the stimulation and parameters, Section 4 describes the simulation results, Section 5 analyze the results and Section 6 describes the conclusion of results.

2. BACKGROUND AND RELATED WORK

Routing packets in MANETs is extensive research in adhoc networks. In this section we present an overview of research in MANET with regard to geographical routing and black hole attack.

Black hole attack:

The MANETs face security threats which interrupt the normal performance of the networks. In black hole node advertises or publish of having fresh short route to destination route and absorbs all network traffic. When source node sends RREQ message for a destination, the malicious node responds immediately with RREP message regardless of its routing tables. The source starts trusting the malicious black hole and send packets. This phenomena is studied by different authors.

In a work by Marti *et al.* [10] a node detects a misbehaving successor along a packet's path by promiscuously listening on its wireless interface waiting for the packet it forwarded to its successor node. They term this detection mechanism a „watchdog‟. The drawback is high overhead caused for tracing malicious node and rates the new routes. Additionally the malicious nodes are not removed so they can still send the packets in network.

Once the attacker adds itself between the communicating nodes, it can do anything malicious with the packets passing between them. It can then choose to drop the packets thereby creating Denial of Service attacks.[3]

These factors lead to various security threats in mobile ad hoc networks. Black hole Attacks are classified into two categories. In single blackhole attack there is only one malicious node within a zone [14]. Whereas in collaborative blackhole attack multiple nodes in a group act as malicious nodes.

The CONFIDANT[9] method applies the concept of reputation. Each node keeps track of forbidden list of misbehaving nodes. This detection is warned to all trusted peer node about this malicious node. Any type of service from this malicious node is not entertained. This protocol works based on trust, the malicious node can black mail real node and scalability in the distribution of this forbidden list are the limitation in this scheme.

The CORE[15] method tries to eliminate the limitations of previous scheme. The nodes are not allowed to distribute negative status values on any node but they can broad cast positive status. So each node keeps track of reputation values of its immediate neighbors only. This makes the reputation complex systems. The node negative reputation is obtained from neighbor, the misbehaving node will be ultimately isolated from the network and all its neighbor will stop sending packet to it. Neither will they receive the packets from that node. Since all the nodes are mobile node they are constantly changing and results in dropping of packets.

In a work by Buttyan and Hubaux [11], the authors propose a kind of currency, which they call “nuglets”. The packets reach their destination by the sender or the receiver paying sufficient number of nuglets to the number of hops the packet crosses. Each node can increase its nuglets by forwarding packets for other nodes. This scheme solves the selfish node problem.

The works done is earlier years are mostly based on reactive routing protocols like Ad-Hoc on Demand Distance Vector (AODV). The attacks of black hole are reviewed and their effects are analyzed of their disturbance in the performance in MANET. The impact of black hole attack on location routing protocols are comparisions are least studied. This work is to study the effects of black hole attacks on location based protocol i.e. Location Aided Routing (LAR) and Distance Routing Effect Algorithm for Mobility (DREAM).

Location Routing Protocols

The research in recent decade are extensily carried on Mobile Adhoc networks (MANET) because of essential application depend on it. The location information is easily available through small and inexpensive GPS devices. This brought development to adopt the position based operation in MANET. These MANETs depend on location information in their operation and are termed as Location-Based MANETS[16].

These types of protocols assume that the individual nodes are aware of the locations of all the nodes within the network. The Global Positoning System(GPS) determine the exact location in any geographical location. This location information is then utilized by the routing protocol to determine the routes. The most common routing protocols are LAR, DREAM, GPSR, ALERT etc. The main prerequisite for location based routing is that a sender can obtain the current position of the destination.

Ko and Vaidya [4] present Location-Aided Routing (LAR) protocol which uses the location information to identify the request zone and expected zone. Request zone in this protocol is the rectangular area including both senders as well as receive. By decreasing the search area, this protocol leads to the decrease in routing overheads.

S. Basagni et al. [5] proposes DREAM (A Distance Routing Effect Algorithm for Mobility) it maintains each node's location information in routing tables. Data packet is send by using this location information. In order to maintain the location table accurately, each node at regular interval broadcasts a control packet containing its own coordinates and maintains the location table accurately.

Karp and Kung [6] propose GPSR (Greedy Perimeter Stateless Routing) which uses the location of node to forward the packets on the basis of distance. The packets are forwarded on a greedy basis by selecting the node closest to the destination. This process continues until the destination is reached. In some cases the best path may be through a node which is farther in distance from the destination node. In such scenario right hand rule is applied to forward around the obstacle and resume the greedy forwarding as soon as possible.

ALARM [8] propose issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol. ALARM uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques, it offers protection against passive and active insider and outsider attacks.

Haiying Shen and Lianyu Zhao [7] propose an Anonymous Location-based Efficient Routing protocol (ALERT) to offer high anonymity protection at a low cost. ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

3. Stimulation Tool and Parameters Setup

OMNET++

We have implemented black hole attack using OMNET++ [12] tool, a simulation environment free for academic use and its INET Framework, a set of simulation model released under GPL. Scenarios in OMNeT++ are represented by a hierarchy of reusable modules written in C++. Modules' relationships and communication links are stored as Network Description (NED) and can be modeled graphically. Simulations are either run interactively in a graphical environment or are executed as command-line applications. It also provides modules that allow the modeling of spatial relations of mobile nodes and IEEE 802.11 transmissions between them.

Parameters

Performance indicators selected to evaluate the black hole attack are packets end-to-end delay, throughput of the network and the network load, packet loss. Delay is used to produce the comparative results and depict the average time needed to pass a package in network.

Another performance measure is packet loss parameter, which indicates the drop of packets between sender and receiver under the black hole.

The next parameter is throughput, which measures fastness in sending through the network. It also includes delay time caused by the transmission.

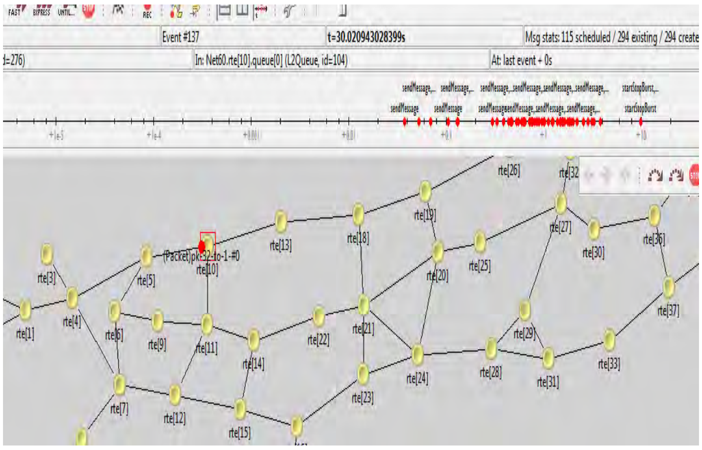
Another parameter is network load, which indicates the volume of traffic on the network.

Table 1.Stimulation Parameter

SIMULATION PARAMETERS	
Examined protocols	LAR and DREAM
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	16 and 30
Traffic Size	CBR
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Speed	10m/s
Packet Size	512 bytes
Packet Rate	5 packets
Mobility Model	Random waypoint
Channel	Wireless Channel
Simulator	OMNET++4.2.2
No of Connections	60% of nodes

4. Stimulation Results

When the number of nodes increased there was delay in both LAR and DREAM. The mobility model used is Random way point since mobile nodes have random movement. The pause time represent the movement of objects. When the objects move, they stop for some time to change the direction and move randomly.



Event #137

t=30.020943028399s

Msg stats: 115 scheduled / 294 existing / 294 create

d=276)

In: Net60.rte[10].queue[0] (L2Queue, id=104)

At: last event + 0s

Fig.1. Simulation environment for 30 nodes

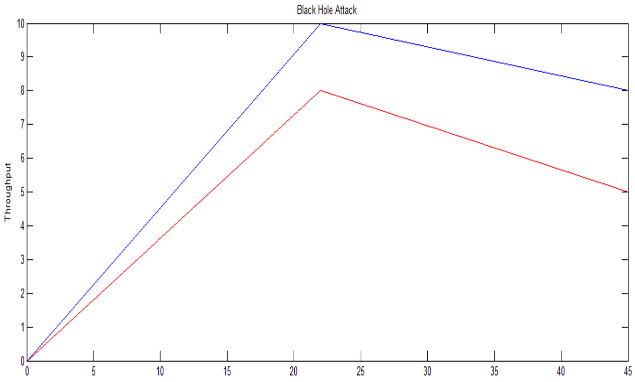


Fig.2. Throughput decreases with black hole in both LAR and DREAM

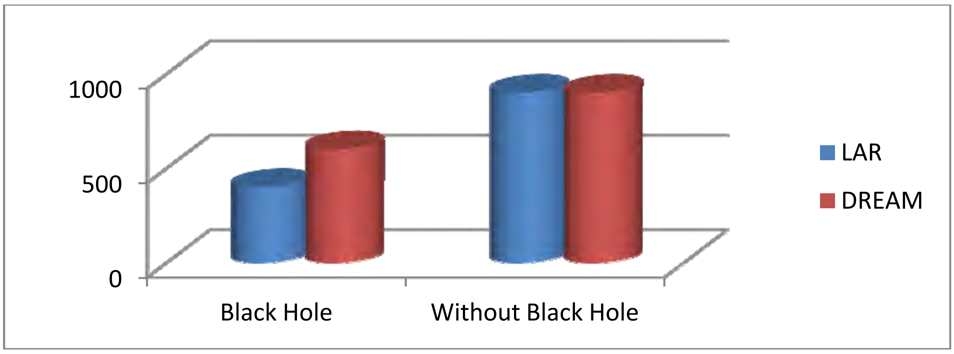


Fig.3. Throughput performance in kbps

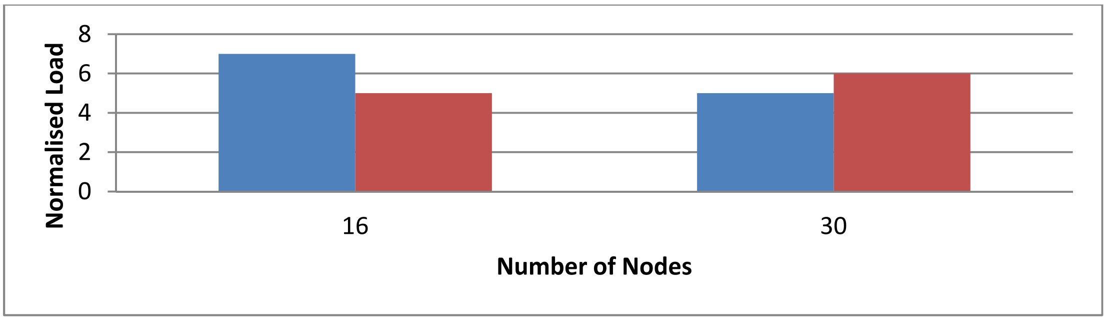


Fig.4. Normalized Routing Load with black hole and without black hole .

To test the protocol we used a small network in of 16 nodes, 30 nodes, with the black hole node and other without black hole node. After the introduction of black hole we evaluated the packets that could reach the destination. The some of the packets are absorbed by black hole. It is measured that packet delivery ratio are drastically decreases when there is a malicious node.

The compared results of simulation are analyzed below.

5. Performance Analysis

When nodes are increased from 16 to 30 and when network load is high, the packet delivery reduces in both but LAR produces much better results. The result shown is based on LAR and DREAM with and without black hole attack.

The packet delivery ratio calculated is 98.8% when there is no effect of Black hole attack and packet delivery decreases to 88.8% because of the dropping of packets by black hole.

Throughput of network is improved without black hole node for both LAR and DREAM is shown in the figure 2 and Fig.3. It shows that the performance of the network is reduced with black hole attack in both Routing algorithms. However the DREAM shows the increase in throughput performance over LAR. The simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. If the number of Black Hole Nodes is increased then the data loss is expected to increase.

Normalized Routing Load with /without black hole, refers to amount of data or traffic overhead being carried by the network. Normalized Routing Load graph of LAR and DREM is shown in figure 3. The network load in case of DREAM protocol is less as compared to LAR protocol.

6. Conclusion

MANET has important application to be carried but has many challenges to overcome. The MANET security suffers the threat commonly from black hole. The blackhole can be launched in any network. In this paper we performed and analyzed the black hole attack in two popular location based protocol LAR and DREAM. The simulative results shows that DREAM performs better than LAR in case of parameters like throughput, end- to end delay and packet dropping ratio. However when network nodes increase the LAR produces better results. The LAR and DREAM protocol differs in its features but both shows degradation in their performance after the black hole node. The detailed study of these two different protocols will enable us to develop new routing protocol with security against black hole to get high performance in mobile adhoc networks. We may conclude that LAR is vulnerable to attack than DREAM.

Acknowledgement

I thank our President Dr. J. Ramachandran and Vice-Chancellor Col. Dr. G. Thiruvasagam of AMET University for providing necessary infrastructure and support. I am also thankful to Research Director for his constant encouragement. I am thankful to my guide for the valuable suggestions. I thank all my department associates for their support in bringing out the paper successfully. I also thank authors in reference section.

Reference:

[1] M. Mauve, J. Widmer and H. Hartenstein, A Survey on Position Based Routing in Mobile Ad-hoc Networks, IEEE Network Magazine, 15(6):30–39, November 2001.

[2] S. Capkun, M. Hamdi, and J. Hubaux, “Gps-free Positioning in Mobile Ad Hoc Networks,” Proc. Hawaii Int’l. Conf. System Sciences, Jan. 2001.

[3] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, ―A Survey of Secure Mobile Ad Hoc Routing Protocols‖, IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, Fourth Quarter 2008.

[4] Y.B. Ko and N. H. Vaidya, "Location-Aided Routing in Mobile AdHoc-Scale for Ad Hoc Networks," Proceedings of the second ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, Wireless Networks (6)307–321, 2000

[5] S. Basagni, I. Chlamtac, V.R. Syrotiuk, B.A. Woodward, “A distance routing effect algorithm for mobility (DREAM)” in: Proceedings of the ACM MOBICOM, pp. 76–84, 1998.

[6] B. Karp and H. Kung,. “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks” in: Proceedings of ACM MobiCom, 2000, pp. 243–254.

[7] Haiying Shen and Lianyu Zhao ALERT, “An Anonymous Location-Based Efficient Routing Protocol in MANETs” IEEE TRANSACTIONS ON MOBILE COMPUTING, 2013, (12) 6:1079-1093.

[8] El Defrawy, Karim, and Gene Tsudik. "ALARM: anonymous location-aided routing in suspicious MANETs." Mobile Computing, IEEE Transactions on 10.9 (2011): 1345-1358.

[9] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002.

[10] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[11] Buttyán, Levente, and Jean-Pierre Hubaux. "Stimulating cooperation in self-organizing mobile ad hoc networks." Mobile Networks and Applications 8.5 (2003): 579-592.

[12] Varga, András, and Rudolf Hornig. "An overview of the OMNeT++ simulation environment." Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[13] Kaur, Ramanpreet, Amrit Lal Sangal, and Krishan Kumar. "Modeling and simulation of DDoS attack using Omnet++." Signal Processing and Integrated Networks (SPIN), 2014 International Conference on. IEEE, 2014.

[14] Meenakshi, Kapil Kumar Kaswan. "SIMULATION OF BLACK HOLE ATTACK IN ADHOC NETWORK USING NS2." SIMULATION 3.1 (2014).

[15] Michiardi, Pietro, and Refik Molva. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks." Advanced Communications and Multimedia Security. Springer US, 2002. 107-121.

[16] Qadri, Nadia N., and Antonio Liotta. "Analysis of pervasive mobile ad hoc routing protocols." Pervasive Computing. Springer London, 2010. 433-453.

[17] S. Seys and B. Preneel, "Arm: Anonymous routing protocol for mobile ad hoc networks," International Conference on Advanced Information Networking and Applications, 2006