Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study on Black Whole Attacks in Mobile Ad Hoc Networks

[1]Dr Venkata Surya Narayana T, [2] *M. Ambica,* [3] *P. Datta Dev,* [4] *Y.Bala TripuraSundari*

[1]*Associate Professor, ECM Dept, K L University, Guntur, India.*

[2] *Assist Professor,CSE Dept, LAQSHYA Institute of Technology & Sciences, Tanikella(V),Khammam, India*

[3] *IV B.Tech, CSE Dept, NRI Institute of Technology, Agiripalli(M), Vijayawada, India*

[4]*III B.Tech, ECM Dept, K L University, Guntur, India*

Abstract: Mobile ad hoc networks (MANETs) are a set of mobile nodes which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. [1]. The absence of a central management agency or a fixed infrastructure is a key feature of MANETs. Security issues in MANET are a challenging task nowadays. MANETs are vulnerable to passive attacks and active attacks because of limited number of resources and lack of centralized authority. Blackhole attack is an attack in network layer which degrade the network performance by dropping the packets. This paper identifies black whole attack against Optimized Link State Routing (OLSR) protocol, one of the four standard routing protocols for MANETs. We analyze in detail the impact of this attack in order to show the necessity for a countermeasure to guard against the attack.

Key Words: MANET,OLSR,

I. INTRODUCTION:

A mobile ad hoc network (MANET) [2] [3], is a dynamic self configurable wireless network, which has no fixed infrastructure or central administration. These characteristics make MANETs suitable for mission-critical applications, such as disaster recovery, crowd control, search and rescue and automated battlefield communications, yet make the routing in MANETs very difficult. Nodes can move arbitrarily, network topology can change frequently and unpredictably, and the bandwidth and battery power are limited. For these reasons, the development of routing protocols in MANET is extremely challenging.

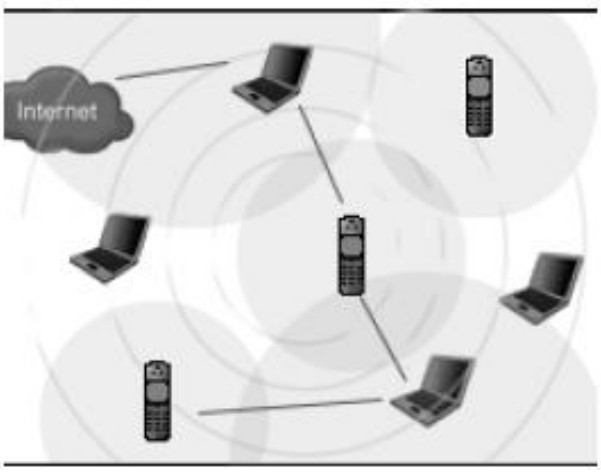

Fig 1: A Typical MANET

The chief characteristics and challenges of the MANETs [4] can be classified as follows:

Dynamism of Topology:

The nodes of MANET are randomly, frequently and unpredictably mobile within the network.[5] These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes.

Cooperation:

If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi hop communication. Hence each node is to act as a host as well as a router simultaneously.

Resource constraints:

MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

Lack of fixed infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

II. OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR):

The Optimized Link State Routing Protocol (OLSR) [6] is developed for mobile ad hoc networks. It operates as a table driven, proactive protocol, i.e exchanges topology information with other nodes of the network regularly. OLSR is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks. OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs, to retransmit control messages.

This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is, that all nodes, selected as MPRs, MUST declare the links to their MPR selectors. Additional topological information, if present, MAY be utilized e.g. for redundancy purposes. OLSR is designed to work in a completely distributed manner and does not depend on any central entity. The protocol does NOT REQUIRE reliable transmission of control messages: each node sends control messages periodically, and can therefore sustain a reasonable loss of some such messages. Such losses occur frequently in radio networks due to collisions or other transmission problems. Also, OLSR does not require sequenced delivery of messages. Each control message contains a sequence number which is incremented for each message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission.

The key concept of the protocol is the use of "multipoint relays" (MPR). Each node selects a set of its neighbor nodes as MPR. Only nodes, selected as such MPRs, are responsible for generating and forwarding topology information, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding topology information by reducing the number of transmissions required. The protocol is best suitable for large and dense network as the technique of MPRs work well in this context. Fig. 2 illustrates a node broadcasts its messages throughout the network using standard flooding (Fig.2 (a)) and MPR flooding (Fig. 2 (b)). The core functionality of OLSR includes neighbor sensing, multipoint relays selection, topology diffusion and routing table calculation.

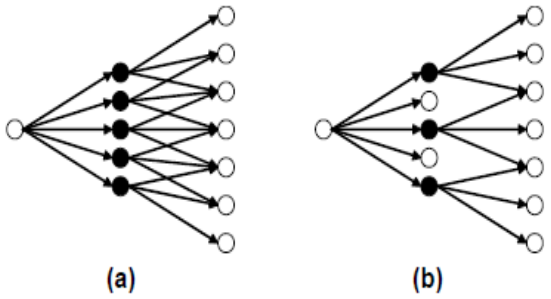

Fig. 2. The broadcast from the leftmost node is retransmitted: (a) by all its neighbors (b) by its MPRs only.

III. ROUTING ATTACKS

In MANETs, every ode participates in the routing process. Hence, it is possible for attackers to launch attacks against the routing protocol by sending false routing information. The possibility of such attacks was already mentioned in [7]. In [8] these attacks against the routing protocol are referred to as routing disruption attacks. By sending false routing information, an attacker may try to dispose other nodes to make him a part of their routes. This is often referred to as 'route attraction'. If an attacker succeeds in attracting routes, he may perform several attacks including

- eavesdropping messages,
- selectively dropping data,
- manipulating data, or
- launching a denial-of-service (DoS) attack.

Like in [9], we assume protection against eavesdropping and manipulation by means of cryptography. Additionally, selective dropping of data is a special case of a DoS attack.

Black Hole Attack

There are several examples of DoS attacks against routing protocols. A black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. Additionally, a special case of the black hole attack called gray hole attack is mentioned in [8]. In this case some packets are discarded (e.g. application

data) while others are forwarded (e.g. routing packets). However, a gray hole is only a special case of a black hole that has similar impact but is harder to detect.

In the following, we will without limitation of generality focus on an attacker forwarding routing packets and dropping application data packets. We will refer to this attack as black hole attack. The actual implementation of the black hole attack strongly depends on the deployed routing protocol.

Black Hole Attack in OLSR

In order to run a DoS attack against OLSR, it is reasonable to fake HELLO and/or TC messages, because they are used to provide the basic connectivity in the network. The first possibility is faking only TC messages. This is not reasonable because it is possible to detect a fake TC message by means of local plausibility checks [10]. The second possibility is to fake both HELLO and TC messages. This approach is not chosen in this work, as a single node receiving a TC message including its address while not considering the originator, a neighbour will be able to detect the attack. We implemented a third approach. A node acting as black hole sends fake HELLO messages. In these messages an attacking node claims to have links to more neighbours than it actually has. Thus, there is a high probability that this node is chosen as an MPR by its neighbour.

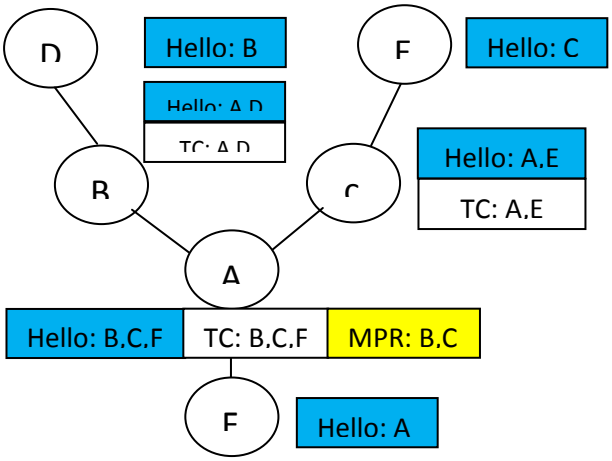

Fig 3(a) OLSR without Blackhole

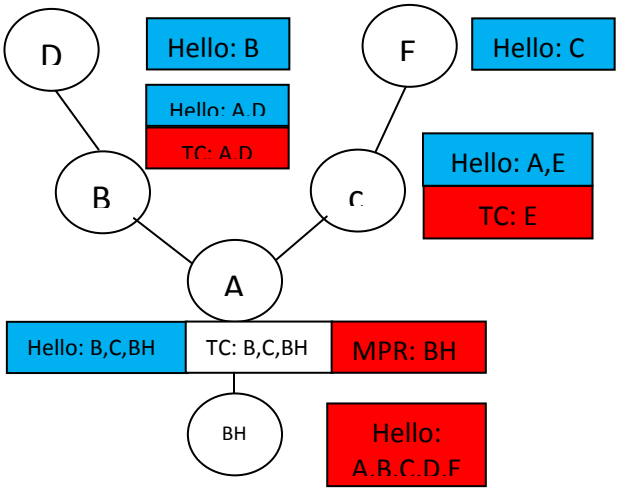

Fig 3(b) OLSR with Blackhole

The more neighbours the attacking node claims to have, the larger the potential impact of the attack. Due to the fake messages of the attacker, in its neighbor hood falsified TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture routes. Figure 3(b) shows the OLSR network presented in Figure 3(a). This time node F has been taken over and acts as black hole. This leads to some changes in the network.In this figure, the lines just show Node A's view of the network. Change Nr.1 is the fake Hello message of the black hole node. It contains nodes A,B,C,D and E. This leads to Node A selecting only the black hole node as MPR. Since Node A does not select nodes B,C as MPRs, these send TC messages not containing Node A. Additionally, instead of sending data packets to nodes D,E via nodes B respectively C, node A tries to send these data packets via the black hole node. Therefore, the black hole has gained control over the connections from A to D and E.

IV. SECURITY-FOCUSED DEVELOPMENT PROCESS GOALS

This is the easy part the goal of a process to help build more secure software is to produce more secure software! Actually, there's a little more to it than that. The goal should be to reduce the chance that the designers and developers

will inject security vulnerabilities into the design and code in the first place. This goal has the positive side effect of producing more secure software. You can take several key actions to integrate security into your software development process.

Create a Central Security Team

This group's role is to be an internal security "consulting" organization for the rest of your development team. The team defines process requirements and best practices, defines and build tools, helps perform code and design reviews, does threat analysis, and provides education for the software development staff.

Use Secure Design Practices

Designers and architects should adhere to good security design principles, such as least privilege, reduced attack profile, simplicity, fail-closed defaults, appropriate protection of key material, and so on. Several books and articles offer many good design concepts toward this goal.

Build More Secure Code

Software construction errors can lead to implementation flaws, some percentage of which will become security vulnerabilities. Thus, a major goal is to reduce the chance that developers introduce security vulnerabilities. To this end, you should employ secure coding best practices: many good references can help. You must also have security code reviews, and review all the codenot just new code. I outline a simple process to advance security code reviews in a recent article.

Security tools are a powerful adjunct to code review, but don't use tools to replace competent engineers and good discipline. The advantage of tools is that they can help scale the code-review task; reviewing thousands of files can be slow and tedious, and some tools can find low-hanging fruit. However, most tools don't find deep and complex bugs; you need human review for that. Tools aren't limited to just helping the code-review process. Some, such as Security Innovation's Holodeck and fuzz testing can help uncover security flaws by perturbing the environment in which an application runs or by creating purposefully malformed packets. Tools are an adjunct to the development process, not a replacement for lacking skills. When defining your security process budget, focus on your team members first, then buy appropriate tools.

V. Conclusion:

Recently, MANETs are receiving a tremendous attentions from the networking research community due to their flexibility and their easy deployment. MANET uses routing protocol to provide connectivity between nodes who are not within the same radio range. Existing MANET routing protocols assume a trusted and cooperative environment. However, in hostile environment MANET are susceptible to various kinds of attacks which is more serious than conventional wired network. In MANET, routing attack is particularly a major concern. In this paper, we have presented a routing attack, called black whole attack, against OLSR-based mobile ad hoc network. This attack allows attacker(s) to a specific node or a group of nodes from receiving data packets from other nodes who is further than two hops. After analyzed the Attack in detail, we have presented a simple technique to detect the attack. One shortcoming of the proposed solution is that it might not detect the attack in which two consecutive nodes work in collusion. Currently, we are seriously working on this issue. Our future work will also be focused on investigating other sophisticated attacks which have not been well studied as well as studying the possible countermeasure against such attacks

References:

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.
[2] Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANET) Working Group Charter.
[3] J. JUBIN AND J. D.TORNOW, The DARPA packet radio network protocols, in Proc. of the IEEE, vol. 75. No. 1, January 1987, pp. 21–32
[4] George Aggelou, *Mobile Ad Hoc Networks*, McGraw-Hill, 2004.
[5] E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," *AusCERT2006 R&D Stream Program, Information Technology Security Conference*, May 2006.
[6] Th. Clausen et. al, "Optimized Link State Routing Protocol," IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.
[7] J. Hubaux, L. Butty´an, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking & Computing, 2001.
[8] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.
[9] M. Jahnke and J. T¨olle, "Bedrohungen gegen taktische mobile Adhoc-Netzwerke (MANETs)," FGAN/FKIE, Wachtberg, Germany, Tech. Rep., December 2005, appointed by the Federal Office for information management and information technology of the German Federal Armed Forces [in German]
[10] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for OLSR MANET protocol," Proceedings of 1st IEEE ICNP Workshop on Secure Network Protocols, 2005.

