A SURVEY FOR ANALYZING & PREVENTING OF GRAY-HOLE ATTACK MINIMIZATION FOR OLSR BASED NETWORK

BOBBY K SIMON[1], Ms. ANJANA P NAIR[2]

[1]BOBBY K SIMON M.Tech Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta Pathanamthitta , Kerala, India.
[2] Ms. ANJANA P NAIR Assistant Professor Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta, Pathanamthitta, Kerala, India

---***---

Abstract - *Ad-hoc networks are quite popular for especially on networks system (MANETs, IoT, VANETs, and so forth.), identification &mitigation procedures are only functioning after the attack was initiated Prevention, however, attempts of an attack can be monitored before it is executed. This survey gives us knowledge about how attacks are been analyzed with this two strategies can be acknowledged either by the aggregate collaboration of network nodes or by internal detection of the attack state. It also shows the method for minimizing the gray-hole DoS attack and how to reduce the count of number of packets been dropped. Our survey gives an answer for no explicit node collaboration, with every node utilizing just internal knowledge picked up by routine routing information. This also shows the benefits of the different techniques threat models for better understanding of the attack surface and its prevention. We recognize their respective motivations and distinguish their advantages and drawbacks in a comparative survey.*

***Key Words*: MANET, OLSR, DCFM, RND, MITM, Gray-hole attack.**

1. INTRODUCTION

Optimized Link Routing Protocol (OLSR) is a proactive routing protocol which is widely used MANET protocols. The quality-of-service (QoS) of OLSR significantly depends on the selection of its parameters, which determine the protocol operation and represents a better technology that stop the sudden undisturbed attack in counting of network nodes. Security is a main thing for ad-hoc network. Data transferring network protocols analysing & monitoring have become increasing attack in now a days. Ad-hoc network are the most challenging area for network protocol design and implementation have become increasingly complex, Because of network topology, internal deduction, and collective collaboration of network nodes.

Network protocols are usually for maintaining efficient in data transferring between other nodes. The optimization strategy is used in this paper to find as fine-tuned as possible configuration parameters of the OLSR protocol, although it could directly be used also for a number of other routing protocols (AODV, PROAODV, GPSR, FSR, DSR, etc.) [1].

Denial Contradiction with Fictitous Node Mechanism (DCFM) is an algorithm used to specially to monitor the DoS (Denial of Service). It can figure out the problems of node isolation in OLSR based network. This node mechanism can be used for reducing dropped packets in gray-hole attacks effectiveness. An ad-hoc network consists of a collection of "peer" nodes that are able to communicate without the help from a fixed infrastructure. DCFM's main mechanism it's to mitigate the node isolation attack by relying solely on internal knowledge acquired by each node during routine routing. And in utilizing the same technique used for the attack to prevent damage. As both node isolation and gray-hole attacks require similar preliminary steps for attack execution, namely coaxing a victim into appointing the attacker as sole multipoint relay (MPR) node, which is responsible for broadcasting a node's existence to the network. DCFM is and good basis for mitigating the gray-hole attacks.

Among the different various types of attacks including wormhole attack [3], spoofing attack [2], replay attack[4], Black-hole attack[7], flooding attack[7], colluding mis-replay attack [6]and many other attacks gray hole attack is more default and destructive to analyze. On MANETs it manifested when a malicious node is able to silently discard some messages known as gray hole attack and in case of all messages it is known as black hole attack. The attack can be further defined as, if the attacker is able to smoothly manipulate routing tables so as to increment the probability that messages would be routed through it. Gray-hole is more disastrous and storm threat, as it seductively discards messages, it is also difficult to figure out this uncertainty of messages.

The remainder of this section II provides that this survey will provide a better understanding of the different directions in which research has been done on this topic, and how techniques developed in one area can be applied in different domains for which they were not intended to begin with. And added two more different categories of attacks and its prevention techniques, information theoretic and spectral techniques used for gray-hole attack. This survey is an attempt to provide a structured and broad overview of extensive research on anomaly detection techniques spanning multiple research areas and application domains. Most of the existing surveys on attacks either focus on a particular application domain or on a single research area.

2. LITERATURE SURVEY

2.1 Attacks on Ad-hoc Network

MANET technology is used immediately to provide secure access between multiple mobile nodes without the need for a present communications infrastructure achieving a multi-hop architecture with the basis of two principles: routing and auto-configuration. While there are already quite a lot of established works undertaken for routing and alternatively these are related to secure routing. This, in turn, led to the current situation where these protocols are threat to a multitude of attacks, such as worm-hole attack [3] when the nodes fake a route that is shorter than the original one within the network. And confuse routing mechanisms which rely on the knowledge about distance between nodes.

Spoofing attack [2], when a malicious party impersonates another device. The different types of spoofing attacks includes; IP Address, ARP spoofing (Address Resolution Protocol), and DNS Server. A SYN flood [4] is a form of denial-of-service attack which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. A replay attack [5] (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

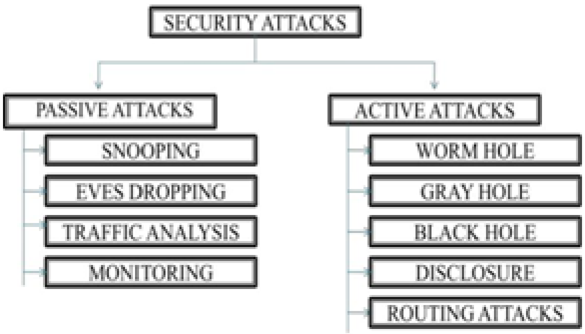

Chart-1: Various attacks of network routing protocols.

This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it. An attack on a security protocol using replay of messages from a different context into the intended (or original and expected) context, thereby fooling the honest participant(s) into thinking they have successfully completed the protocol run. Colluding mis-relay attack [6] is been detected when a multiple attackers work at a time in collusion to modify or drop routing packets to disrupt routing to destination in a MANET. And to detect these types of attack a conventional acknowledgement-based method is used. These are some various different types of attacks seen in ad-hoc networks as shown in chart 1.

2.2 Black- and Gray-Hole Attack

Black holes in the network refer to locations where malicious nodes discard network traffic without the source being told that the parcel did not achieve the asked goal [7]. Notwithstanding of the mobile routing protocol, every node on the path between the source and goal is a potential black-hole attacker. The attack surface can be upgraded, be that as it may, with particular advances executed by the attacker to expand the likelihood of arriving on the path to/from a particular (or all) victim(s).

Black-hole is a special case of the more general gray-hole, in which packets are selectively dropped while allowing others through. It focuses on the case in which the attacker selectively forwards data packets of every node except the victim's [8]. It does not try to isolate the victim; thus, control packets are forwarded. An OLSR based network is vulnerable to gray-hole attack. The attacker may send, for instance, a bogus HELLO messages to its one-hop neighbors, claiming to know more one-hop neighbors than it actually does. This will illegitimately increase its probability of being chosen as a sole MPR by its neighbors. The more neighbors an attacker claims to have, the larger the potential impact of the attack.

Consider Fig 2, depicting a specific network topology [1], where *x* is an attacker and *v* a victim. *x* advertises a bogus HELLO message containing *{f, v, g}* namely, *v* and each of its two-hop neighbors, and adds a fictitious *Fx* in order to ensure the attack's success.

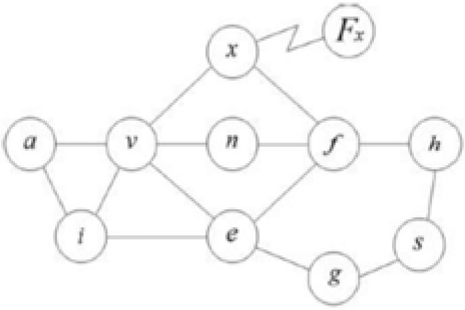

Fig -2: Example of a gray-hole attack.

Being the most cost-effective node in *v's* view of the network topology, it nominates *x* as its sole MPR. From here the attack can easily commence, as nodes from all around the network will direct data traffic destined for v towards *x*, which can drop packets at will.

2.3OLSR Routing Protocol Optimization for VANETs

In this paper [10], the author defines an optimization problem to tune the OLSR (Optimized Link State Routing protocol) protocol, obtaining automatically the configuration that best fits the specific characteristics of VANETs. It is also an optimization of the classical Link-State Routing protocol (LSR) which focused for reducing network overhead. OLSR selectively re-transmits messages based on a specified set of rules. The crux of the optimization is based upon a subset of 1-hop neighbors, called multi-point relays, which are designated as forwarding agents for control packets throughout the network. This protocol has been chosen since it presents a series of features that make it suitable for highly dynamic ad hoc networks

The main drawback of OLSR is the necessity of maintaining the routing table for all the possible routes. Such a drawback is negligible for scenarios with few nodes, but for large dense networks, the overhead of control messages could use additional bandwidth and provoke network congestion. This constrains the scalability of the studied protocol.

OLSR daemons periodically exchange different messages to maintain the topology information of the entire network in the presence of mobility and failures. The core functionality is performed mainly by using three different types of messages: HELLO; topology control (TC); and multiple interface declaration (MID) messages.

i. HELLO messages are exchanged between neighbour nodes (one-hop distance). They are employed to accommodate link sensing, neighborhood detection, and MPR selection signaling. These messages are generated periodically, containing information about the neighbor nodes and about the links between their network interfaces.

ii. TC messages are generated periodically by MPRs to indicate which other nodes have selected it as their MPR. This information is stored in the topology information base of each network node, which is used for routing table calculations. Such messages are forwarded to the other nodes through the entire network. Since TC messages are broadcast periodically, a sequence number is used to distinguish between recent and old ones.

iii. MID messages are sent by the nodes to report information about their network interfaces employed to participate in the network. Such information is needed since the nodes may have multiple interfaces with distinct addresses participating in the communications.

Each node in the network maintains network topology based on both the HELLO and TC messages it receives. It then calculates and stores, for each node discovered, the shortest distance (i.e., the minimal required hops between the source and the destination) between itself and one of the destination's node MPRs; hence, the shortest path to the destination.

2.4 DCFM

DCFM was proposed by [1] in order to address the problem of node isolation in OLSR based networks. It identifies potential malicious nodes trying to falsify HELLO messages using only internal information within the victim, without relying on any centralized or external trusted party. Such early detection prevents a possible attack before it can manifest. DCFM verifies the validity of a HELLO message by looking for contradictions between what the message claims and its pre-acquired topological knowledge. According to DCFM, sole MPRs nominations are allowed only when no contradictions are found. With the presence of contradictions, an MPR can be nominated for all two-hop neighbours for whom the suspected node is the only access point. It cannot, however, be nominated as sole MPR for two-hop neighbours that can be reached through other paths.

I. PREVENTING THE GRAY-HOLE ATTACK USING DCFM

The original DCFM was developed in order to identify and prevent the node isolation attack [1] In the gray-hole attacks, however, this solution is incomplete. Attackers can still orchestrate their attack by dropping data packets that were to be routed through them-even when it was not appointed as sole MPRs.

Avoidance of selecting a suspected node as a sole MPR, which is the crux of DCFM, mainly prevents the gray-hole attack. There are, however, two additional venues in which a malicious node can circumvent DCFM based protection:

i. When it is a natural candidate for passing data from *ADJ2(v)* to *v*; and

ii. When topology restraints require that it be appointed as sole MPR, i.e., when there is no other connection to some node.

This simulations show that although the probability of attack success is less in either of these attack venues when compared to the main venue, non-the-less it is still feasible. Using internal knowledge gained by DCFM, it present an improved method denoted by IMP (short for IMProvement), as a method of further decreasing attack success to include these two venues as well.

DCFM defines three rules that must be satisfied before a HELLO message sender is considered trustworthy. Example of a gray-hole attack: node *x* claims to know every two hop neighbor of *v*, as well as *Fx*, a non-existent node. Trusted senders can be nominated as sole MPRs for two-hop nodes that can otherwise be reached, subject to the OLSR protocol [1].

i. When node *x* advertises a HELLO message containing *ADJ(x)*. For every node ∈ ( ) ∩ ( ) should verify that ∈ ( ).

ii. For each node *y* mentioned in a HELLO message, *v* should check whether there exists *z* ∈ ( ).

iii. *v* must treat a HELLO message containing all nodes of the network except for *ADJ(v)* , as a potential attack. Nodes must apply each of the mentioned rules sequentially, advancing from one rule to the next iff there are no contradictions. Failure of any of the rules would require that *v* appoint *x* as a sole MPR only for the nodes that were exclusively declared in its HELLO message.

2.5. Different threat models

i. Passive Silent Attacker (PSV): This attacker was randomly placed within the network. It has done nothing for increasing its chances of becoming a routing node for the packets (in order to drop them). Results of this attacker type were used as a baseline for the gray-hole attack when compared with the more sophisticated attacks.

ii. Randomly Located Attacker (RND): Similar to the passive attacker, this malicious node is randomly placed within the network. It differs by the fact it would try to get itself appointed as a sole MPR of the victim whenever there is one-hop neighbors.

iii. Initially One-Hop Neighbor Attacker (1HOP): Attacker who is initially located as a one-hop neighbor of the victim. This attacker is similar to the one above, except its initial position isn't random. It is purposely placed close enough to the victim so as it will begin as one-hop neighbors.

iv. Shadow Attacker (shdw): This attacker was given the capability of shadowing the victim's movements from a distance of 190 meters, constantly remaining a one-hop neighbor of the victim. This distinguishes it from the previous attacker who only begins as a neighbor, but the distance can increase as the simulation commences.

v. MITM Attacker (MITM): This attacker improves the ability of the shadow attacker. Not only does it remain a one-hop neighbor poised for attack, it is given awareness for the source node location. This allows it to locate itself on a line between the two nodes, increasing the likelihood of being on the shortest path between the source and victim.

For each of the attackers, it will be examined with these following cases:

i. The package arrived at its destination (arrived).

ii. The package was lost by third party on its way for some obscure reason irrespective of the attacker (lost3rd).

iii. The package was dropped by the attacker, who (by chance or orchestrated) is a neighbor to the victim, even though there was at least one other node who could have forwarded the packet (attacker Neighbour).

iv. The package was dropped by the attacker, who (by chance or orchestrated) is a neighbor to the victim, but was the only route available (attacker Single Neighbor).

The package dropped by the attacker located at least two-hop from the victim (attacker). With the help of these different attackers and techniques, the attack can be analyzed and prevented. The information gained from theoretical and spectral techniques and contradiction rule, it gives a better understanding of gray-hole attack and OLSR based network.

3. CONCLUSION

This survey is an attempt to provide a structured and broad overview of extensive research on gray-hole attack and techniques. For each of the categories, we not only discuss the techniques, but also identify unique assumptions regarding the nature of attacks. We also provide the prevention techniques, and then show how the different existing techniques in that category are variants of the basic technique. This template provides an easier and more succinct understanding of the techniques belonging to each category. Further, for each category we identify the advantages and disadvantages of the techniques. We also provide a discussion of the computational complexity of the techniques since that is an important issue in real application domains. Thus the dropped packets can be reduced using this mechanism.

REFERENCES

[1] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Roy David Margalit, and Asaf Shabtai "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 16, NO. 8, AUGUST 2017.

[2] D. Raffo, C. Adjih, T. Clausen, and P. M€uhlethaler, "An advanced signature system for OLSR," in Proc.2nd ACM Workshop Secur. Ad Hoc Sensor Netw., 2004, pp. 10–16. [Online].Available: http://doi acm.org/.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE J. Select. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

[4] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," in Proc. OLSR Interop Workshop, 2005, pp. 28–29.

[5] C. Adjih, T. Clausen, P. Jacquet, A.Laouiti, P.Muhlethaler, and D. Raffo, "Securing the OLSR protocol," in Proc. Med-Hoc-Net, 2003, pp. 25–27.

[6] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Nis01–2: A collusion attack against OLSR-based mobile Ad Hoc networks," in Proc. IEEE Globecom, Nov. 2006, pp. 1–5.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M.Jahnke, and J. Tolle, "Detecting black hole attacks in tactical MANETs using topology graphs," in Proc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.

[8] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," in Proc. Int.Conf. Wireless Netw., Las Vegas, Nevada, 2003, pp. 570–575.

[9] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in Proc. World Congr. Eng. Comput. Sci., 2008, pp. 22– 24.

[10] J. Toutouh, J. Garcia-Nieto, and E. Alba, "Intelligent OLSR routing protocol optimization for VANETs,"IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1884– 1894, May 2012.

[11] Onkar V.Chandure, V.T.Gaikwad, "Detection &Prevention of Gray Hole Attack in Mobile Ad-Ho Network using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012 27.