www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 2 February 2018, Page No. 23551-23556
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i2.06

A Survey for Analyzing & Preventing of Gray-hole Attack Minimization for OLSR Based Network

Bobby K Simon[1], Anjana P Nair[2]

[1] M.Tech Computer Science & Engineering.
Sree Buddha College of Engineering, Ayathil, Elavumthitta
Pathanamthitta, Kerala, India.
[2] 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 network (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.
Keywords: MANET, OLSR, DCFM, Gray-hole attack**.**

1. Introduction

Optimized Link Routing Protocol (OLSR) is a proactive directing convention which is generally utilized MANET conventions. The quality of-service (QoS) of OLSR fundamentally relies upon the choice of its parameters, which decide the convention operation and speaks to a superior innovation that stop the sudden undisturbed attack in checking of network nodes. Security is a primary concern for specially appointed network. Information exchanging network conventions dissecting and checking have turned out to be expanding attack in now a day. Especially ad-hoc network are the most difficult zone for organize convention plan and execution have turned out to be progressively mind boggling, Because of network topology, inward conclusion, and aggregate cooperation of network nodes. Network protocols are usually for maintaining capable in data transferring between other various nodes. The optimization framework is used as a piece of this paper to find as balanced as possible setup parameters of the OLSR protocol, in spite of the way that it could particularly be used in like manner for different other routing protocol(AODV, PROAODV, GPSR, FSR, DSR, et cetera.) [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. A specially appointed network comprises of a gathering of "peer" nodes that can convey without the assistance from a settled framework. DCFM's primary instrument it's to mitigate the node confinement attack by depending exclusively on interior information procured by every node amid routine routing. What's more, in using a similar procedure utilized for the attack to anticipate harm. As both node disengagement and dark opening attacks require comparative preparatory strides for attack execution, in particular

cajoling a casualty into designating the attack as sole multipoint relay (MPR) node, which is in charge of broadcasting a node's presence to the network. DCFM is and great reason for moderating the gray-hole attacks.

Among the distinctive different sorts of assaults including wormhole attack [3], ridiculing attack [2], replay attack[4], Black-hole attack[7], flooding attack[7], collouding mis-replay attacks [6],and numerous different attacks gray hole attack is more default and dangerous to dissect. On MANETs it showed when a malevolent node can noiselessly dispose of a few messages known as dark opening assault and if there should be an occurrence of all messages it is known as black hole attack. The attack can be additionally characterized as, if the attack can easily control steering tables in order to increase the likelihood that messages would be directed through it. Gray-hole is more appalling and tempest danger, as it enticingly disposes of messages; it is likewise hard to make sense of this vulnerability of messages.

The rest of this section II gives that this review will give a superior comprehension of the distinctive headings in which inquire about has been done on this theme, and how procedures created in one region can be connected in various areas for which they were not expected in any case. What's more, included two more unique classifications of attacks and its counteractive action procedures, data theoretic and otherworldly networks utilized for gray-hole attack.. This review is an attempt to provide a structured and broad overview of extensive research on anomaly detection techniques spanning multiple research areas and application domains. The majority of the current studies on attacks either concentrate on a specific application domain or on a single research zone.

2. Literature Survey

2.1 Attacks on Ad-hoc Network

MANET innovation is utilized promptly to give secure access between various portable nodes without the requirement for a present correspondences foundation accomplishing a multi-hop architecture with the premise of two standards: routing and auto-setup. While there are now a considerable amount of set up works embraced for routing and then again these are identified with secure directing. This, thusly, prompted the present circumstance where these conventions are risk to a large number of attacks, for example, worm-opening attack [3] when the nodes counterfeit a route that is shorter than the first one inside the network. Furthermore, confuse routing mechanisms which depend on the information about separation 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 network in an attempt to consume enough server resources to make the network unresponsive to legitimate traffic. A reply attack [5] (also known as playback attack) is a form of network attack in which a valid data transmissions is malignantly or falsely rehashed or postponed. This is done either by the originator or by an enemy who blocks the information and re-transmits it. An attack on a security protocol utilizing replay of messages from an alternate setting into the planned (or unique and expected) setting, subsequently tricking the legit participant(s) into supposing they have effectively finished the protocol run. Colluding mis-relay attack [6] is been identified when a various attacker work at once in arrangement to adjust or drop routing bundles to disturb directing to goal in a MANET. What's more, to recognize these kinds of attack a regular affirmation based technique is utilized. These are some various different type of attacks seen in ad-hoc networks as shown in Figure 1.

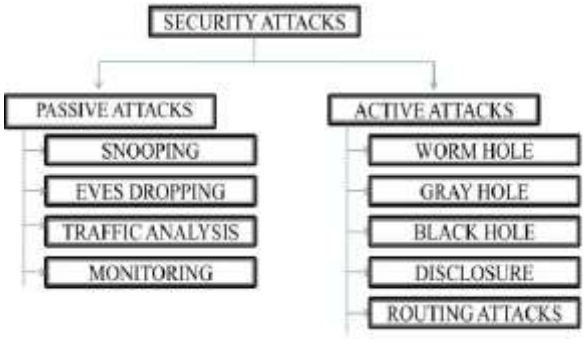

Figure 1: Various attacks of network routing protocols

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 unique instance of the more generally gray-hole attack, in which packets are specifically dropped while permitting others through. It concentrates working on this issue in which the assailant specifically advances information bundles of each node with the exception of the casualty's [8]. It doesn't attack to separate the casualty; hence, control parcels are sent. An OLSR based network is defenseless against dark opening attack. The assailant may send, for example, a false HELLO messages to its one-hop neighbors, guaranteeing to know more one-jump neighbors than it really does. This will misguidedly expand its likelihood of being picked as a sole MPR by its neighbors. The more neighbors an attacker claims to have, the bigger the potential effect of the attack.

Think about Figure 2, depicting a particular network topology [1], where *x* is an attack and *v* a victim. *X* advertises a bogus HELLO message containing *{f, v, g}* to be specific, *v* and each of its two hop neighbors, and includes an invented *Fx* so as to guarantee the attack's prosperity.

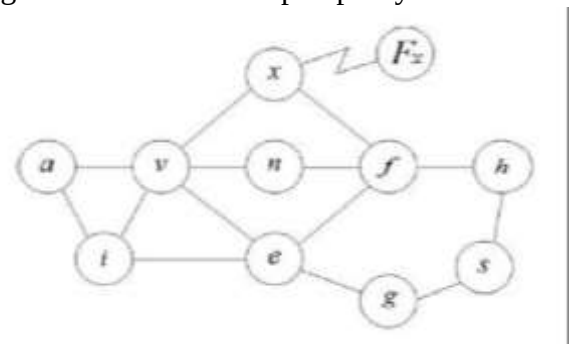

Figure 2: Example of a gray-hole attack.

Being the most cost-effective node in *v's* perspective of the network topology, it assigns *x* as its sole MPR. From here the attack can without much of a stretch initiate, as nodes from all around the network will coordinate information activity bound for *v* towards *x*, which can drop packets voluntarily.

2.3 OLSR Routing Protocol Optimization for VANETs

In this paper [10], the creator characterizes an optimization issue to tune the OLSR (Optimized Link State Routing protocol) protocol, acquiring consequently the design that best fits the particular attributes of VANETs. It is additionally a streamlining of the traditional Link-State Routing protocol (LSR) which centered for decreasing network overhead. OLSR specifically re-transmits messages in light of a predetermined arrangement of tenets. The essence of the streamlining depends on a subset of 1-hop neighbors, called multi-point relays, which are assigned as sending specialists for control parcels all through the network. This protocol has been picked since it introduces a progression of highlights that make it reasonable for very unique especially ad hoc networks.

The fundamental drawback of OLSR is the need of keeping up the routing table for all the possible routers. Such a downside is irrelevant for situations with couple of nodes, yet for expansive thick networks, the overhead of control messages could utilize extra data transmission and incite arrange congestion. This constraints the adaptability of the considered protocol.

OLSR daemons occasionally trade distinctive messages to keep up the topology data of the whole network within the sight of portability and disappointments. The core functionality is performed essentially by utilizing three unique kinds of messages: HELLO; topology control(TC);and multiple interface declaration (MID) messages.

i. HELLO messages are exchanged between neighbor nodes (one-hop distance). They are utilized to suit interface detecting, neighborhood detection, and MPR choice flagging. These messages are produced intermittently, containing data about the neighbor nodes and about the connections between their network interfaces.

ii. TC messages are produced intermittently by MPRs to show which different nodes have chosen it as their MPR. This data is put away in the topology data base of each network node, which is utilized for directing table counts. Such messages are sent to alternate nodes through the whole network. Since TC messages are communicated occasionally, a succession number is utilized to recognize later and old ones.

iii. MID messages are sent by the nodes to report data about their network interfaces utilized to take an interest in the network. Such data is required since the nodes may have different interfaces with distinct

addresses participating in the communications.

Every node in the network keeps up organize topology in view of both the HELLO and TC messages it gets. It then calculates and stores, for every node found, the most brief separation (i.e., the insignificant required bounces between the source and the goal) amongst itself and one of the goal's node MPRs; thus, the most limited way to the goal.

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 utilizing just inward data inside the casualty, without depending on any centralized or external trusted party. Such early recognition keeps a conceivable attack before it can show. DCFM confirms the legitimacy of a HELLO message by searching for inconsistencies between what the message cases and its pre-acquired topological information. As indicated by DCFM, sole MPRs assignments are permitted just when no logical inconsistencies are found. With the nearness of logical inconsistencies, a MPR can be named for every one of the two-hop neighbors for whom the presumed node is the main access point. It can't, not withstanding, be selected as sole MPR for two-hop neighbors that can be come to through different ways.

2.4.1 Preventing the Gray-Hole Attack Using DCFM

The first DCFM was produced with a specific end goal to recognize and keep the node disconnection attack [1]. In the dark opening attacks, be that as it may, this arrangement is deficient. Assailants can in any case organize their attack by dropping information parcels that should have been directed through them-notwithstanding when it was not delegated as sole MPRs.

Shirking of choosing a speculated node as a sole MPR, which is the core of DCFM, essentially keeps the dark gap attack. There are, notwithstanding, two extra scenes in which a pernicious node can dodge DCFM based assurance:

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 Improvements), as a method of further decreasing attack success to include these two venues as well.

DCFM characterizes three decides that must be fulfilled before a HELLO message sender is viewed as reliable. Case of a dark opening attack: node *x* cases to know each two bounce neighbor of *v*, and *Fx*, a non-existent node. Trusted senders can be designated as sole MPRs for two-jump nodes that can generally be achieved, subject to the OLSR protocol [1].

i. When node *x* advertises a HELLO message containing *ADJ(x)*. For every node $Z \in ADJ(x) \cap ADJ(\ )$, should verify that $x \in ADJ(z)$.
ii. For each node *y* mentioned in a HELLO message, *v* should check whether there exists $z \in ADJ(y)$.
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 if 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

The attacker can be designed with one of the five following different capabilities [11], [1]:

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).

v. The package dropped by the attacker located at least two-hop from the victim (attacker).

With the assistance of these different attack and networks, the attack can be examined and anticipated. The data picked up from hypothetical and ghastly methods and logical inconsistency govern, it gives a superior comprehension of dim opening attack and OLSR based network.

3. Conclusion

This review is an attempt to give an organized and expansive diagram of broad research on gray-hole attack and methods. For each of the classifications, we examine the networks, as well as distinguish interesting suspicions with respect to the idea of attacks. We additionally give the counter active action strategies, and after that show how the diverse existing methods in that class are variations of the essential procedure. This format gives a simpler and more compact comprehension of the procedures having a place with every class. Further, for every class we distinguish the preferences and inconveniences of the methods. We likewise give a talk of the computational unpredictability of the procedures since that is a vital issue in genuine application areas. Subsequently the dropped parcels can be diminished utilizing this instrument.

References

[1] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Roy David Margalit, and AsafShabtai "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. Muhlethaler, "An advanced signature network 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. Area 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] OnkarV.Chandure, V.T.Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012 27.

Author Profile

Bobby K Simon received the Bachelor's Degree in Computer Science and Engineering from Karpagam University, Tamil nadu, India in 2017. He is currently pursing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Kerala, India. His research area of interest includes the field of internet security, data mining and technologies in Department of Computer Science and Engineering.

Anjana .P.Nair received the bachelor's degree in LBS Institute of Technology for Women, Kerala, India. And master's degree in Computer Science and Engineering from Sree Buddha College of Engineering, Kerala, India in 2013. She is a lecturer in the Department of Computer Science and Engineering, Sree Buddha College of Engineering. Her main area of interest is Core Computers and has published more than 10 referred papers.