Mitigating Various Attacks in OLSR Using 3D Framework

L.M.Mary Jelba
Research Scholar, Dept. of Computer Science, Sri Krishna Arts & Science College Coimbatore, Coimbatore, Tamilnadu, India.

S.Gomathi
Head of the Department, Dept. of Computer Technology, Sri Krishna Arts & Science College Coimbatore, Coimbatore, Tamil Nadu, India.

Abstract – Mobile Ad-hoc networks (MANET) are more defenseless against security violations in many circumstances. This is undesirable due to their communication channel being wireless and the co-operative nature of the nodes forming a network. Attacks can be classified into many types based on the process and behavior. But the attacks generally fall under one of the following categories: Black hole attack, node isolation attack, Flooding attack, Wormhole attack, Spoofing attack, grayhole attack, Detour attack, Falsified route error generation attack and Rushing attack. Optimized Link State Routing (OLSR) protocol is designed based on optimization of link state protocol and performs effectively for large and dense ad- hoc network. Different solutions have been proposed for different types of attacks, but, these solutions often compromise routing efficiency or network overload and generated many false alarms. There are several attacks are unhandled in OLSR protocol. So this paper handles different types of attacks in OLSR with novel techniques. In this paper we handled 3 types of attacks in OLSR named as grayhole, wormhole and black hole along with the DOS attack. The proposed system generates an effective framework with virtual nodes called as Virtual Interaction Framework to detect, defend and dispense (3D-OLSR).

Index Terms – MANET, Node isolation attack, MPR selection, OLSR protocol.

1. INTRODUCTION

In mobile ad-hoc networks there are several routing protocols are proposed. These types of protocols are categorized into two types known as proactive and reactive protocols. In this paper, we have used OLSR (Optimized Link State Routing), which is a proactive protocol. In proactive nature, every node in the network maintains a list of routing information. Although OLSR is quite efficient in bandwidth utilization and in path calculation, it is vulnerable to various attacks such as Black hole attack, node isolation attack, Flooding attack, Wormhole attack, Spoofing attack, grayhole attack, Detour attack, Falsified route error generation attack and Rushing attacks [1][2][3].

In this paper we review n number of security attacks such as gray hole, black hole, wormhole, and node isolation attack [4] and proposes a new 3D (detect, defend and dispense) method to thwart those attacks.The proposed framework on OLSR with Virtual Interaction Framework (VIF) relies on the internal knowledge acquired by each node during routine routing, and expansion of virtual nodes. Moreover, VIF utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is consistent with [5]'s general claim that OLSR functions best on large networks.

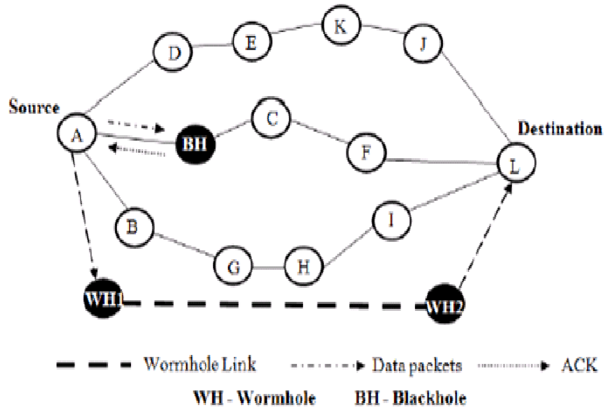
2. LITERATURE REVIEW

Technique	**Advantages**	**Disadvantages**
Public Key Infrastructure With distributed Certificate Authority	improves the control traffic load	malicious nodes with proper credentials could not be identified
Secure Clustering based OLSR (SCOLSR).	Increases the life time of ad-hoc networks in the presence of selfish nodes in the network. Reduced Multi Point Relay (MPR) nodes.	accumulation of reputation is very complicated

MPR S witching (FMS-OLSR)-collusion attack	observes symptoms of attack and temporarily blacklist potential attackers	False alarms exists
Acknowledgement scheme	Protects the network from link spoofing, wormhole attack without requiring location information or the full topology of the network. Increases PDR	Communication overhead

a. Black hole attack:

In OLSR, black hole attack is a malicious node, which uses its routing protocol in order to release of false news about the routing, these type of nodes sends a fake data, that they are having the shortest path to the destination node. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. In the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [6]. In protocol based on flooding, the reply from attacker node will be received before the actual node reply by the requestor node. So based on this, the forged route is created. If the route established by the attacker, the data either can be transmitted to the unknown address or the packets may dropped.



b. Wormhole attack:

Wormhole attack is another severe attack in MANET, which also handled in this paper. In OLSR with the use of two malicious nodes the wormhole attack can be performed.

OLSR is open to wormhole attack, there are several security threatens affects OLSR performance. In case of wormhole attacks, the attacker node creates a tunnel to transmit the data to the unauthorized destination. In such case the nodes may send hello and topology control messages to its own neighbors for dissemination as false information into the set of contacts. So, this will create two isolated nodes to wrongly consider themselves as neighbors, and this will lead to failure of OLSR.

After they form a tunnel between them as shown in FiG:1, whenever a malicious node receives packets it tunnels them to the other malicious destination and in turn it broadcasts the packet to the same. So, the packet is travelling through the tunnel it reaches the destination speeder than other route and moreover the hop count through this path is going to be less so this path is established between the source and the destination [6]. When the path is established between the source and the destination through wormhole link they can misbehave in many ways in the network such as continuously dropping the packets or dropping a specific set of packets and analyzing the traffic and performing Denial of Service attack ie node isolation attacks.

c. Grayhole attack

In MANET, the most unpredictable attack is Grayhole attack. It will act as legitimate node for some duration and act as a malicious node at the rest of the time. The probability of being malicious is not easily determined. This increases the unpredictable packet loss.

d. Node isolation attack

Denial of service attack in OLSR is another critical security attack; the node isolation attack is a type of attack, which comes under DOS attack. This will be launched by malicious node in the network against the OLSR protocol. In such attack dishonest node creates forged link information and makes the network vulnerable. While sending the hello packets target node after receiving fake hello message the target node select the attacker node as only its MPR node. Here, the malicious node is only available to the legitimate node to communicate the destination. The destination node only sends and receive message from attacker node in networks.

3. PROPOSED SYSTEM

The proposed framework for secure OLSR is named as 3D-OLSR. The 3D refers the detect, defend and dispense. The proposed secure OLSR contains several state of authentication process, which is stated below.

The first step of the proposed method is that each node will only use information available to the node, because the proposed work is a decentralized framework. The framework actively verifies the HELLO message and its route information periodically and checks for the integrity of every HELLO message from each hop.

After every transaction the activity score will be calculated. If the node changes the route information, the activity score will be reduced. Based on the activity score the path will be selected. In case of node isolation attack, virtual node will be created and data will be delivered via the virtual node.

And the second process in utilization of node localization and time span option. Using and analyzing the node location information's, the attacker can be detected. And with the help of time span the wormhole attack can be detected.

a. Architecture

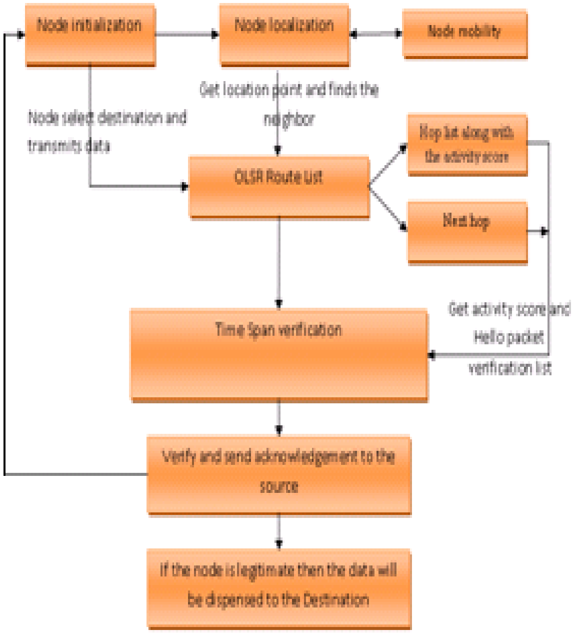

Node initialization
Node localization
Node mobility
Get location point and finds the neighbor
Node select destination and transmits data
Hop list along with the activity score
OLSR Route List
Next hop
Get activity score and Hello packet verification list
Time Span verification
Verify and send acknowledgement to the source
If the node is legitimate then the data will be dispensed to the Destination

Fig: 1.0 Proposed secure OLSR architecture

The above fig 1.0 represents the overall process of the proposed 3D architecture. The first step is node initialization and node localization, the location details will be frequently updated and verified using node mobility.

Algorithm

Steps:

Step: 1 if node not in malicious node list then

Step 2: Add the HELLO message information in 1-hop

Step 3: if 1-hop node reply received then

Step 4: Verify the accuracy adevertised by the

Step 5: HELLO message sender node

Step 6: if node is accurate

Step 7: Select that node is MPR node

Step 8: else

Step 9: Move the HELLO message sender to malicious list and update activity score

Step 10: end if

Step 11: end if

Step 12: Inform the network about the presence of new malicious node

Step 13: end if

4. CONCLUSION

Security is the most challenging issue in mobile ad hoc networks in specific in OLSR. This paper reviews the most important and vulnerable attacks namely the Blackhole, wormhole, Grayhole and node isolation attacks. Hence it becomes very important to detect such type of attacks as early as possible. Many techniques to mitigate these attacks have been provided. Every technique has its own advantages and limitations which are also listed in this paper. Further research should be carried out to develop the techniques for avoidance or detection of such attacks which would have minimum limitations.

REFERENCES

[1] S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777. [Online].vailable: ttp://www.google.com/patents/US20060176829

[2] C. E. Perkins and P. Bhagwat, "Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers,"in Proc. Conf. Commun. Archit., Protocols Appl., 1994, pp. 234–244.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Proc. IEEE Int. Multi Topic Conf. Technol., 2001, pp. 62–68.

[4] T. Clausen and P. Jacquet, "RFC 3626-Optimized Link State Routing Protocol (OLSR)," p. 75, 2003. [Online]. Available: http:// www.ietf.org/rfc/rfc3626.txt

[5] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," Dynamic Source Routing Protocol (DSR) Mobile Ad Hoc Netw. IPV4, 2007. [Online]. Available: http://tools.ietf.org/html/rfc4728

[6] C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.,Feb. 1999, pp. 90–100.

[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] 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.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” IEEE Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.

[10] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, “Implementation & evaluation of an ids to safeguard olsr integrity in manets,” in Proc. Int. Conf. Wireless Commun. Mobile Comput., 2006, pp. 45–50.

[11] D. Raffo, C. Adjih, T. Clausen, and P. M€uhlethaler, “An advanced signature system for OLSR,” in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 10–16.

[12] C. Adjih, D. Raffo, and P. M€uhlethaler, “Attacks against OLSR: Distributed key management for security,” in Proc. 2nd OLSR Interop/Workshop, Palaiseau, France, 2005.

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

[14] B. Kannhavong, H. Nakayama, and A. Jamalipour, “Nis01-2: A collusion attack against olsr-based mobile ad hoc networks” in Proc. IEEE Global Telecommun. Conf., Nov. 2006, pp. 1–5.

[15] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, “Analysis of the node isolation attack against olsrbased mobile ad hoc networks,” in Proc. Int. Symp. Comput. Netw.2006, pp. 30–35.

[16] Mittal, Poonam, Sanjay Batra, and C. K. Nagpal. "Implementation of a novel protocol for Coordination of nodes in Manet." International Journal of Computer Networks and Applications 2.2 (2015): 99-105.

[17] S.Zafar, H.Tariq,K.Manzoor, “Throughput and Delay Analysis of AODV, DSDV and DSR Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Computer Networks and Applications (IJCNA) Volume 3, Issue 2, March – April (2016).

[18] Sonal Telang Chandel, Sanjay Sharma.” Performance Evaluation of IPv4 and IPv6 Routing Protocols on Wired, Wireless and Hybrid Networks”, International Journal of Computer Networks and Applications (IJCNA), 3 (3), PP: 57-62.

[19] Priyaganga Guruswamy, Madhumita Chatterjee. “A Novel Efficient Rebroadcast Protocol for Minimizing Routing Overhead in Mobile Ad-Hoc Networks”, International Journal of Computer Networks and Applications (IJCNA), 3 (2), PP: 38-43.

[20] Ravneet Kaur, Neeraj Sharma. “Dynamic Node Recovery in MANET for High Recovery Probability”, International Journal of Computer Networks and Applications (IJCNA), 2(4), PP: 158-164.