IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Analysis of Attacks against Optimized Link State Routing Protocol -based Mobile Ad Hoc Networks

Himani Bali[1*], Naveen Hemrajani[2]

[1] Himani Bali, Assistant Professor, ECE, JECRC University, Jaipur, India
[2] Naveen Hemrajani, Professor, CSE, JECRC University , Jaipur, India

[*]*Corresponding Author: himani.bali@jecrcu.edu.in, Tel.: 0191-2455763*

Available online at: www.ijcseonline.org

Accepted: 09/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Mobile Adhoc Networks are vulnerable to attacks due to its dynamic topology. All attacks, blackhole, dropping attack and flooding are analyzed and implemented against Optimized Link State Routing Protocol on Network Simulator-3. The results clearly show how attacks could rigorously affect communication and, the need for security solutions for such highly dynamic networks.

***Keywords*—** Mobile Adhoc Networks, Optimized Link State Routing Protocol, Attacks, Blackhole, Dropping , Flooding.

I. INTRODUCTION

Conventional communication technology is changing rapidly. The opportunity to communicate via wireless technology brings about unlimited alternatives such as Mobile Adhoc Networks (MANETs), and wireless sensor networks (WSN). In MANETs, mobile nodes can communicate with no fixed infrastructure. This infrastructure less characteristic of MANETs enables the application of many different communication technologies. MANETs are expected to become widespread once certain research challenges have been successfully addressed, such as the provision of security for these dynamic networks.

Although MANETs are vulnerable to new forms of attack. A malicious node could disrupt the network and, cause unwanted results such as loss of information. An attacker could achieve its purpose mainly through exploitation of the weakness of the routing protocols and application protocols in MANETs.

An extensive analysis of attacks is necessary in order to develop suitable security solutions for MANETs, which is the primary aim of this study. In this paper, we identify three types of attacks, namely blackhole, dropping and flooding against Optimized Link State Routing Protocol (OLSR)-based MANET, analyze the attack in detail, and demonstrate the impact of the attack through simulations.

In this paper, Section I contains the introduction of MANETs , Section II contains the related work giving more emphases on attacks on MANETs, Section III and IV contain the description of OLSR and various attacks, their effect on OLSR respectively .Section V describes the results and discussion. Section VI concludes research work with future directions for improving the security of MANETs.

II. RELATED WORK

Security is a significant feature in MANETs, especially when they are used in some really critical applications like battlefields or tragedy recovery. Ad-hoc networks are vulnerable to several routing attacks, including address spoofing, alteration of packets, black hole, and dispersed denial-of-service.

Bounpadith Kannhavong & Abbas Jamalipour [4] and Lalith Suresh [2] have talked about collusion attack against OLSR. It has been presented a technique to detect the attack by utilizing information of two hops neighbors.
One of the most analyzed attacks to be found in the literature is the blackhole attack, due to being a specific attack to ad-hoc routing protocols. Four routing protocols (AODV, DSR, OLSR, and TORA) were analyzed under blackhole attack in MANETs [3]. The results showed that AODV performed poorer than other protocols on simulated networks under attack.

Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma [5] classifies various types of attacks on MANETs such as Black-Hole, Worm-Hole, Subil, Jellyfish & Rushing attack and their prevention techniques.

G.A. Pegueno and J. R. Rivera [7] made an extention to MAC 802.11 to make the network more secure and reliable in case of various attacks like blackhole, wormhole etc.
Ankur Thakur and Anuj Gupta [8] studied blackhole attack in detail and discussed various methoeds to protect the network from blackhole attack by making certain changes in route request and route reply messages.

III. ROUTING PROTOCOLS: OLSR

OLSR is proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. OLSR has also three types of control messages which are described below.

HELLO: The HELLO message is a control message that is transmitted for information about the neighbors and for calculating Multi-Point Distribution Relays (MPR).

Topology Control (TC): TC messages are generated and flooded using the MPR optimization process at regular intervals and also when there is a change in MPR selector set.

Multiple Interface Declaration (MID): The list of all IP addresses is contained by MID messages in the network. All the nodes running OLSR transmit these messages on more than one interface.

A. *OLSR Working*

OLSR diffuses the network topology information by flooding the packets throughout the network. The flooding is done in such a way that each node receives the packets and retransmits the received packets. These packets contain a sequence number so as to avoid loops. The receiver nodes register this sequence number making sure that the packet is retransmitted once. MPR is selected to reduce the retransmissions of the duplicate packets.

Only MPR nodes broadcast route packets. The nodes within the network keep a list of MPR nodes. MPR nodes are selected within the surrounding area of the source node. MPR is selected based on communication via HELLO messages sent between the neighbor nodes and to find an existing path to each of its 2 hop neighbors through MPR node. Once the routes are established , the source node can start sending data. The process is shown in Figure 1.

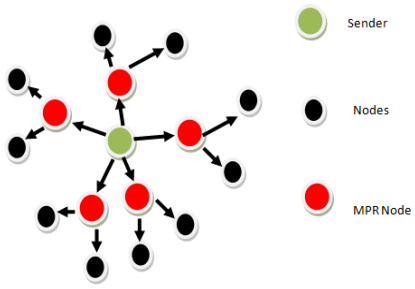

Figure 1.Flooding Packets using MPR

IV. ATTACKS ON MANETs

MANETs face various security threats or attacks in order to disrupt the performance of the networks. Blackhole attack, flooding and dropping attacks are described in this chapter.

A. *Blackhole Attack*

Blackhole attack is a kind of denial-of-service (DoS) attack which is launched by a malicious node against the sender node [8]. An attacker sends fake routing information to the neighbor node that it is having the shortest path between the source and destination. So, the other nodes send information through the malicious nodes and the attacker will capture all the data. An attacker drops the data packets or modifies the data packets coming from the source node and sends it to the destination. Only with the help of HELLO & TC messages the information is exchanged between the nodes in OLSR [8]. The node acting as a black hole sends a fake HELLO to the nodes and shows that it is having the multiple neighbor nodes for retransmitting the data. As a result, the source node thinks that the blackhole node has the access to all the nodes and hence it is selected as MPR. After selecting as the MPR all the data which is sent through the neighbor nodes will pass through miscellaneous MPR and the entire data packet will be captured.

Let us take a network based on OLSR as shown in Figure 2. In this figure, the lines just show Node A's view of the network.Let us take node M as the black hole node. This leads to some changes in the network as shown in Figure 3. The black hole node M sends fake HELLO message containing nodes A, B, C, D and E. This leads to Node A selecting only the black hole node M as MPR node. As a result nodes B, C will send TC messages not containing Node A and Node A will send data packets to nodes D, E through node M instead of B and C respectively . Therefore, the black hole node M has gained control over the connections from A to D and E.

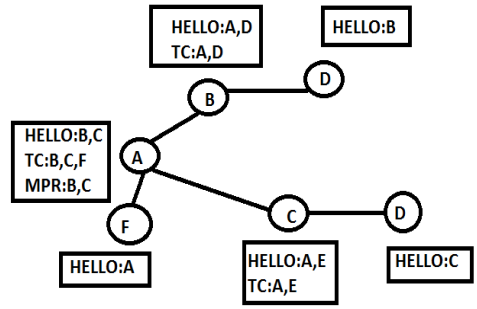

Figure 2.OLSR without Blackhole Attack

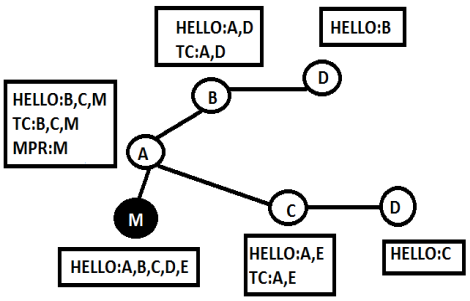

Figure 3. OLSR with Blackhole Attack

B. *Dropping Attack*

In dropping attack type, all the packets received by a malicious node are simply dropped. It is different from blackhole attack as the malicious node claims itself to have the shortest path and takes control of the traffic, and then drops the data packets. However, in a packet dropping attack scenario, the malicious node only drops data packets if a packet is transmitted through it. Even a simple dropping attack could cause serious consequences, especially in safety-related applications. Furthermore, it is difficult to distinguish from legal packet dropping on networks with high mobility.

C. *Flooding Attack*

The flooding attack is a type of DoS attack. The main aim of the attack is to exhaust the network by sending numerous control packets, resulting in network nodes unable to process legitimate traffic. Fake packets are continually sent in both routing protocols until the simulation terminates which decrease the functionality of OLSR. OLSR has less overhead as compared to other proactive protocols but this flooding attack increases the overhead.

V. METHODOLOGY

Each attack is evaluated against well-known network performance metrics: packet delivery ratio (PDR), overhead, end-to-end (E2E) delay.

All simulations are conducted in a widely used network simulator, Network Simulator-3(NS-3). The simulation parameters used in the experiments are given in Table 1.

Table 1: Simulation Parameters

Simulation Parameters	Value
Simulation Time	200 seconds
Network Area	800m×800m
Number of nodes	35
Routing Protocol	OLSR
Packet Size	512 bytes
Node movement at maximum Speed	Random
Communication Range	250 m
MAC Layer Protocol	802.11

VI. RESULTS AND DISCUSSION

A. Packet Delivery Ratio (PDR)

PDR is defined as the ratio of packets successfully received to the total sent.

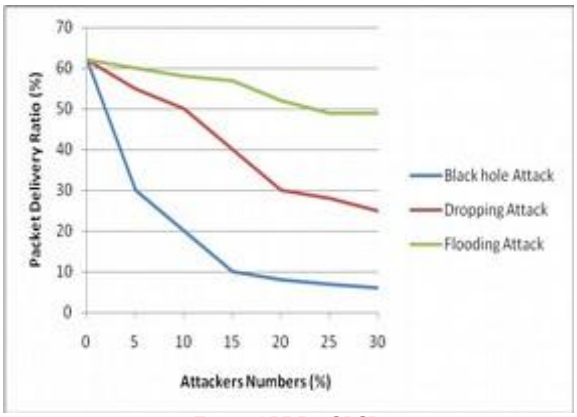

Figure 4.PDR– OLSR

Figure 4 shows the PDR of OLSR. As expected, while the attacker percentage in the network increases, PDR decreases.

Flooding attack does not have as severe effect as blackhole and dropping attack do. As the number of fake packets broadcast to the network increases, it will cause more packets to be dropped due to heavy traffic impacting the network.

B. Overhead

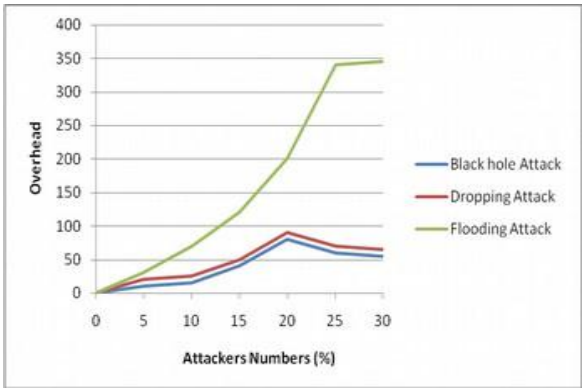

Figure 5. Overhead – OLSR

Figure 5 shows the overhead results for the attacks in OLSR. As the number of attacker increases, the overhead also increases due to disrupted routes. Flooding attack due to its very nature increases overhead the most. Blackhole and dropping attack also increases the overhead considerably due to its disruption of effective routes.

C. End-to-End (E2E) delay

E2E delay refers to the time taken by the packet to transmit across a network from source to destination.

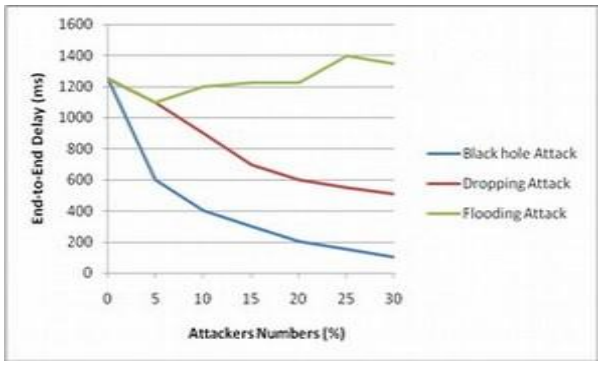

Figure 6. E2E – OLSR

After exceeding a certain threshold in flooding there is a slight change in E2E delay. In the existence of blackhole or dropping attacks, since fewer data packets are trying to be sent, they will be able to reach their destinations without waiting due to fewer traffic levels in the network. As shown in Figure 6, End to end delay is more prominent in Flooding.

VII. CONCLUSION AND FUTURE SCOPE

Mobile ad hoc networks are an emerging technology believed to be extensively used in the near future. However, security is a key issue that first needs to be addressed. In order to be able to develop suitable prevention and detection mechanisms for MANETs, the nature of attacks and their effects on the network should be carefully analyzed; and which was the primary aim of this study. The attacks, namely blackhole, flooding and dropping attack, are implemented on OLSR routing protocols. Although there have been some analyses of attacks specific to MANETs, their effects on more dynamic environments are lacking in the literature, hence they were explored in this current study. For OLSR, the attack type is more influential in such experimental settings. The subtle attacks such as blackhole attack decreases the performance of OLSR dramatically. The simulation results clearly show the need for security mechanism suitable for a highly dynamic environment.

ACKNOWLEDGMENT

This work would not have possible without the support of JECRC University for providing labs and software. I am especially indebted to Dr. Naveen Hemrajani, Head of Department of Computer science, JECRC University, Jaipur for providing me the idea and also for supporting my career goals.

REFERENCES

[1] R. D. Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "*Security in wireless ad-hoc networks a survey," Computer Communications*, vol. 51, pp. 1 – 20, 2014.

[2] E. F. Ahmed, R. A. Abouhogail, and A. Yahya, "*Performance evaluation of blackhole attack on vanet's routing protocols*," International Journal of Software Engineering and Its Applications, vol. 8, no. 9, pp. 39 – 54, 2014.

[3] P. Yi, Z. Dai, S. Zhang, and Y. Zhong, "*A new routing attack in mobile ad hoc networks,"* International Journal of Information Technology, vol. 11, no. 2, pp. 83–94, 2005.

[4] Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour "*Analysis of the Dropping Attack Against OLSR-based Mobile Ad Hoc Networks*" Proc. 7th IEEE International Symposium on Computer Network, pp 30-35,2006.

[5] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharm, "A *Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks*" Paper published in Journal of Computing, { ISSN-2151-9617}, pp. 41-48, January 2011.

[6] K. Biswas and Md. Liaqat Ali, "*Security threats in Mobile Ad-Hoc Network"*, Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[7] G.A. Pegueno and J. R. Rivera, "*Extension to MAC 802.11 for performance Improvement in MANET*", Karlstads University, Sweden, December 2006.

[8] Ankur Thakur and Anuj Gupta, "*Black Hole Problem with OLSR Protocol in MANETs"*, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4. Pp, 1-4, Sept 2014.

[9] R.Kumari, P. Nand, "*Performance Analysis of existing Routing Protocols"* International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE), ISSN-2320-7639, Vol. 5 No. 5, October-2017.

[10] R. Kumari, P. Nand , " *Performance analysis for MANETs using certain realistic mobility models:NS-2",*International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE),Vol.6, Issue.1 , pp.70-77, Feb-2018.

[11] Leena Pal, Pradeep Sharma, Netram Kaurav and Shivlal Mewada, "*Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks"*, International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.5, pp.1-4, 2013.

[12] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "*A Novel Security Based Model for Wireless Mesh Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.11-15, 2013.

Authors Profile

Ms. Himani Bali pursed Bachelor of Technology Integrated Masters of Technology in Electronics and Communication from Lovely Professional University in 2012. She is currently pursuing Ph.D. and working as Assistant Professor in Department of Electronics and Communication, JECRC University, Jaipur, since 2012. Her main research work focuses on wireless communication,Mobile Adhoc Networks. She has 5 years of teaching experience and 3 years of Research Experience.

Dr Naveen Hemrajani is currently working as Professor and HOD in Department of Computer Science, JECRC University, Jaipur, India, since 2013.He has published more than 70 research papers in reputed international journals. His main research work focuses on Computer Network and Software Engineering. He has got more than 15 years of teaching experience and 7 years of Research Experience.

