Indonesian Journal of Electrical Engineering and Computer Science
Vol. 13, No. 2, February 2019, pp. 677~682
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i2.pp677-682

Black hole attack behavioral analysis general network scalability

Layth A. Khalil Al Dulaimi[1] R.Badlishah Ahmad[2], Naimah Yaakob[3], Mohd Hafiz Yusoff [4], Mohamed Elshaikh[5]
[1,3,5]Embedded Networking and Advance Computing Cluster, School of Computer & Communication Engineering, Universiti Malaysia Perlis (UniMAP) Tingkat 1, Kampus Tetap Pauh, Perlis, Malaysia
[2,4]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, 21300 Kuala Terengganu, Malaysia

Article Info

Article history:

Received Sep 22, 2018
Revised Nov 10, 2018
Accepted Nov 25, 2018

Keywords:

AODV
BlackHole Attack
Mobile ad hoc network
(MANET)

ABSTRACT

A mobile ad hoc network (MANET) is a frameworkless system of different mobile devices known for its self-arranging conduct. MANETs can convey over moderately data transfer capacity compelled routing connections. In a blackhole assault, a malicious node falsely advertises the shortest path to the destination node, intending to disrupt communication. Our objective was to review the impact of a blackhole assault on networks. To accomplish this, we simulated MANET situations, which include the blackhole node, using the OMNET++ simulator to demonstrate the effects of a single blackhole attack and multiple blackhole attacks on MANET performance have examined for networks. We analysed MANET performance under blackhole assaults through the use of performance grids.

Corresponding Author:

Layth A. Khalil Al Dulaimi,
School of Computer & Communication Engineering,
Universiti Malaysia Perlis (UniMAP) Tingkat 1,
Kampus Tetap Pauh, Putra 02600 Arau, Perlis.
Email: Layth.a.khalil@gmail.com

1. INTRODUCTION

The The wireless network is an innovation that enables clients to access services and data electronically, regardless of their environmental position. The mobile ad hoc network (MANET) is an independent wireless network containing autonomous nodes that transfer and dynamically modify network connectivity [1, 2]. In MANETs, nodes are allowed to move randomly; therefore, the network's wireless topology may change quickly and unpredictably. MANETs eradicate the restraints of infrastructure and allow gadgets to make and join networks anywhere and anytime for almost any application since an ad hoc wireless network is self configuring, self organising and adaptive [3, 4]. A node in an ad hoc network can be the destination, source or intermediate node among any destination and source [1, 5]. The arbitrariness of specially appointed portability with no settled foundation, as well as the transmission nature of wireless channels and cooperative multi-hop communications among mobile nodes of mobile ad hoc networks, increases weaknesses [6, 7]. Penetrations can be classified as passive or active based on attacker behaviour. Passive penetration is in acquiring significant information regardless of cutting the routing process by spying on traffic. Active penetration is a more serious attack, as it attempts to gain illegitimate access to the network by intersecting the routing process to reduce network performance. Examples of possible active security penetrations in MANETs include rushing attacks, wormhole threats and blackhole attacks [8, 9]. A Byzantine attack [10] includes attacks on routing table access, as well as poisoning route caches, gray hole attacks [11-13] and the distributed denial of service threats [14, 15]. Blackhole assault is a serious security assault as it attempts to redirect the flow of information away from the proposed destination, as an aggressive node acts to possess the ideal path to the

destination node and adapts denial-of-service behaviour by killing data packets [16, 12] or forwards data packets to undesired destinations [16, 11, 17].

The main objective of this paper is to audit the impact of blackhole assaults on networks. To accomplish this, we simulated MANET scenarios, include blackhole nodes, using the OMNET++ simulator [3]. To simulate the blackhole node in MANETs, we simulated a blackhole attack assault to demonstrate its properties. We then assessed the impact of a blackhole assault on MANET.

The main contributions of this paper are to demonstrate the impact of single blackhole assaults and multiple blackhole assaults on MANET performance. We examined networks with 10 diverse numbers of nodes.

2. BLACK HOLE ATTACK

One of the most critical attacks on MANETs that affects network security is a blackhole attack. The classification of a blackhole attack is based on whether an attack is simple or cooperative. Normally a simple or ordinary blackhole attack likely occurs in MANETs when a bad-intentioned node (malicious node) tampers with the packet stream [9] and exploits routing protocol to answer the request from source node RREQ with a fake reply packet RREP pretending to own the ideal path to the goal node supported by highest sequence value as evidence the highest sequence value as evidence [19]. Consequently, a bad-intentioned node (blackhole node) blocks data packets from being delivered to the goal node or from even being forwarded to neighbouring nodes [20]. Figure 1 depicts simple blackhole behaviour.

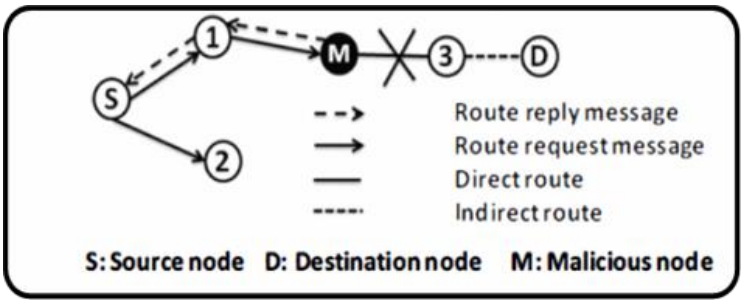

Figure 1. Simple black hole attack

On the other hand, in a cooperative blackhole attack, a group of nodes—at least two adjoining bad-intentioned nodes—aggressively collaborate to stop data packets from reaching their legitimate destination. This attack is more threatening than a simple blackhole attack due to the effortless nature of the attack execution and the difficulty for other participating nodes in the network to reveal this attack [6]. A cooperative attack is accomplished when a blackhole-intentioned node is the first among other neighbours of the source node. This node receives a RREQ packet from the source node to answer with a fake RREP packet offering the best route to the destination. Consequently, the source node begins to push data to the blackhole-intentioned node, which in turn passes data packets to the next blackhole teammate that either imprisons the data packets or participates with the blackhole teammate to swallow the data rather than pass it to the legitimate destination. Figure 2 shows a simple cooperative blackhole attack in which S and D denote source node and destination node sequentially, while B1 and B2 denote cooperative blackhole attack nodes.

Based on the ability of simple and cooperative blackhole attacking nodes to tamper routing information, it is obvious that blackhole attacks impact network layers [21] and this is considered a sort of denial-of-service threat that damages transmission of the network layer [22]. Successful schemes have been suggested in an attempt to reveal and block simple blackhole threats. However, the efficient detection of cooperative blackhole attacks is still unfeasible to schemes used for detecting simple blackhole attacks, and this motivates researchers to suggest more schemes to target such attacks. It is worth mentioning that blackhole attacks not only pose a threat to communication security in MANETs but also to vehicular ad hoc networks (VANET) [27] and wireless mesh networks (WMNs) [28].

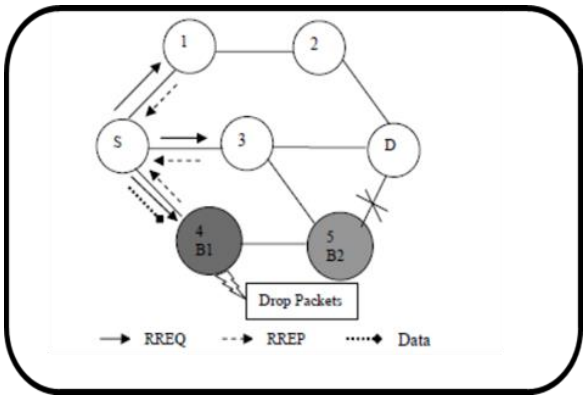

Figure 2. Cooperative blackhole attack

3. INVESTIGATING BLACKHOLE ASSAULTS IN AODV PROTOCOLS

The implementation of the blackhole attack is attempted on the ad hoc network. To be sure the execution worked effectively, we used OMNET++, one of the most common simulation tools in the networking field. Additionally, the NETAttack framework is based on the same idea as OMNET++ [23]. To test the implementation, we performed three simulations. In the first one, we did not use any blackhole node. In the second one, we added a single blackhole attack. In the third one, we added a cooperative blackhole attack nodes. We compared the outcomes of the simulations.

Simulation parameters and measured metrics. We utilised the following metrics in our review:

1) Packet delivery ratio (PDR): calculated by dividing the number of packets received by the destination by the number of packets originated from the source;
2) Average throughput: the average of successful message delivery over a communication channel; and
3) Average end-to-end delay: defined as the time taken for a data packet to be transmitted across MANETs from source to destination [18].

To take exact outcomes from the simulations the common parameters to all situations (scenarios) are reported in the Table 1.

Table 1. Simulations Parameters

Parameter	Value
Number of Mobile Nodes	20, 40, 60, 80 and 100
Simulation area	1000m x 1000m
Communication range	250m
Simulation time	600s
Simulation runs	50
Generated networks	10
Routing protocol	AODV
MAC layer protocols	802.11g
Number of attackers	1,5
Constant Bitrate (CBR) connection	4 packets/s
Packet size	512 bytes
Movements randomly	start between 0.5 and 1.5 s and they end amongst 290 and 295 s
Speed	1 m/s and the maximum differs from 5 to 20 m/s with a pause time of 15 s

4. PPRAISAL OF RESULTS

The (3) diverse simulations were tested. In the one, the nodes worked in collaboration among themselves save the network in communication. The two had one malicious node and the (3) had three malicious nodes performing by a blackhole attack.The results of these(3) simulations were compared to comprehend the network and node practices.To start, we assessed the PDR: Total number of data packets delivered divided by total number of data packets sent [30].

Table 2 shows that PDR was almost 1 before a blackhole attack, This means that almost all packets sent by the sender's node are received by the future node. But for the network with the Blackhole node, I lowered the PDR to 0, which means that all packets sent by the sender's node were dropped by the Blackhole contract.

Table 2. PDR Comparison

No. of nodes	No. of blackhole attacks	Single blackhole attack	Cooperative attack
20	93.67762	95.14093	90.03275
40	92.71282	92.22668	91.34945
60	97.36575	98.78501	98.04665
80	85.58254	90.9558	79.20676
100	69.67809	70.11424	65.1216

Figure 3 uses the data from Table 2, which compares the PDR before a blackhole attack and after one and two blackhole attacks.

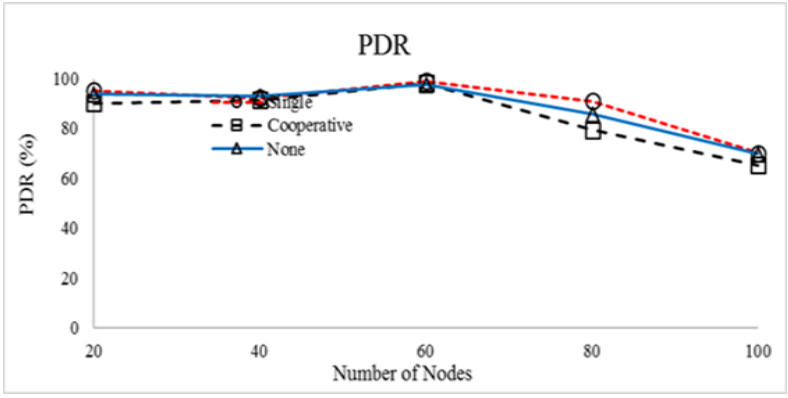

Figure 3. PDR

Table 3 shows the end-to-end delay (The average time used by a data packet to be sent to the destination). It is computed as the average of the specific end-to-end delay of every packet, thus extracting the average end-to-end delay for the entire network). There were end-to-end delay increases in situations with blackhole attacks as a result of dropping packets when receive packets by blackhole nodes.

Figure 4 which is drawn from above table's information compares end-to-end delay before blackhole attack and after one and three cooperative attacks:

Table 3.End-to-End Delay Comparison

No. of nodes	No. of blackhole attacks	Single blackhole attacks	Cooperative attacks
20	0.003601	0.002206	0.022125
40	0.008627	0.008805	0.010446
60	0.007723	0.006791	0.00929
80	0.010548	0.016151	0.014682
100	0.014768	0.014717	0.017243

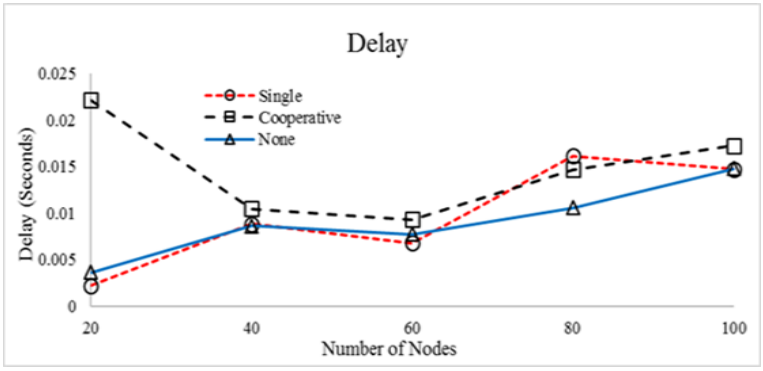

Figure 4. Delay

Table 4 shows throughput (defined as the ratio of the number of bits received over the time difference between the first and the last received packets). For diverse situations. When entering the blackhole, nodes in the network route request throughput increase. This implies that, after a blackhole attack, the number of data packets that communicate are fewer than the number of control packets generated.

Table 4.Throughput Comparison

No. of nodes	No.of blackhole attacks	Single blackhole attacks	Cooperative attacks
20	134357	136460.3	129131.2
40	308778.3	307389.1	304871.4
60	418781.9	424887	421710.5
80	490644.1	424347.6	454090.8
100	499438.3	353802.2	466776.1

Figure 5 uses data from Table 4, which compares throughput before a blackhole attack and after single and cooperative blackhole attacks.

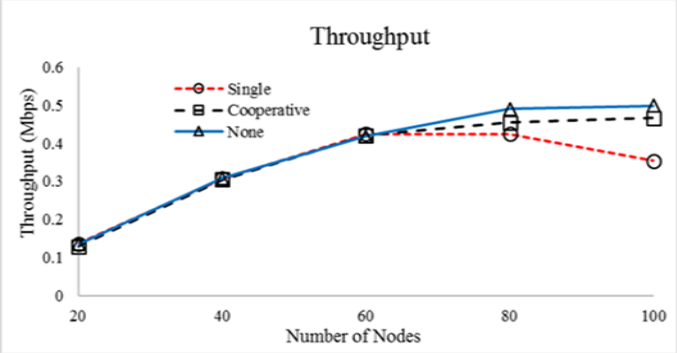

Figure 5. Throughput

5. CONCLUSION

In MANETs, nodes depend on each other to keep the network associated. In this manner, unlike customary wireless arrangements, such networks do not require any previous (settled) foundation, which limits their cost and sending time. Hence, security in MANETs is the greatest concern when considering the fundamental usefulness of such networks. MANETs regularly experience the ill effects of security assaults because of elements such as open medium, dynamic changes to their topology, the absence of focal observation and administration, helpful algorithms and no reasonable defence mechanisms. Blackhole attacks are an interesting topic for many researchers.

Hence, in this work, we analysed the effects of blackholes in an AODV network. For this reason, we applied an AODV protocol that behaves like a blackhole in the OMNET++ simulator (4.2.2). We simulated three scenarios on 20, 40, 60, 80 and 100 nodes, where the simulation was completed using UDP packets. In each situation, we assessed network performance before and after single and cooperative blackhole attacks. We investigated the effects of blackhole attacks on network performance, noting that attacks increased the number of dropped packets and decreased the PDR. Even when increasing the number of blackhole nodes, dropped packets increased and PDR dropped off. Blackhole attacks increased the number of dropped packets and decreased PDR in MANET performance.

REFERENCES

[1] V. Anil Kumar, R. C. Joshi, and M. Guide Dave "Design and development of a routing protocol for mobile ad hoc". *PhD diss*, 2008.

[2] N. H. Mistry, D.C Jinwala,. and M.A Zaveri,.,. MOSAODV: " solution to secure AODV against black hole attack". *IJCNS. International Journal of Computer and Network Security.*2009, 1(3): 42-45.

[3] M. Consolee, and A. Shahrabi. "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks". *In Advanced Information Networking and Applications Workshops, AINAW'07. 21st International Conference on*2007, 2: 679-684 .

[4] C. Ranajoy, and M. Routray. “Black Hole Combat Using Node Stability System in MANET. In International Joint Conference on Advances in Signal Processing and Information”. *Technology Springer* Berlin Heidelberg. 2011,, 1: 249-254.
[5] N. Adnan, and M. Howarth. “Protection of MANETs from a range of attacks using an intrusion detection and prevention system”. Telecommunication Systems 2013,52(4): 2047-2058.
[6] L. Nai-Wei, and F. Liu. “A secure routing protocol to prevent cooperative black hole attack in MANET”. In Intelligent Technologies and Engineering Systems Springer New York, 2013. pp. 59-65.
[7] P. Niroj Kumar, and S. Mishra. “Secure Hybrid Routing for MANET Resilient to Internal and External Attacks”. ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I. Springer International Publishing2014, 1: 449-458.
[8] S. Umang, B. Reddy, and M. N. Hoda. “Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption”. IET communications 2010 4(17): 2084-2094.
[9] J., Shahram Behzad Shahram. “A survey over black hole attack detection in mobile ad hoc network”. International Journal of Computer Science and Network Security (IJCSNS) 2015.15(3): 44.
[10] T. Tejasvi, N. Arora, and P. Vyas. “Literature Survey of MANET under Blackhole and Gray hole attack”. International Journal of Advanced Research in Computer and Communication Engineering. 2015, 4(9).
[11] T. Fan-Hsun, L. Chou, and H. Chao. “A survey of black hole attacks in wireless mobile ad hoc networks”. 2011 Human-centric Computing and Information Sciences 1(1): 4.
[12] Y. Bo, R. Yamamoto, and Y. Tanaka. “Historical evidence based trust management strategy against black hole attacks in MANET”. In Advanced Communication Technology (ICACT), 2012 14th International Conference on, pp. 394-399.
[13] R.Nandakumar, and K. Nirmala. “Security Challenges in Mobile Ad Hoc Network- A Servey”. Australian Journal of Basic and Applied Sciences2016, 10: 654-66.
[14] W. Bing, J. Chen, J. Wu, and M. Cardei. “A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless network security”, Springer US, 2007 pp. 103-135.
[15] L. Al-Dulaimi, Al, , B. Ahmad, and L. A. Hassnawi. “Black Hole Malicious Behaviour Via Different Detection Methods”.2016. 10(16):149-160.
[16] M Sergio, J. Thomas G. Kevin Lai, and M. Baker. “Mitigating routing misbehavior in mobile ad hoc networks”. In Proceedings of the 6th annual international conference on Mobile computing and networking. ACM,2000. pp. 255-265.
[17] V. Kamatchi, , and R. Mukesh. "Securing data from black hole attack using aodv routing for mobile ad hoc networks ". Advances in Computing and Information Technology. Springer Berlin Heidelberg, 2013pp :365-373.
[18] S. Casado, Leovigildo, R. A. Rodríguez-Gómez, R. Magán-Carrión, and G. Maciá-Fernández. "NETA: evaluating the effects of NETwork attacks. MANETs as a case study." In Advances in Security of Information and Communication Networks, Springer Berlin Heidelberg, 2013 pp. 1-10.
[19] P. Bhoomika, and K. Trivedi. Improving AODV “Routing Protocol against Black Hole Attack based on MANET”. IJCSIT) International Journal of Computer Science and Information Technologies .2014. 5(3): 3586-3589.
[20] S. Ranjeet, and S. Tamhankar. “Performance analysis and minimization of black hole attack in MANET”. International Journal of Engineering Research and Applications (IJERA),2012 ISSN: 2248-9622.
[21] C.Apoorva, and S. Thakur. “Performance evaluation of hybrid routing protocols against network layer attacks in MANET”. Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, pp. 239-244.
[22] S. Abdul-Rahman, and R. Hamamreh. “Efficient Mechanism For Mitigating Multiple Black Hole Attacks In Manets”. Journal of Theoretical and Applied Information Technology. 2016 83(1): 156.
[23] T. Navamani, and P. Yogesh. “Secure Efficient Routing against Packet Dropping Attacks in Wireless Mesh Networks”. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Springer International Publishing,2015. pp. 673-686 .