Behavioral and performance jellyfish attack

Layth A. Khalil Al Dulaimi[1] R.Badlishah Ahmad[2], Naimah Yaakob[3], Syadiah Nor Wan Shamsuddin[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 3, 2018
Revised Nov 13, 2018
Accepted Nov 26, 2018

Keywords:

AODV
Jellyfish attack
Security of Ad hoc networks

ABSTRACT

We provide a simulation-based study of the effects of jellyfish attacks on mobile ad hoc networks (MANETs). For this purpose we suggest a simulation based on the effects of jellyfish attacks on the network through a number of different scenarios. In particular, we examine how the number of attackers affects performance measures such as the ratio of packet delivery, throughput, and end-to-end delays. The results have enabled us to propose measures to reduce the effects of jellyfish attacks on MANETs.

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, Malaysia.
Email: Layth.a.khalil@gmail.com

1. INTRODUCTION

A dedicated mobile network is a network of mobile nodes that communicate with each other with the help of wireless links without any existing infrastructure or any central access point or base station [1].

A dedicated network is a wireless network in which the contract collaborates to form a set of nodes that do not require any communication and work infrastructure. It is a scalable, self-configuring network, and the quality of the mobile nodes of the network needed to configure it quickly expands without the need for specific or special infrastructure. MANETs may limit communications to a group so that each node must perform its work as the host, and the router also works and packets are sent to nodes that are not within the next direct transmission area in a multi-hop direction. Each node has full participation in the custom routing protocol with regard to effective sessions between nodes [2, 5].

These networks are particularly suitable in cases where infrastructure is unavailable or impossible to put into place because it is too expensive, weak or destructive [3].The quality of communication can change quickly over time or even disappear altogether. The nodes can look, disappear and come back again over time, and all the time network connections must work between the nodes that make it up. As one can no doubt imagine, these types of dynamic networks are weak and unimplemented. Because custom networks dynamically change the topology of a network and it opens up in the middle, there is no clear line of defense, and there is a lack of communication and centralized monitoring. Therefore, MANET also inherits the security threats they face in the case of wired and wireless networks, and offers security attacks that are unique to themselves [4]. The simulation and study of jellyfish attacks becomes necessary in order to provide defense against these types of attack.

2. JELLYFISH ATTACK

AODV is a routing protocol that is affected by jellyfish attacks. [6]A jellyfish attack is a kind of non-active attack that is difficult to identify in the light of the fact that the aggressor does not ignore any of the Protocol's rules. It is a kind of denial of service attack. An attacker changes the order of data packets or reduces traffic to a minimum or zero by dropping data packets. The first step to be taken by a jellyfish striker is to access the routing network and introduce a redirection package. It is like a Blackhole attack in the sense that in an attack on the Blackhole node the attacker drops the data packets, but in a jellyfish attack there is a delay before the packets are sent and then received from the packets in the grid. This only means that it is not the same as a Blackhole attack. The jellyfish attack is aimed at closed loop flows because these flows interact with network conditions such as packet loss and packet delay [7]. A jellyfish attack is specifically damaging to transfer control protocol traffic in that those cooperative nodes can hardly distinguish these attacks from network congestion. Figure 1 three ways of Jellyfish attack [7].

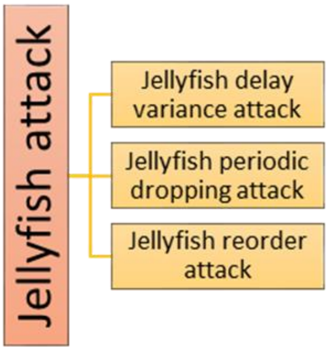
Jellyfish attack
Jellyfish delay variance attack
Jellyfish periodic dropping attack
Jellyfish reorder attack

Figure 1. Three ways of jellyfish attack

2.1. Jellyfish delay variance attack

In this type of attack, the request does not change the packets. Rather, the packets are delayed in a random way. The malicious node has to secure the routing paths and then all the packets are received by a previous redirection delay. We have tested this type of attack in order to study the effectiveness and impact of the network and the performance of the protocol under different circumstances, and under the influence of an attacker. We have tested this in the case of more than one attacker

2.2. Jellyfish periodic dropping attack

This is most commonly found in the relay nodes. Because of congestion, it is necessary for the node to drop packets periodically and the transition of the control protocol will decrease to zero.

2.3. Jellyfish reorder attack

In such an assault, the malicious node forward packets in the random order from the queue, resulting In zero good put, in its place of initial transmittal (first in first out). Packets can be placed in the arbitrary buffer instead of the first in first out buffer. It is rearranged by the Jellyfish node and packets are then sent from the buffer. In terms of the destination, after the packets do not arrive in accordance with the real demand, the acknowledgement frequency is sent to the source.

Therefore, if you repeat the receipt of three acknowledgements on the source side, the packet retransmissions are the beginning of a denial of waiting as far as the retransmission timeout is concerned. Even if the packet reaches its destination, the source still correctly accepts that the packet has been lost and may keep retransmitting the packet. A Jellyfish reorder attack is shown in Figure 2.

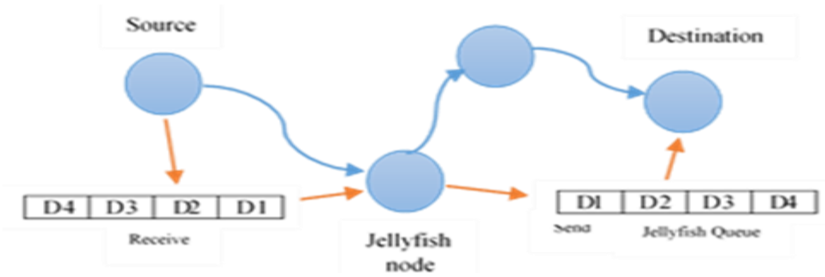

Figure 2. Jellyfish reorder attack

3. INVESTIGATING THE JELLYFISH ATTACK

The execution of a Jellyfish attack is tried on an ad hoc network. To be sure the execution is effectively working, we used the OMNeT++ in that it is one of the most commonly used simulation tools in the networking field. Additionally, the NETA framework is based on the same idea as OMNeT++ [9]. To test the implementation, we used three simulations. In the first situation, we did not use any Jellyfish AODV node. In the second situation, we added a single Jellyfish attack in the AODV node to the simulation. In the third situation, a cooperative Jellyfish attack in the AODV node was added to the simulation. At that point, we compared the outcomes of the simulations.

3.1. 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 [10].

To measure the outcomes from the simulations, the common parameters to all situations (scenarios) were defined. It generated 10 networks with 20, 40, 60, 80 and 100 nodes. The simulation area was limited to a 1000 m x 1000 m four-sided, with each node using a communication range of 250 m. The simulation time was set to 600 s. The results were derived from 50 simulation runs. AODV and 802.11g were selected as the routing and medium access control (MAC) layer protocols respectively, and the RTS/CTS mechanism was used to send packets. The number of attackers varied from one to three. The attacks were performed during the entire simulation time and the corresponding attack rate was set to 100%, where the attack rate was the probability of an attacker node triggering its attack. There was a constant bitrate (CBR) connection of four packets, where the packet payload size was 512 bytes. The movements randomly started between 0.5 and 1.5 s and they ended between 290 and 295 s. The minimum speed was set to 1 m/s and the maximum was set to between 5 to 20 m/s, with a pause time of 15 s. [8].

4. APPRAISAL OF RESULTS

Three diverse simulations were tested jellyfish delay variance attack. In the first, each node worked in collaboration with each other to guard the network in communication. The second simulation had one malicious node while the third had five malicious nodes that transmitted the Jellyfish attack.In this analysis, the results of these three simulations are compared to understand the network and node behaviors.

To start with, packet delivery ratio (PDR). As Table 1 shows, the PDR is almost 1 before the Jellyfish attack. This means that almost all the packets sent by the sender node are received by the receiver node, but for a network with a Jellyfish node, the PDR decreases due to increased retransmission timeout led by delay Introduced by attacker. This means that almost all of the packets sent by the sender node are delay by the jellyfish nodes.

Table 1. Packet Delivery Ratio Comparison

Number of nodes	No Jellyfish attack	One Jellyfish attack	Five Jellyfish attack
20	93.67762	90.03275	81.63087
40	92.71282	91.34945	89.62668
60	97.36575	98.04665	98.00649
80	85.58254	87.79698	76.02213
100	69.67809	74.54496	81.28284

Figure 3 is drawn from the data contained in Table 2. This compares the PDR before the Jellyfish attack and after one and five Jellyfish attacks, we notice nods behavior when the number of nodes becomes 60 because sparse network (is a network with less number of links than the maximum possible number of links within the same network): Figure 3 PDR.

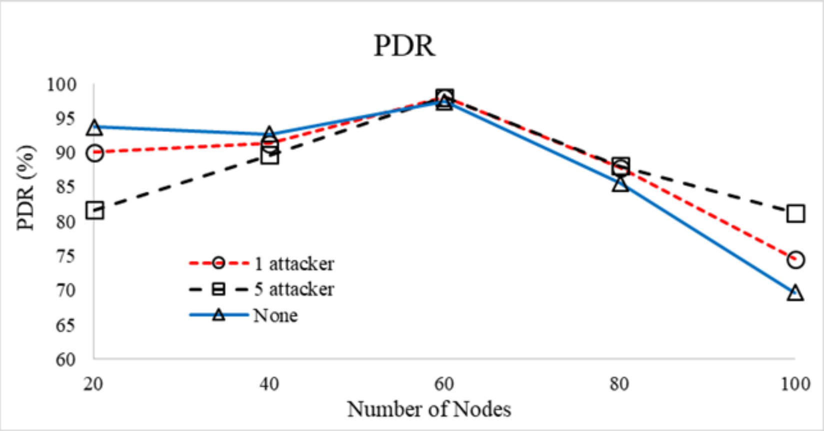

Figure 3. PDR

Table 2 shows the End-to-End Delay: End-to-End delay is the average time of the data packet to be successfully transmitted across a MANET from source to destination [11]. We can see an end-to-end delay increase in situations involving a Jellyfish attack. This is the result of delay packets when receiving packets by Jellyfish nodes, the reason for the delay increase is due to the attack node behavior.

Table 2. End-to-End Delay Comparison

Number of nodes	No Jellyfish attack	One Jellyfish attack	Five Jellyfish attack
20	0.003601	0.022125	0.004558
40	0.000627	0.002446	0.001067
60	0.005723	0.00929	0.006894
80	0.010548	0.014682	0.012038
100	0.014768	0.017243	0.016615

Figure 4 is drawn from Table 2's information. It compares the end-to-end delay before a Jellyfish attack and after one and five Jellyfish attacks:

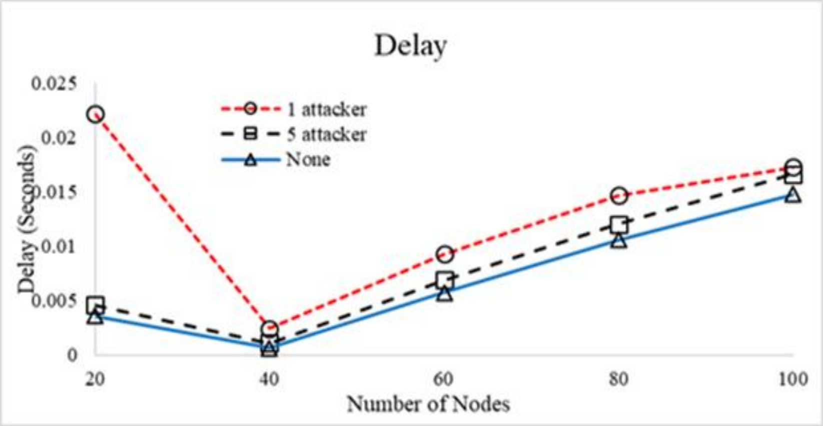

Figure 4. Delay

Table 3 shows the throughput for diverse situations (*The ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput*)[11]. Next, on entering Jellyfish nodes into the network routing request, the throughput decreases. This implies that after the Jellyfish attack, the number of data packets that are communicated is less than the number of control packets generated.

Table 3. Throughput Comparison

Number of nodes	No Jellyfish attack	One Jellyfish attack	Five Jellyfish attack
20	134357	129131.2	117080.1
40	308778.3	304871.4	299938.5
60	418781.9	421710.5	421537.1
80	490644.1	409664.9	451585.4
100	499438.3	336039.3	490775.3

Figure 5 is drawn from the data in the above table. This allows us to compare throughput before the Jellyfish attack and after one and five Jellyfish attacks:

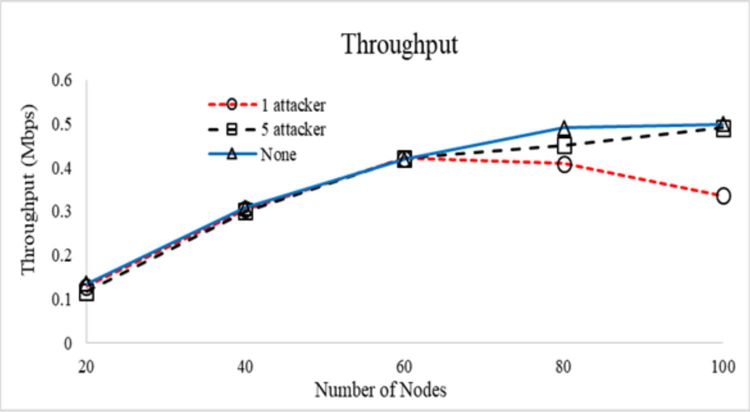

Figure 5. Throughput

5. CONCLUSION

In mobile ad hoc networks (MANET), nodes depend on each other to keep the network associated. In this manner, unlike customary wireless arrangements, such networks don't require any previous (settled) foundation. This limits their cost and sending time. Hence, security in a mobile ad-hoc network is the most imperative worry for the fundamental usefulness of the network. MANETs regularly experience the ill effects of security assaults in view of such elements as its open medium, changing its topology dynamically, the absence of focal observing and administration, helpful algorithms, and no reasonable defense mechanism. A jellyfish attack is a very important type of attack that has become of interest to many researchers.

Hence, in this work, we have analyzed the effect of Jellyfish attacks in an AODV network. For this reason, we have applied an AODV protocol that behaves as a Jellyfish attack using an OMNET++ simulator (4.2.2). We simulated 3 scenarios on 20, 40, 60, 80 and 100 nodes. The simulation was done using UDP packets. In each situation, we applied network performance before and after one Jellyfish attack and five Jellyfish attacks. We investigated the effects of the Jellyfish attacks on network performance jellyfish attack affects adversely throughput of network because of congestion caused due to retransmissions and PDR decreases due to increased retransmission timeout led by delay introduced by attacker. It increases end-to-end delay of the network. The effect is more devastating as number of jellyfish node increases. The performance degradation depends on the delay introduced by the jellyfish nodes.

REFERENCES

[1] N.Hoang Lan, and U. Trang Nguyen. A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks **6**(1): 32-46 (2008)..
[2] H. Lu. Wireless Ad-hoc Networks. Wireless personal Communication journal **4** (2004).

[3] M. Sergio, T. J. Giuli, K. 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, pp. 255-265 (2000).

[4] J. Apurva, and A. Shrotriya. Investigating the effects of black hole attack in MANET under shadowing model with different traffic conditions. In Computer, Communication and Control (IC4), 2015 International Conference on, pp. 1-6(2015).

[5] P. Nidhi, R. Sinha, and K. Maurya. Simulation study of Black hole and Jellyfish attack on MANET using NS3. In Engineering (NUiCONE), 2011 Nirma University International Conference on IEEE, pp. 1-5 (2011).

[6] G. Sakshi, and S. Chand. Enhanced AODV protocol for defence against JellyFish Attack on MANETs. In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference , pp. 2279-2284 (2014).

[7] Sachdeva, Sakshi, and Parneet Kaur. "Detection and analysis of Jellyfish attack in MANETs." In *Inventive Computation Technologies (ICICT), International Conference on*, vol. 2, pp. 1-5. IEEE, 2016.

[8] 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.

[9] 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 .

[10] K. Simranpreet, R. Kaur, and A. K. Verma. Jellyfish attack in MANETs: A review. In Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on, pp. 1-5 (2015).

[11] B, Tarunpreet, and A. K. Verma. "Performance Evaluation of AODV under Blackhole Attack." International Journal of Computer Network and Information Security 5, no.: 12, pp35 (2013).