ISSN: 0974-6471, Vol. 13, No. (2-3) 2020, Pg. 110-116

Oriental Journal of Computer Science and Technology

www.computerscijournal.org

Design and Efficient Network Investigation of Passive Periodic Drop Attack

SUNIL KUMAR[1] and MANINDER SINGH[2]

[1]Directorate of Livestock Farms, Guru Angad Dev Veterinary and Animal Sciences University, Ludhiana.
[2]Department of Computer Science, Punjabi University, Patiala.

Abstract

A Mobile Ad Hoc Network (MANET) is much more vulnerable to various security attacks due to its high mobility, multi-hop communication and the absence of centralized administration. In this paper, we investigate the impact of Jellyfish periodic dropping attack on MANETs under different routing protocols. This investigate is under the class of denial-of-service attack and targets closed loop flows which results in delay and data loss. In this paper, the simulation results are gathered using OPNET network simulator and its effect on network performance is studied by analysing re-transmission attempts, network load and throughput. The results have shown that the impact of Jellyfish periodic dropping attack which reduces the network performance. Performance shows OLSR performs better than AODV under periodic drop attack.

Article History

Received: 26 February 2021

Accepted: 24 March 2021

Keywords

Aodv; Jellyfish; Manet; Olsr; Periodic Drop.

Introduction to MANET

A Mobile Ad Hoc Network or MANET is referred to that there is no wired connection is released for the communication in the network because the nodes are mobile and set-up their paths dynamically in-order to transfer packets among themselves.[1] In a MANET, the area of network boundary; nodes can transfer the data directly to the specified node in the region of network but, if the communicating nodes are outside the range, then they have to depend on other nodes in order to forward messages. Therefore, MANETs have a multi-hop scenario and every node also works as a router.[2] Hence, various characteristics of MANETs include no wired structure, proactive topology creation, constraints for the resources and less security.Security is very essential issue these days, as a variety of different attacks can happen on MANETs.[3] Classified based on the following:

- Active or Passive attack
- Internal or External Attack
- Attacks on various layers

CONTACT Sunil Kumar sunilkapoorldh@gmail.com Directorate of Livestock Farms, Guru Angad Dev Veterinary and Animal Sciences University, Ludhiana.

Doi: http://dx.doi.org/10.13005/ojcst13.0203.08

Passive attack does not cause any harm to the network but it uses the important information and therefore, violates confidentiality.[7] Example of passive attack includes Jellyfish attack etc. On the other hand, Active attacks steal, destroy, modifies the important information and causes disruptions to the network operations. Active attacks include Black hole and Wormhole attacks.[4] External attacks are launched by opponents who are not authorized to join the network operations. The aim of these attacks is to create network congestions, denying an access to particular network service. These attacks are started by the external attackers.[5] Whereas, internal attacks are performed by the authorized nodes present inside the networks, and might start from either compromised or misbehaving nodes.[6] As per the stack presentation in network layers; various attacks classified as:

- Data Corruption attack and repudiation under the Application Layer.
- SYN flooding and session hijacking under the Transport Layer.
- Blackhole attack, wormhole attack and Byzantine attack under the Network layer
- Location Disclosure Attack and Resource Consumption under the Data Link Layer
- Traffic and Monitoring analysis, Disruption MAC (802.11) under Physical Layer

Formulation of this paper is to investigate the effects of Jellyfish periodic dropping attack on the performance of MANETs using routing protocols i.e. AODV and OLSR.Further the paper described as: section 2 includes the work done by various researchers on this topic. Jellyfish periodic dropping attack is explained in section 3 and section 4 includes the experimental setup and analysis of simulation results using OPNET simulator, which is followed by conclusion and future scope in Section 5.

Literature Review

In this section we are going to explore related work done in the area of Jellyfish attack. Wazid *et al*.[8] have evaluated the performance of MANET using reactive routing protocols such as DSR, AODV and TORA, under JF delay variance attack. According to authors TORA has shown high throughput as compared to other protocols. Wazid *et al*.[9] have observed that if the Jellyfish attackers are less than 10% then throughput reduces only 0.03%, but if the attackers are increased to 20% the throughput would reduce up to 7.58%. Therefore, they concluded that the performance of network degrades less when up to 10% JF attackers are present and becomes worse if JF attackers are increased to 20%. Patel *et al*.[10] gave a new approach for guarding the MANETs against JF reordering attacks. The new model has used the time space cryptography technique and enhanced hash function for authentication. The experimental results have shown that the new technique has increased network performance.

S. Garg *et al*.[11] explained the improved version of AODV protocol for creating a defense method against JF attacks. They have also used MAC addresses to find the routes in order to send packets to the destination. The attacker did try to delay the packets and tried to reduce the network performance. But they have also proposed an improved version of AODV routing protocol, in order to find out and eliminate the malignant node. Zalte *et al*.[12] gave an efficient solution to secure packets by introducing digital signatures which are based on symmetric cryptography by using AES algorithm secure hash function (SHA2). The nodes fails to perform any communication in the network if they are not using digital signatures, and able to control access control, spoofing, and non-repudiation.

Jellyfish Periodic Dropping Attack

Jellyfish periodic dropping is a kind of denial of service attack,[9] which disturbs the entire working of MANET-TCP. It reduces the network throughput and increases the network load by deliberately dropping some of the data packets.[6] In TCP, after successfully processing of each packet the sender sends back the acknowledgement (ACK) because TCP is reliable protocol. Due These ACK packets should reach the source node in time but gets delayed due to periodic dropping attack, which makes the source assume that packet is destroyed. Therefore, the source node re-transmits the same packet again and due to this retransmission of data packets the congestion occurs in the network and TCP becomes worst. In jellyfish periodic drop attack, the attacker nodes drop the packets for a small time of duration once per retransmission time out. Jellyfish node drops the data only a short duration of time during transmission process.[6] Due to the congestion in the network, a node is forced to drop packets from the network and if the node drops packets from

the network periodically then in results TCP will reduce the throughput to zero.[6] With the effect of periodically dropping the data with a small fraction of packets which reduce the good put of all visited closed loops flows.

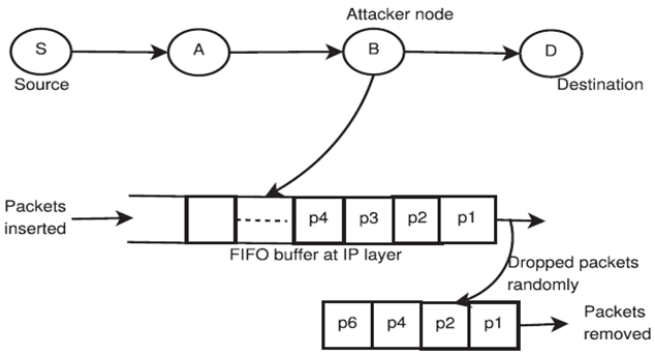

Fig. 1 Jellyfish Periodic dropping attack

The attacker node may choose to banish a piece of packets for example, dropping of 100 packets from every 1000 packets or may banish all the packets received during a period of time. Due to this process, it increases its RTO value and process of the retransmission timeout of TCP.[6] The sender will ultimately enter in the arena of timeout when attacker node starts remove packets for some duration. This leads to increases the network load and decrease throughput of the network. Frequency of dropping packets increases due to the attacker nodes which decreases the throughput of the network. Jellyfish attacker node drop packets as soon as the TCP sender exits its slow start phase which maximize the impact of attack. The process will always be in a frail slow-start state. An illustration outlined in the attack is shown in Fig. 1.

Table 1: MANET Environment Settings

Attributes	Values
Simulator	Opnet Modeler 14.5
Campus Size	12*12 KM
Network Nodes	40 Nodes
Frame Inter arrival Time	10 Frames/Sec
Frame Size in bytes	128*120 pixels
Mobility Model Type	Random waypoint
Traffic Type	Voice Traffic (PCM Quality)
Simulation Duration	10 Minutes
Addressing Type	IPv4
Ad-Hoc Routing Protocols	OLSR and AODV
Periodic Jelly Fish Scenario	Four Scenarios
Packet Size	1024
Frame Interval Time Information	10 frames/sec

Experimental Setup

In order to study the impact of Jelly Fish periodic dropping attack in MANET, experiments are conducted in network simulator OPNET using MANET routing protocols (OLSR and AODV).[13-15] Selection of JF attacker nodes, mobility speed of each node and visibility area and other parameters have been specified. In this research, total four simulation scenarios have been considered depending on the type of data flow (normal or under passive periodic drop attack), type of routing protocol (AODV or OLSR) and number of MANET nodes. For example, one simulation scenario is MANET with 50 nodes is under periodic drop attack and uses OLSR for routing. The nodes were randomly placed within certain gap from each other in 12 x 12 km

campus environment. Voice traffic with PCM quality is generated in the MANET network via mobile application configuration node. All the experimental parameters are configured according to Table 1.

Results And Explanation

In this section, we are going to briefly explain the experiments that illustrates the effects of Jellyfish periodic dropping attack based network metrics i.e. through put, retransmission and network load.

Retransmission

For obtain high reliability the retransmissions are mandatory. In Fig. 5 and 6, the combination of reliability and blacklisting metric are sufficient to achieve high path reliability with a small number of retransmission. When there are mobile nodes which behave as an attacker node in the network then packets will take time to reach the destination. This affects the performance of the network. From the results, AODV with periodic attack does don't spread the attackers in the network in the starting of the simulation but in the end of simulation it shows the effect and degrade the performance of the network. In OLSR, don't make any large effect on the network. JF attack increases the retransmission attempts due to loss of packets both cases (AODV and OLSR) as shown in Table 2 and Fig. 2-3.

Table 2: Retransmission of Packets

	AODV	OLSR
Normal Flow	0.78	1.07
JF Attack	0.82	1.09

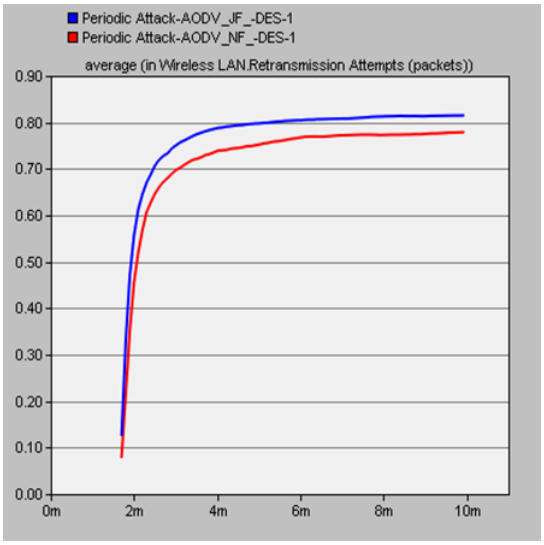

Fig. 2: Retransmission of AODV

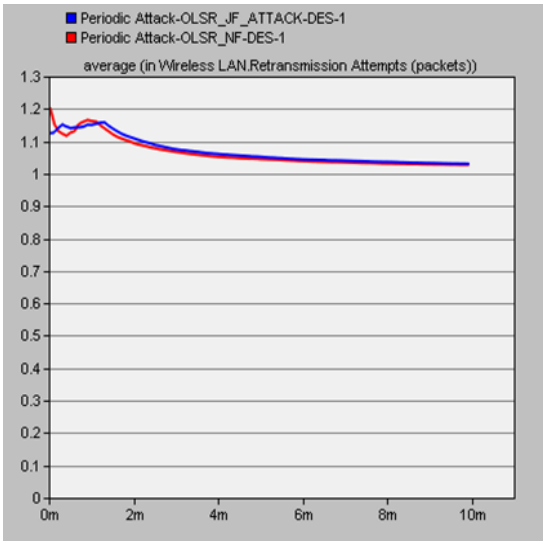

Fig. 2: Retransmission of AODV

Throughput

As simulation process, the function of dropping period shows that throughput in the action of degradation is highly non-linear. According to the result, slow time scale congestion avoidance procedure of TCP exploiting by the attacker node(s), which flows must infer that multiple packet losses within round trip time are an indication of serve congestion. Here the data dropped by malignant node rather than forwarding it to the ending node, which affects the network throughput. Acknowledgement is received after some delay; next packet is dropped by the attacker which reduces the throughput of the network. Same function is occurred in the performance of OLSR. Finally, the degradation in throughput due to the periodic attack which changes the scenario of whole network (Table 3 and Figs. 7–8).

Table 3: Throughput

	AODV	OLSR
Normal Flow	72,50000	44,8000
JF Attack	60,25000	41,7500

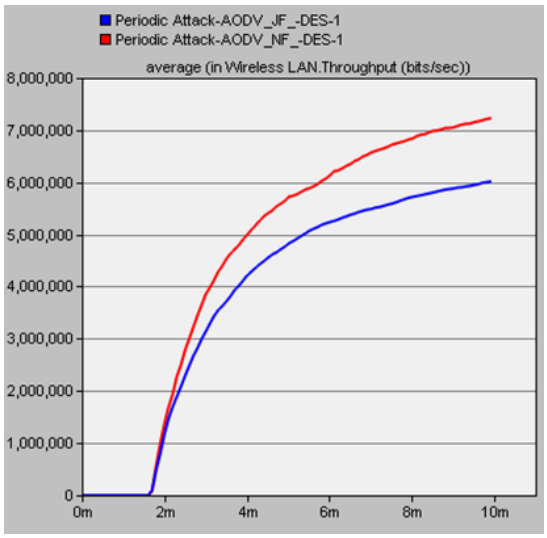

Fig. 4: Throughput of AODV

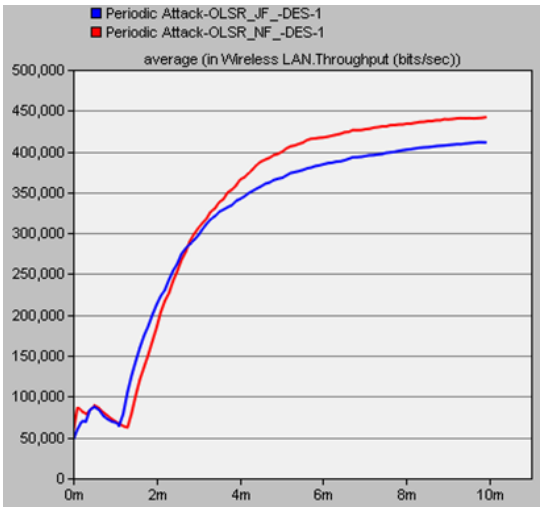

Fig. 5: Throughput of OLSR

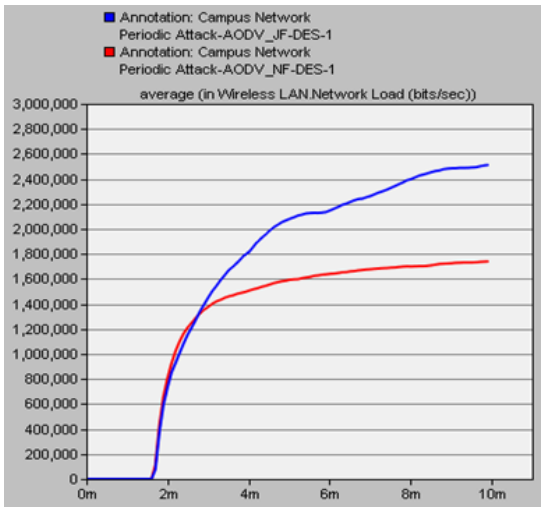

Fig. 6: Load of AODV

Table 4: Load (bits/sec)

	AODV	OLSR
Normal Flow	17,50000	23,90000
JF Attack	25,49000	27,00000

Load

The effect of attacker nodes on the network load metrics when varying node mobility during the communication process. It can be observed that Maximum RRP generated due to the flooding attack, which generates the high network load in the network. Delay keeps increasing due to more traffic load in the network which creates network congestion and stay more time in queuing buffer for the packets to be transmitted. This condition leads to longer delay in heavy load situation. (Table 4 and Figs. 9–10).

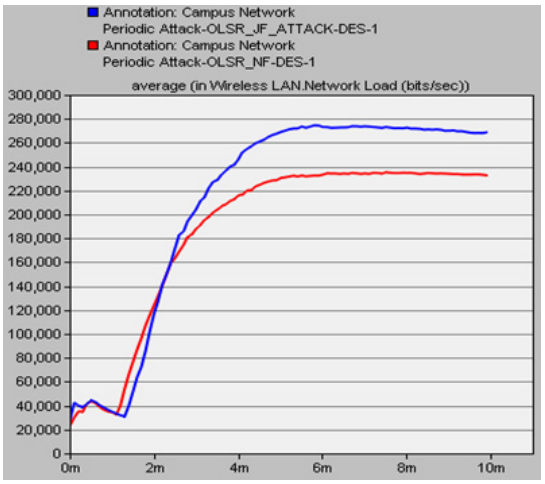

Fig. 7: Load of OLSR

As per results, AODV has a maximum load due to traffic. OLSR uses traffic conditions so have least load. This happen simply because of nodes has randomly mobility function. In link state, there is a frequent change and this result, due to mobility there is change in MPR node(s).

Conclusion and Future Scope

In the paper, we have evaluated the performance of Jellyfish periodic dropping attack over TCP-MANET. Experimental results arecollected over the different network scenarios with varying number of attacker nodes, intermediate adjoiningnodes and other attack attributes.The experimental results have proved the degradation of network throughput, with increase retransmission and network load and this all is happening due to the occurrence of Jellyfish periodic dropping attack. JF Periodic dropping attack is protocol-compliant and has a destructive strike on the throughput of closed-loops flows. Overall JF periodic dropping attack affect the overall administration of network.Finally, the result goes in the favor of OLSR; because degradation of network performance using OLSR is lessas compared to AODV under the periodic drop attack. In future, anefficient Jellyfish attack detection and prevention mechanismneed to be devised, which will be more secure and reliable.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of Interest

The authors do not have any conflict of interest.

References

1. Weerasinghe, H., Fu, H. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation, Future Generation Communication and Networking, vol. 2, pp. 362- 367, 2007.
2. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L. Security in mobile ad hoc networks: challenges and solutions, IEEE Wireless Communications, vol.2, pp. 38-47, 2004..
3. Chlamtac, I., Conti, M., Liu, J.Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks,vol 1, pp. 13-64, 2003.
4. Tamilselvan, L., Sankaranarayanan, V. Prevention of Black hole Attack in MANET, IEEE International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-21, 2007
5. Kurosawa, S., Jamalipour, A.Detecting black hole attacks on AODV based mobile adhoc networks by dynamic learning method, *International Journal of Network Security*, vol 5(3),pp. 338–346, 2007.
6. Laxmi, V., Mehta, D., Gaur, M., Faruki, P.,Lal, C. Impact analysis of Jellyfish attack on TCP-based mobile ad-hoc networks, 6th *International Conference on Security of Information and Networks*, pp.189-195, 2013.
7. Wu, B., Chen, J., Wu, J., Cardei,M. A survey of attacks and countermeasures in mobile ad hoc networks In Wireless Network Security, Springer US, pp. 103-135, 2007.
8. Wazid, M., Kumar, V., Goudar, R.Comparative performance analysis of routing protocols in mobile ad-hoc network under Jelly fish attack, IEEE International Conference on parallel, distributed and grid computing, 2012.
9. Wazid, M., Singh, R., Goudar, R. Measuring the Impact of JellyFish Attack on the Performance of Mobile Ad Hoc Networks using AODV Protocol, International Conference on Computational Intelligence and Information Technology, CIIT, 2012.
10. Patel, H.,Chaudhar, M.A time space cryptography hashing solution for prevention Jellyfish Reordering attack in wireless ad hoc networks, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-6, 2013.
11. Garg, S.,Chand, S. Enhanced AODV protocol for defense against Jellyfish Attack on MANETs, IEEE Advances in Computing, Communications and Informatics ICACCI,pp. 2279-2284, 2014.
12. Zalte, S., Ghorpade, V.Secure Token for Secure Routing of Packet in MANET", *International Journal of Computer Science and Information Technologies (*IJCSIT), vol. 5 (6), pp. 6916-6919, 2014.
13. Perkins, C., Belding-Royer, E.,Das, S.Ad-hoc On-Demand Distance Vector (AODV) Routing, *Internet experimental RFC* 3561, pp.7-24, 2003.
14. Haerri, J., Filali, F., Bonnet, C.Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns, 5th IFIP Mediterranean Ad-Hoc

Networking Workshop, ITALY, pp. 14-17, 2006.
15. Kumar, S.,Sengupta, J. AODV and OLSR Routing Protocols for Wireless Ad-hoc and Mesh Networks, IEEE International Conference on Computer and Communication Technology (ICCCT), pp. 402-407, 2010.