World Wide Journal of Multidisciplinary Research and Development

World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(6): 88-91
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Sukhpal kaur
Guru Kashi University,
Bathinda, Punjab, India

Dr. Rajinder singh
Assistant professor
Guru Kashi University,
Bathinda, Punjab, India

Correspondence:
Sukhpal kaur
Guru Kashi University,
Bathinda, Punjab, India

Detection and prevention of JFPD attack in MANETS Using NBA technique

Sukhpal kaur, Dr. Rajinder singh

Abstract
In mobile ad hoc networks, the nodes communicate with each other wirelessly and they are also not under the control of any centralized infrastructure. This unattended nature makes the wireless links and the nodes susceptible to various security concerns. Out of many well-known attacks such as black hole attack, wormhole attack, flooding attack; jellyfish attack is one of lesser explored attacks. The jellyfish attack has been defined with three variants, namely jellyfish delay variance attack, jellyfish packet dropping attack and jellyfish reordering attack. This paper considers detection and prevention scheme for jellyfish packet dropping attack by analyzing the behavior of the nodes. If any node is found to drop packets abnormally greater than threshold value, it is detected as malicious node. The scheme has been simulated in NS2.35. The performance has been compared with AODV under attack and proposed scheme on the basis of packet delivery ratio, throughput and packet drops.

Keywords: MANETs, Jellyfish, AODV, delay variance

Introduction
Mobile Ad-Hoc Networks goes under Wireless Networks. Wireless networks are getting outstanding on account of their comfort. Client is not any more subject to wires where he/she is, anything but difficult to move and value being associated with the network. One of the mind-blowing attributes of wireless network that makes it entrancing and extraordinary among the traditional wired networks is portability. This trademark gives customer the ability to move uninhibitedly, while being connected with the network. Wireless networks are generally simple to introduce than wired networks. There is nothing to stress over the foundation of the equipment costs. Wireless networks could be composed predictable with the need of the customers. These can keep running from minimal number of customers to generous full establishment networks where the measure of customers is in thousands.
Mobile Ad-Hoc Networks are autonomous and decentralized wireless frameworks. MANETs include mobile nodes that are allowed to move done in the network. Nodes are the gadgets that are mobile and that take an interest in the networks, for example, mobile telephone, portable PC, individual computerized help, MP3 player and PC.
In mobile ad hoc networks, the nodes communicate with each other wirelessly and they are also not under the control of any centralized infrastructure. This unattended nature makes the wireless links and the nodes susceptible to various security concerns. Out of many well-known attacks such as black hole attack, wormhole attack, flooding attack; jellyfish attack is one of lesser explored attacks. The jellyfish attack has been defined with three variants, namely jellyfish delay variance attack, jellyfish packet dropping attack and jellyfish reordering attack. This paper considers detection and prevention scheme for jellyfish packet dropping attack.

Literature Survey
Preety Dahiya et. al, [2016]This paper [1] modifies the existing TCP and AODV system to handle the jelly fish periodic dropping attack, the jellyfish packet reordering attack and the jelly fish delay variance attack. The proposed system modifies the AODV routing protocol and TCP to handle the jelly fish attack variants. The proposed system uses the E_TCP of the existing system along with the modified AODV routing to get the effective results. In the E_TCP protocol the buffer stores the sequence number and the acknowledgement time while in the NAODV_ETCP protocol the fr (forwarding ratio) is also stored in buffer. This paper

analyzes the performance using PDR, E2Edelay and the throughput on the various scenario attacked by different types of jellyfish attack. The result analysis shows that the performance of NAODV_ETCP is better.

Manjotkaur et. al., [2014] The advancement in Wireless Communication have given arise to various Wireless Networks like Mobile Adhoc Networks (MANETS), Wireless Sensor Networks and many more. MANET networks are vulnerable to various types of attacks and threats due to its unique characteristics like dynamic topology, shared physical medium, distributed operations and many more. There are many attacks, which effect the functioning of MANETS' such as denial of service, which is most commonly used to affect the network, is one of the types of attacks in MANETS. Jellyfish attack has gained its name recently in attack scenario in Mobile Ad hoc networks. JellyFish Attack exploits the end-to-end congestion control mechanism of Transmission Control Protocol (TCP) [2].

Choukri, A. et. al., [2014] describes a routing framework for a correspondence network constituted by a few ad hoc mobile nodes. This framework optimizes energy consumption. It isolates the network into groups. From that point, it recognizes the ideal path in terms of energy. This comprises to figure the energy required for each accessible way and select the ideal passages. Every group is distinguished by a cluster head, which is chosen according to its position and its remaining energy by using a clustering calculation. The main goal of this paper is to upgrade the quantity of live nodes by assigning to every network task the suitable nodes [3].

Abhilasha et. al., [2014] tries to limit the quantity of route requests (RREQs), that is a important source of overhead for the DSR. They adjusted DSR calculation to upgrade its execution. In the altered DSR i.e. Portable internetwork communicate; framework procedure (MIKBIT) multicasting strategy is utilized to diminish packet overheads. The execution parameters like throughput, normal end-to-end delay, normal jitter and packet delivery proportion are computed for the proposed calculation and contrasted and that of existing DSR routing protocol [4].

Mr. Hepikumar R. Khirasariya [2013] said that Mobile ad hoc network (MANETs) are very helpless as there is no nearness of trusted brought together specialist and dynamic system topology. Various senders and recipients can act at a same time in MANET and correspondence is hop by hop through halfway node. Because of such attributes of MANET different sort of attacks are conceivable. Attack in MANET might be active or passive. Jellyfish attack is a sort of DOS (Denial of service) attack in which attackers or noxious nodes attempt to build packet end-to-end defer and delay jitter. Before applying attack jellyfish attacker first access the routing cluster in portable ad hoc organize. This can be conceivable by performing rushing attack. As per change in number of senders, recipients and attack position situations will get change in jellyfish attack. As attacker get hold of sending packets, they begin postponing or dropping information packets for certain measure of time before sending them regularly [5].

Ekta Barkhodia, Parulpreet Singh and Gurleen kaur Walia [2012] have used the 40-node set-up with AODV protocol and explained that as the nodes increases the average end-to-end delay increases but throughput increases as the no. of attacker nodes increases. In the presence of third attacker node is the highest [6].

Harmanpreet Kaur and Er. Jaswinder Singh [2012] has compared three protocols OLSR, GRP and TORA based on delay, load, media access delay and throughput in their research. They have concluded that OLSR performs best in terms of throughput, GRP performs best in terms of delay and routing overhead, TORA is worst choice when we consider all four parameters [7].

Ekta Nehra and Er. Jasvir Singh[2012] in this paper routing protocols AODV, TODV, OLSR and ABR are compared using the various parameters i.e. delay, Network load and throughput. They have concluded that OLSR performs best in terms of network load, throughput, AODV performs worst in case of Load, throughput, Performance of ABR is good for load and throughput, and AODV, s performance is consistent for all three parameters [28].

Proposed Work

When source node has to send data to destination, it will look out for the route to the destination node in the network using the broadcasting process.The normal nodes upon reception of the RREQ packet tend to look out the destination in their routing table. If the address is not found the nodes increase the hop count by 1 and re-broadcast, it to their neighbors.On the contrary, the malicious node would not increase the hop count while forwarding the RREQ packet.

Now when the source node would receive the Route Reply, the hop count of the path containing jellyfish attacker would be less and source node will select this path.When the source node would send data to the destination over the path, the malicious node would drop the packets upon receiving them.

In order to detect and prevent such abnormal behavior, the proposed scheme aims to work in the following way. When the source node receives the route replies, it will store all the paths in its cache memory.Before sending all of the packets at once, it will divide the total number of packets into 3 parts, and will send one block over each path. Thus, data will now be being sent to the destination node over three paths.

When the destination node will receive the packets, it will compare the number of received packets with the threshold value where the threshold value will be set at 80 percent to the number of packets sent.If for any path, the packet delivery rate is found to go below the threshold value, and then over that path, destination node will start the detection procedure in which each node will be asked for the number of packets received and forwarded by it.If again packet delivery rate of a particular node tends to drop below the threshold value, then that particular node will be detected as malicious.ID of the suspected node will be broadcasted to all the nodes in the paths to prevent communication with it.

Results

The proposed and the existing schemes were implemented in NS2.35. The performance of the network was analyzed based on three parameters namely packet delivery ratio, throughput and packet drops in the network.The various simulation parameters used in the simulation of the proposed scheme has been described below:

Parameter	Value
Channel	Wireless
Mac	802.11
Propagation Model	Two Ray Ground
Routing Protocol	AODV
Number of nodes	45
Queue	Drop Tail
Antenna	Omni Directional
Initial Energy	70
Network Area	1000 * 1000 sq. meters

Table 1: Simulation Parameters

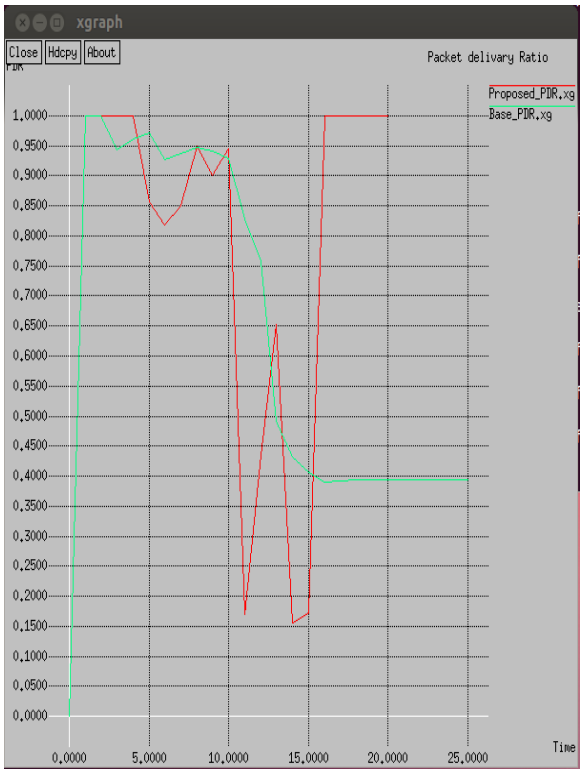

Fig. 1: Comparison of PDR

The above graph shows the comparison of the packet delivery ratio for the AODV protocol under the effect of the jellyfish packet dropping attack (shown in the green line) and the proposed scheme (shown in red line). The value for the packet delivery ratio rises once the attacker node has been detected successfully in the network.

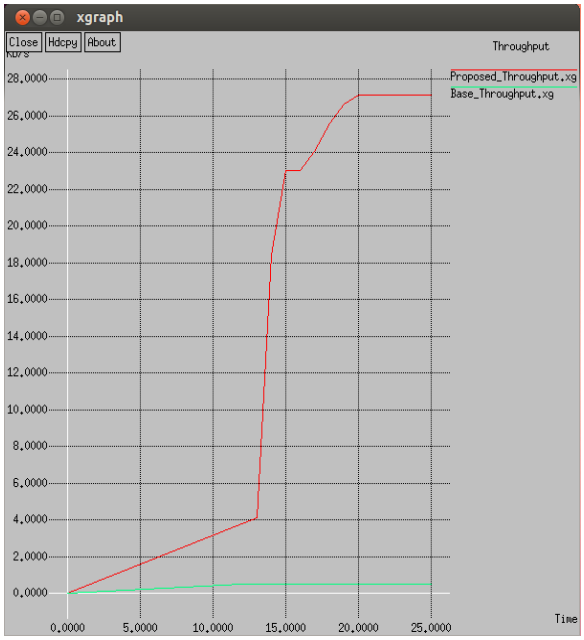

Fig. 2: Throughput comparison

The throughput is the amount of data received at the destination node per unit of time. Since AODV lacks any security measure so the throughput is almost negligible under the effect of the attack.

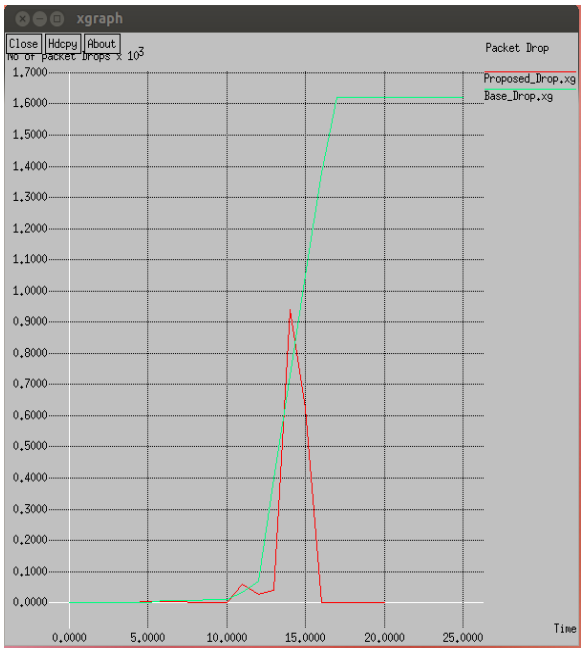

Fig. 3: Packet Drops Comparison

The packet drops rise to a certain level in the proposed scheme but when the attacker free path is chosen to forward the data, the packet drops reduces to zero level.

Conclusion

The proposed scheme aims at the detection and prevention of the Jellyfish packet dropping attack in the AODV routing protocol of mobile ad hoc network. Traditional AODV routing protocol lacks any security measure so any kind of attack or malicious activity becomes successful. The performance of the network was analyzed on the basis of throughput, packet delivery ratio and number of packet drops. The detection is done by checking on the packet

delivery ratio of the paths and then consequently of the nodes. Once the malicious node is found, the source node starts communication over the new path in which attacker is not present. Therefore, that leads to increase in the levels of the above said parameters. Thus, it can be fairly concluded the proposed scheme is successful in detection of the Jellyfish packet dropping attack.

In future, the work can be done for the detection of the third kind of the Jellyfish attack i.e. Jellyfish reordering attack. In addition, other parameters such as delay and energy consumption of the network can also be analyzed in the future.

References

1. Preety Dahiya, Miss Bhawana, "Design and Implementation of NAODV ETCP to Handle Jelly Fish Attack" in International Journal of Engineering and Computer Science May 2016.
2. Manjot Kaur, MaltiSarangal and AnandNayyar, "Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc "in International Journal of Computer Trends and Technology Sep 2014.
3. Choukri, A. Habbani and M. El Koutbi, "An energy efficient clustering algorithm for MANETs,"2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2014, pp. 819-824.
4. Abhilasha Gupta, Raksha Upadhyay, Uma Rathore Bhatt,"Modified DSR for MANET" in IEEE 2014.
5. Mr. Hepikumar R. Khirasariya, "Simulation Study of Jellyfish Attack in MANET (Mobile Ad Hoc Network) Using Ad hoc Routing Protocol", Journal of Information, Knowledge and Research in Computer Engineering October 2013.
6. Ekta Barkhodia; Parulpreet Singh; Gurleen Kaur Walia, "Performance analysis of AODV Using HTTP traffic under Black Hole attack in MANET". CSEIJ, Vol 2 June 2012.
7. Harmanpreet kaur, Er. Jaswinder Singh, "Performance comparison of OLSR, GRP, and TORA Using OPNET", International Journal of Advanced Research in Computer Science and Software engineering, Vol 2, Issue 10, Oct-2012.
8. Ekta Nehra, Er. Jasvir singh, "Performance Comparison of AODV, TODV, OLSR, ABR Using OPNET", International Journal of Advanced Research in Computer Science and Software engineering, Vol 3, Issue 5, May 2013.