Impact of Jelly Fish Attack on the Performance of DSR Routing Protocol in MANETs

Muhammad Sajjad¹, Khalid Saeed², Tariq Hussain³, Arbab Waseem Abbas⁴, Irshad Khalil⁵, Iqtidar Ali⁶, Nida Gul⁷

¹,³,⁴,⁶,⁷ Department of Computer Science & IT IBMS, The University of Agriculture Peshawar, Pakistan
² Department of Computer Science, Shaheed Benazir Bhutto University Sheringal, Pakistan
⁵ Department of Computer Science & IT, University of Malakand, Dir Lower, Pakistan

Corresponding Author: Khalid Saeed
Email: khalidsaeed102@gmail.com

https://doi.org/10.26782/jmcms.2019.08.00012

Abstract

Mobile Ad-hoc Networks (MANETs) could be setup frequently without the need of pre-established infrastructure. The nodes in MANETs are free to move and they can join as well as leave the network. Due to the dynamic nature of nodes in MANETs, routing protocols in MANET are extremely vulnerable to different security attacks. Like other different security attacks, Jellyfish attack is one of the most dangerous attacks in MANETs environment and it degrades the overall performance. In such type of attack, the packets reached its destination but take more time and hence it is difficult to detect such attack. In this research paper, we have analyzed the performance of Dynamic Source Routing (DSR) routing protocol in the presence of Jellyfish attack. To evaluate the performance we have created different scenarios having various number of Jellyfish attacks in MANETs environment. From the simulation result, it has been observed that Jellyfish attack significantly degrades the performance of DSR protocol in terms of end to end delay, throughput and packet delivery ratio. Moreover it has also been observed that when the number of Jellyfish attacks increases in the network then the performance is further degraded. In this research OPNET Modeler 14.5 simulator has been used in order to assess the performance of Jellyfish attack in MANETs environment.

Keywords: Mobile Ad-Hoc Networks, Dynamic Source Routing, Jellyfish Attack, Security Issues.

I. Introduction

MANETs consists of the wireless mobile host, having no central infrastructure station for communications with each other. A node can be moving...
freely within the network communication boundary. In MANETs, each individual node communicates with each other, using packet forwarding through a multiple-hop link. Nodes act as a router and forward its received packet to another communicating node. Due to the dynamic behavior of nodes, routing in MANETs is always a challenging task.[VI].

The malicious attacker can easily access the network as there is no centralized authority for security and high nodes mobility. Comparing with other networks, the MANETs also lack of trust among the mobile nodes, convenient eavesdropping due to the fact of the shared wireless medium, battery and memory issues of mobile and low bandwidth. Among the other network issues, security is the most essential need in MANET senvironment [I]. Dynamic routing protocols are important in the environment of MANETs to function correctly as these have high mobility of nodal, multipath propagation, interference, and path loss. Routing protocols in MANETs can be divided into three categories such as proactive, reactive and hybrid routing protocols.

The routing protocols in proactive category are also called table-driven routing protocols. In such type of routing protocol technique that updates every network node manages and their tables, the network topology alters because of the node’s movement in the network. The nodes can interchange information among each other. These nodes possess the route information at any time when the network needs it [VI]. OLSR and DSDV are the example of the proactive category of routing protocols in MANETs.

In reactive routing protocols as in DSR, routing information is maintained whenever this information is required. The routing protocol does not begin the routes discovery by itself unless it has been requested. Each mobile node in this protocol manages the data information of the active paths. Because of dynamic topology and mobility can alter the active routes and can lead to the route search [IX].

The hybrid category of routing protocols the positive aspects of both the reactive and proactive routing protocols are utilized for improving overall performance in the MANETs environment. In hybrid protocols, the network is partitioned into multiple grids, using multiple protocols at these different grids. Zone Routing Protocol is a routing protocol which belongs to the hybrid category of protocols in MANETs.

A. DSR Routing Protocol

The DSR (Dynamic Source Routing) is a unique and simple but robust protocol estimated to utilize in the ad-hoc networks. Multiple optimizations have been proposed in the current protocol leads to affect the network performance, particularly in that case of mobility of high node and also the lower traffic. The DSR has been used a lot around the world in the case of MANETs. Some of the previous studies suggested that a few routing methods and the optimizations has been projected in the base protocol which affect the performance in different cases and it leads to underperform the DSR. Second most using routing protocol is the AODV. Due to the fact of source routing, the DSR has been considered to be the most favorite
from the security perspective. Majority of the studies showed that the advantage of the turning off a few ‘optimization’ characteristics of the DSR system to enhance the performance of the network. Every node of the network manages the routing cache which leads to caches the routes which it maintained[X].

B. Jelly Fish Attack

This attack is a sort of DOS attack in which the system assailants or the nodes of malicious system attempts to enlarge the end to end delay of the packets as well as the delay jitter. Prior to the usage of the attack, the Jellyfish aggressor ways to deal with the routing group in the MANETs. This can be achieved because of the usage of rushing attack. As per the change in the amount of recipients, senders and the attacker position cases will be altered in the attacksuch as Jellyfish. As the system attacker keep hold of the forwarding packets of system, the aggressors have a go at deferring or disposing of the information packets for the particular amount of time before transmitting them typically[V].

The rest of research paper is structured as follows: First section is regarding introductory overview of the DSR routing protocol and Jellyfish attack. Section II contains the literature review, the details regarding simulation are discussed in section III, results are discussed in section IV, section V includes conclusion and future work, at the end there are references.

II. Literature Review

Research conducted in [II] investigated the influence of Jellyfish attackon AODV routing protocol in MANETs environment. The three scenarios having 20, 40, 60, 80 and 100 nodes are simulated. They investigated the increase in networks end-to-end delay. The outcome is more shocking as several Jellyfish node rises. The degradation in the performance influenced by the delay is due to the Jellyfish nodes.

Researchers in [IV] proposed a new technique for combating and detecting Jellyfish attacks in MANETs known as the Accurate Detection and Prevention of Jellyfish Attacks Detection (APD-JFAD). MANET sare exposed to a large number or amount of diverse attacks, everyone with diverse results and behavior. The Jellyfish attacks are considered as the difficult one attack to identify and it worsens the performance of overall networks. APD-JFAD, hierarchical trust appraisal is carryout so the nodes which are trusted are selected for the construction of route path.

According to the research conducted in [VII] MANETs have turned into a vital part of innovation progressions because of it’s functioning as self-ruling network system. MANETs are helpless against different sorts of attacks and dangers because of its exceptional attributes like element topology, physical medium which is shared, appropriate operations and some other. There are numerous attacks which impact the working of MANETS, for example, refusal of administration which is regularly utilized to influence the system is one of the sorts of attacks in MANETs. The Jellyfish attack has picked up its name as of late in attack situation in Mobile Ad-hoc arranges. The Jellyfish Attack abuses the end to end blockage control system of TCP.
The research conducted in [I] proposed a safe system in TORA protocol utilizing a hub interest path to deal with decrease the effect of Jellyfish attack in MANETs. The specific hub interest approach distinguishes JF hubs amid course creation and doled out it as an idle and chooses a subset of hubs to take an interest as a feature of the system. MANETs are exceedingly helpless as there is no nearness of trusted incorporated power and element network topology. Because of such attributes of MANETs different sort of attacks are conceivable. Jellyfish is another refusal of administration attack. The proposed work is a system that will improve the effect of Jellyfish attack in MANETs by particular hub support approach.

i. The status of the network node variable keeps in the nodes so that it reflects the participation of the nodes in the network.

ii. The tool i.e. probability active constant can estimate the active status of the node in the network.

Authors in [III] showed a mobile path to manage identifying gray and black hole attacks in ad-hoc networks system considering a cross-layer outline. Gray and black hole attacks are sort of routing aggravating attacks and convey extraordinary harm to the system. Subsequently, an effective algorithm to recognize gray and black attack is vital. In networks system layer this proposed a path-based technique to catch the following hop’s activity. Their experimental result checks their hypothesis: the normal identification rate is exceeding 90% whereas the false positive rate is underneath 10%. The simulation comes about to uncover that attacks with gray above 60% would realize significant harm to the system.

According to researchers in [VIII] a group from IETF is working on the improvement of a few routing protocols for MANETs. Be that as it may, the execution of each routing protocol is not the same as each other in various situations i.e. are autonomous to meander in a discretionary movement. Considering the above ongoing applications, this examination concentrates on execution investigation of routing protocols considering their hub thickness and activity design for a settled size grounds region. This examination assesses four routing protocols i.e. DSR, AODV, TORA and OLSR protocols for MANETs systems in view of execution for various hub thickness for ongoing traffics. The execution measurements are taken as deferral, system load, and the throughput. The correlation investigation is completed about mentioned protocols.

III. Simulation Environment

The simulation in this research is done using OPNET 14.5 simulator which provides a scalable environment for MANETs simulation. In order to analyze the impact of Jellyfish attacks on DSR protocols, the DSR was modified to simulate Jellyfish attack. In this research, we have used 30 nodes by adopting wireless network moving by random speed, varying from 1 to 10 m/sec, an average speed of a common person while using a vehicle. Any object can direct in any direction randomly, and then pause time (stop for a limited time) and then alter the direction of the object and then restart moving. The routing protocol DSR is used to do all the simulation works.
along with the different speed of nodes. The parameters of simulation are shown in Table 1.

### Table 1: Simulation Parameters

| Parameter           | Value                  |
|---------------------|------------------------|
| Routing Protocol    | Dynamic Source Routing |
| Types of Attack     | Jellyfish Attack       |
| Model for Mobility  | Random Way point       |
| Simulation Time     | 300                    |
| Nodes               | 30                     |
| Simulation Area     | 1000m × 1000m          |
| Node Speed          | 1-10m/sec              |
| Pause Time          | 10 sec                 |
| Types of Traffic    | Constrain Bit Rate     |

### IV. Results and Discussion

In this section the performance of DSR routing protocol in MANET environment with different number of Jellyfish attacks is evaluated using different performance evaluation parameters such as packet delivery ratio, end to end delay and throughput.

#### A. Packet Delivery Ratio (PDR)

PDR engrossed by the end node and by the forwarding packets along with the total packets taken from the source nodes. PDR is calculated using equation 1.

\[
PDR = \frac{\text{total packets received}}{\text{total packets sent}} \times 100
\]  

Fig. 1 shows the PDR values for different scenarios. From Fig. 1 it can be revealed that the PDR for DSR without attack is 93.88%. When one Jellyfish attack node is introduced in the network then PDR becomes 75.24% which shows a significant decrease in PDR value as compared to DSR without Jellyfish attack.

When the number of Jellyfish attacks is 2 then PDR becomes 69.46% which shows further degradation in performance as compared to DSR with one Jellyfish attack. The PDR for scenarios having 3 and 4 Jellyfish attacks are 61.78% and 53.79% respectively. It can be concluded from Fig. 1 that when the numbers of Jellyfish attack nodes increases in the network then the PDR decreases which shows the performance degradation in terms of PDR in the presence of Jellyfish attack.
Fig. 1: Simulation of Packet Delivery Ratio for the DSR along with up to four Jellyfish Attacks

B. End-to-End Delay

The express to transmit the information from the starting node to the final node, every delay leads due to the temporary store line up the time, the retransfer delay, the total time consumed by the packet’s information reaches to its end nodes. In normal traffic when there are no Jellyfish attacker nodes in the networks, there is less End-to-End delay from sender to receiver nodes. Fig. 2 reveals the simulation results of End-to-End delay of the DSR protocol along with up to four Jellyfish attacker node in the network.

It is clear from Fig. 2 that when there is no Jellyfish attack in the MANETs environment then the value of end to end delay is 0.0031 sec. When single Jellyfish attacker node is introduced in the MANETs environment then end-to-end delay becomes 0.0118 sec which shows an increase in end to end delay as compared to the scenario having no Jellyfish attack. The end to end delay is 0.022 sec when the numbers of Jellyfish attacker nodes are two. The simulation results in Fig. 2 show that the end to end delay for DSR having three and four Jellyfish attacker nodes is 0.036 sec and 0.076 sec respectively. It means that when the number of Jellyfish attacker nodes increased in the network then end to end delay significantly increased. Moreover the Jellyfish attack significantly worsens the performance of DSR routing protocol in terms of end to end delay.
C. Throughput

Throughput is the definition of success required to pass to their destination in the number of packets per unit time. The calculation of throughput is in bits per second (bps). We have used four different scenarios with different numbers of Jellyfish attacker nodes deployed. From the simulation result, as shown in Fig.3, the throughput for DSR without Jellyfish attack is 46081.03 bit/sec. When one Jellyfish attack is introduced in the network then throughput of DSR with one Jellyfish attack becomes 28164.48 bit/sec which illustrates a significant degradation in the performance of DSR routing protocol in terms of throughput.

By increasing the numbers of Jellyfish attacker node, throughput decreases gradually. Fig. 3 shows the result of DSR protocols along with two Jellyfish attacker nodes in the network. It can be concluded from Fig. 3 that the throughput of the DSR protocol decreased to 26077.29 bit/sec when the number of Jellyfish attacker nodes are two. Fig.3 also shows the result of DSR protocol along with the three and four Jellyfish attack in the network. The simulation result revealed that the throughput of DSR routing protocol decreased to 9060.704 bit/sec and 6292.42 bit/sec respectively.

From the simulation result shown in Fig. 3, it can be concluded that the Jellyfish attacker node highly degrades the performance of DSR protocol in terms of throughput. By increasing the numbers of Jellyfish attacker nodes decrease the throughput of the DSR protocol.
In this research paper, we considered the impact of Jellyfish attack on the performance of DSR routing protocol in terms of different performance evaluation parameters in MANETs environment. We evaluated and analyzed the performance degradation under different numbers of Jellyfish attack on DSR routing protocol during data transmission. Simulation results are compared in term of difference performance evaluation parameters such as throughput, end-to-end delay and PDR. It is concluded that PDR and throughput decrease with increasing the numbers of Jellyfish attacker node in the network. End-to-End Delay increases whenever the number of Jellyfish attacker nodes increase in the networks. Since in this type of attack, the packets reached to its destination but take more time. Therefore, early detection of such attacks is a challenging task. This research can further be expanded in many ways, such as early detection of Jellyfish attack and for avoiding Jellyfish attack in DSR. Moreover, there are such techniques that can speed up the removal mechanism of Jellyfish attack. There is also a need for an automatic mechanism that can automatically detect and remove Jellyfish attack in MANETs environment.

**V. Conclusion and Future Work**

![Throughput graph](image)

Fig. 3: Average Throughput (bits/sec) of DSR with up to four Jellyfish Attacks

|              | JF1         | JF2         | JF3         | JF4         |
|--------------|-------------|-------------|-------------|-------------|
| Normal DSR   | 46081.03    | 46081.03    | 46081.03    | 46081.03    |
| DSR with JF attack | 28164.48    | 26077.29    | 9060.704    | 6292.42     |
References

I A. Kaur and D. T. P. Singh, “Securing MANET from jellyfish attack using selective node participation approach,” International Journal of Engineering and Technical Research (IJETR) ISSN, pp. 2321–0869.

II Al Dulaimi, L. A. K., R. B. Ahmad, N, Yaakob, S, N, W, Shamsuddin and M, Elshaikh 2018. Behavioral and performance jellyfish attack. Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 2, February 2019, pp. 683–688,

III Cai, J. P. Yi. J.Chen. Z. Wang and N. Liu. 2010. An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network . 24th IEEE International Conference on Advanced Information Networking and Applications; pp 775-780

IV Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: Accurate prevention and detection of Jelly Fish attack in MANET. Ieee Access, 6, 56954-56965.

V Khirasariya H. 2001. Simulation study of jellyfish attack in MANET (mobile ad hoc network) using Aodv Routing Protocol.Journal Of Information, Knowledge And Research In Computer Engineering; Vol(2); pp 344-347

VI M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” Ad hoc networks, vol. 2, no. 1, pp. 1–22, 2004.

VII M.Kaur, M.Rani,and A. Nayyar. 2014. A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks. International Journal of Computer Science and Mobile Computing; Vol(3): pp 199-203

VIII Mewara, H.S. and S. Porwal. 2010. Node Density and Traffic based Modelling and Analysis of Routing Protocols for MANETs; pp 1-6

IX P. Misra, “Routing protocols for ad hoc mobile wireless networks,” Courses Notes, available at http://www. cis. ohiostate. edu/~ jain/cis788-99/adhoc routing/index. html, 1999.

X R.V Boppana, and A. Mathur. 2005. Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks. Workshop on Next Generation Wireless Networks; pp 1-8.