Impact Analysis of JellyFish Attack in MANETs

Abdul Kayum Ali, Bobby Sharma and Usha Mary Sharma
Don Bosco College of Engineering and Technology, Assam Don Bosco University
Airport Road, Azara, Guwahati - 781017, Assam. INDIA.
a.kayum001@email.com
bobby.sharma@dbuniversityl.ac.in
ushamary.sharma@gmail.com

Abstract: ***MANETs or Mobile Ad Hoc Networks is a network that consists of mobile nodes, is self-organizing and short lived. Due to the openness, decentralized and infrastructure less architecture it can be prone to different types of attacks. One such attack is the JellyFish attack. It is a type of passive attack .It is very difficult to detect this attack as it complies with the protocols. In this paper we present a study on this attack and its variants. The first section gives a brief introduction on MANETs and the different types of attacks on it from different point of view. The later section we concentrate on the JellyFish Attack. Further a review on the analysis is carried out from different sources to understand the impact of this attack on the performance and its effect on the network.***

Keywords: Active attacks, Passive Attacks, JellyFish Attack, AODV, DSR, TORA, GRP.

1. Introduction

Mobile Ad Hoc Network or MANETs consists of mobile nodes that are short lived and self-organizing wireless network. Communication between the nodes take place through the radio links without the use of any fixed pre-established infrastructure for communication. MANETs usually consists of small devices that are light weight and are battery operated. As with any networks, MANETs is also vulnerable to different types of attacks and security issues. This is because of the openness of the medium, dynamic topology, decentralized administration, distributed co-operation, lack of clear line of defense and power constrains. Different secure routing protocols are available for MANETs like SAODV, ARAN, SRP, SAR, etc. But these protocols may not be able to provide optimized performance. There may be a tradeoff between Security and Performance. [1][2][3][4]

Securityrefers to protecting the privacy, availability, integrity and non-repudiation. Security implies the identification of potential attacks, use, modification or destruction, unauthorized access. An attack is the compromisation of security information without any authorization. Two broad types of attack are possible in MANETs. They are PASSIVE Attacks and ACTIVE Attacks. [4]

In PASSIVE attacks the attacker listens to the traffic channels to gain valuable information and data. The attacker does not change any data or cause any type of disruption in the network. Snooping is one of the Passive attacks. These types of attacks are very hard to detect. [4]

In ACTIVE attack the attacker tries to disrupt the network. The attacker may modify, listen and inject messages in the communication channel. This attack can be internal from someone within the network or external from outside the network. Internal attacks are most serious as the attacker has idea of the useful recourses of the system. Different types of Active attacks are *Jamming Attack, Wormhole Attack, Black hole Attack, Sinkhole Attack, Grey hole Attack, Byzantine Attack, Information Disclosure Attack, Resource Consumption Attack, Man-In-The-Middle Attack, Neighbor Attack, Routing Attacks, Routing Attacks, Stealth Attacks,*

Session Hijacking Attack, Repudiation Attack, Denial of Service Attack, Repudiation Attack, Sybil Attack, Misrouting Attack, Device Tampering Attack, JellyFish Attack, Eclipse Attack. [4][5][6]

All the above mention attacks occur in the different layer of the network. Figure 1 show the different type of attack according to the layers.

2. Types of Attacks

When MANETs is integrated with Internet some other types of attacks come into picture. These are called Attacks on Internet Connectivity. Some of this type of Attack is a) Bogus Registration,

b) Forged FA, c) Replay Attack. In general, attacks on Internet connectivity are caused by malicious nodes that may modify, drop or generate messages related to mobile IP such as advertisement, registration request or reply to disrupt the global Internet connectivity. [6]

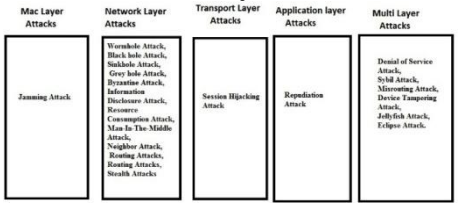

Figure1: Attacks on different layer

In this paper we try to understand about the JellyFish attack on MANET. We later study the different impacts of this attack and try to analysis the results based on some of the research paper. In the later section we present the concept of JellyFish Attack and analyze the impact on MANETs.

3. Jellyfish Attack

The JellyFish is a type of passive attack. In this attack a malicious node make use of the vulnerabilities of the protocol and may reorder, delay and drop packets. It complies with the protocol making it very difficult to detect. Application that uses TCP is more vulnerable to this type of attack as TCP has well known vulnerabilities to mis-order,

drop, delay the packets. A JellyFish attacker obeys the rule of the protocol so that it cannot be detected. Like a black hole attack the JellyFish attacker captures the packets but instead of dropping the packets it may decide to reorder, or drop some of the packets but not all at once. Close loops flows are generally targeted by the attacker. The attacker's main aim is to reduce the throughput of the network by dropping some packet or delaying them. Thus it is also a kind of Denial of Service attack as it tries to disrupt the services in the network. A JellyFish attacker will take part in the route discovery and packet forwarding process so that it may not be discovered. Reference also described that malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets. The below Figure shows an attack scenario for a JellyFish Attack.[7][8]

As shown in Figure 2, JF is the JellyFish Attacker node .When node A communicates with node D via the node C and JF, the attacker node JF can either drop or delay the packets to D. The node JF will take part in node discovery and packet forwarding, and will make use of the vulnerabilities of the protocol, such that he remains undetecTABLE and in time reduce the good put of the network. [8]

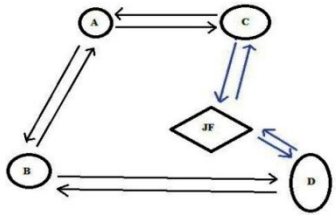

Figure2: JellyFish Attack scenario

JellyFish attack is divided into three sub categories

[24] JellyFish Reorder Attack,
[25] JellyFish Periodic Dropping Attack and
[26] JellyFish Delay Variance Attack.

3.1 JellyFish Reorder Attack

In this attack the attacker reorder the packet maliciously. An attacker receive packet and places all the packets in a reordering buffer instead of the FIFO buffers and the delivers them. The attacker uses the vulnerabilities of TCP that provides mechanism to increase the robustness for out of order packets. [8][9]

3.2 JellyFish Periodic Dropping Attack

In this attack, the attacker drops some packets before forwarding it. The packets are drop for a short period of time. This timing pattern is known and decided by the attacker. The attacker knows the flow of packets and itself induces a loss in the transmissions of packets. [8][9]

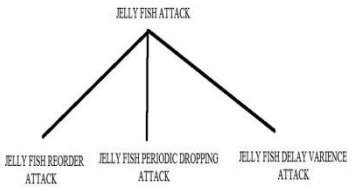

Figure3: JellyFish Attack Sub-categories

3.3 JellyFish Delay Variance Attack

In this attack the packets are delayed as they are forwarded by the JellyFish Attacker node .One of the TCP component is the variable round trip times due to congestion. By delaying the packets the attacker can reduce the TCP throughput significantly. Thus the performance of the network is affected. The attacker waits for significant amount of time before servicing the packets and thus increases the delay significantly. [8][9]

4. Literature Review

JellyFish attacks in MANETs were first discussed by Aad et al [9].In this paper the author first gives a description of the attack and then discuss the different variance of the attack. They later do the simulation of the attack's three variance that is the reordering attack, packet dropping attack, delay variance attack. Their study scenario consists of a simple chain with a series of nodes between the sender and receiver, some out of which being a JellyFish attacker node. They first study the JellyFish reorder attack. They see that if the attacker increases the reordering of the packets by increasing their reordering buffer the throughput decrease significantly. If 3 or more packets are reorder in the buffer then the throughput at the peak value is decreased by approximately 1% resulting in successful attack and near flow starvation. They also mention a TCP-PR as a solution to reduce this variant of the attack. The second scenario is for the JellyFish periodic dropping attacks. Their study showed a 9% dropping time and 91% forwarding time for a JellyFish attacker node dropping packets for 90 microsecond every 1 second thus showing attacker's successful exploitation of the slow-timescale congestion avoidance mechanism of TCP. In the third scenario i.e., for the delay variance attack, the JellyFish attacker node act as a vacation sever and alternates between period for serving no packets and serving packets with maximum capacity, each period being of equal length. This introduces jitters and increase in the jitters decreases the goodput. The increased mean delay also decrease the throughput of the network. [9]

In paper[10], authors have performed the simulations to study the effect of JellyFish attacks on four routing protocols that is, Ad-hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic source routing protocol(DSR), Temporally ordered routing protocol(TORA), Geographical routing protocol(GRP). The simulation scenario consists of an Opnet modeler 14.5, area of 10*10,two network of size 30 nodes and 50 nodes, a random mobility model, random topology, a high resolution video traffic type, simulation time of 20 minutes ,an ipv4 address mode and routing protocols AODV,DSR,TORA,GRP. There were 2 scenarios for each routing protocol one without a JellyFish node and one with the JellyFish node for a network size of 30 and 50 nodes respectively. The simulation shows the results of performance based on Data dropped due to buffer overflow, Data dropped due to retry threshold exceeded, load, media access delay, retransmission of packets. For 30 nodes, data dropped due to buffer overflow is very high for TORA in presence of the JellyFish node, so was the data dropped due to retry threshold exceeded found high in TORA. When he node size is increased to 50 the drops gets high on DSR. Delay is low in GRP if we increase the node density. Load is

less in case of AODV and TORA. For lower density of nodes i.e. 30, GRP performs better for Media Access Delay and Retransmission Attempts and when we increase the density up to 50 nodes, AODV performance is good. DSR performs worst. [10]

In paper [11] the author studies the JellyFish attacks based on the simulation using the AODV routing protocol. They studied the attack based on the number of attackers and the End to End delays and Delay jitters. Their studies area includes Number of Flows, Node Mobility, Traffic loads, and Attack positions. For number of flow, with increase in the number of attackers leads to end to end delay being longer and a larger increase in the delay jitters. For mobility, end to end and delay jitters are shown higher for slow mobility rate which is because of the difficulty of the attacker to invade the routing path. For Traffic load, the end to end and delay jitters increase the traffic load with increase in the number of attackers. For attack position, the studies show that near sender position are the most vulnerable causing high end to end delay and jitters. Their Studies shows that the more attackers there are in the network, the more damage they inflict on a flow in terms of packet delivery ratio and delay jitter. Similar studies have also been done by the author of [12].

In paper [13], simulations have been done the authors to understand the performance of MANETs in the presence of an JellyFish attacker. Their simulation considers 3 scenarios viz, Normal Flow, 2 JellyFish Attacker and 4 JellyFish Attacker. Their simulation results showed the increase in the number of hops due to attacker presence. The delivery of packets is also delayed due to the presence of the attacker node resulting in packets being drop. Because of the presence of the attacker the delay produce in delivery of packets cause reduction of traffic received. There is an end to end delay increase in the network due to the presence of the JellyFish node which delivers the packet in the network. The throughput is badly affected due to the increase of the presence of the JellyFish Attacker. Their studies show that there is an increase of 3.38% for 10% attackers and 10.76% for 20% attackers for the end to end delay.

Though there has been much development in intrusion detection and trust-based systems to protect ad hoc networks against attacks, defensive mechanism may not able to detect protocol compliant JellyFish attacks [14]. In [14], the author introduce a security scheme called JAM (JellyFish Attacks Mitigator) which can be used to detect and mitigate JellyFish attacks in ad hoc networks. A MAC layer Acknowledgements (MAC ACK) is used by the destination to inform the source for successful reception. For unacknowledged frames the source resends the frames. A secure AODV protocol such as SAODV for authentication and message integrity is supposed to be working. In their proposed model, the TCP protocol is modified so when low goodput or high RTO values are observed, it starts sending packets called catalyst-helper packets (CHPs) in a constant ratio to check for congestion. This avoids long waiting times if there is no longer network congestion and allows observing nodes to detect misbehaviors by attackers and hence those nodes can be isolated. The packet is identified with a cumulative sequence numbers (SEQs) in clear text. A unique id number (flow id) is provided each new flow. The nodes identify packets by 3-tuple values (IP address, flow id, SEQ).Nodes can easily detect JellyFish reorder attacks by comparing the SEQs of outgoing packets only. For JellyFish periodic attacks, reception time of each packet is stored by the nodes. A packet that is not forwarded within a specific period is considered as dropped. Nodes also collect a set of distances between two successive drop intervals to emulate the malicious periodic drop interval. For forwarded packets, the set of offsets relative to the set of distances is determined and the biggest gap is computed. When the found gap contains several drop intervals within it, a JellyFish periodic attack is detected. The accuracy of detection improves with an increase in the number of forwarded packets considered. [14]

In [10], the author observed the following results of their simulation .the measure the different performance metrics of network under a normal aloe and under a network under a JellyFish attack.

From above the authors in [10] concludes that if good time services and no loss of information needs then TORA is a good choice and if we want low delay produced during transmission and reception of information and data then go for AODV. In comparison with the protocol, DSR is poor. If we increase node density, forwarding rate of packets, use different protocol and introduced JellyFish periodic dropping attack the performance may vary.

5. Result and Analysis

As per paper [9], the author observes the following aspect of the JellyFish Attack on the performance of the network.

TABLE 1: Observation for the three scenario of JellyFish Attack from [9]

Scenerios	**Without the JellyFish Attack**	**With the JellyFish Attack**	**Remarks**
JellyFish reordering attack	A throughput of 710 kb/s is observed.	Reordering of 3 or more packets, causes the throughput decreases to approximately 1% of the peak value indicating a successful attack and near starvation of the flow.	There is a decrease in the throughput
JellyFish periodic dropping attack	When no attack ,the flow obtains a throughput of 710kb/s	When under attack to obtain a null at 1second, the JellyFish node drops packets for 90 ms every 1 second, which results in dropping 9% of the time, and forwarding 91% percent of the time, values easily incurred by a congested node	The attack is therefore successfully exploiting the slow-timescale congestion avoidance mechanism of TCP and the throughput is reduced.
JellyFish Delay Variance Attack	There is no jitters and very less delays and good throughput is observed.	JellyFish node behaves as a server with vacations, alternating between periods of serving no packets (and queuing, but not dropping them) and serving packets at its maximum capacity. Both idle and active periods are of equal lengths. This introduces Jitters and delays.	The decrease in the Throughput due to increased mean delay and jitters indicates that the effects of this attack can be quite severe.

TABLE 2 : Results of the simulation on the performance of a network under Normal and JellyFish Attack Conditions

Metrics		30 nodes				50 nodes			
Data dropped (Buffer overflow) (kb/sec)	Protocols	AODV	DSR	TORA	GRP	AODV	DSR	TORA	GRP
	Normal Flow	88000	260000	97000	18500	85100	329000	18000	279000
	JellyFish Flow	71000	250000	250000	18900	45100	361000	31500	284000
Data dropped (Retry threshold exceed) (kb/sec)	Protocol	AODV	DSR	TORA	GRP	AODV	DSR	TORA	GRP
	Normal Flow	7.5	14.3	6.28	14.7	7300	24600	2570	33700
	JellyFish Flow	7.2	13.9	13.8	15.9	9000	29600	2830	37300
Load (kb/sec)	Protocols	AODV	DSR	TORA	GRP	AODV	DSR	TORA	GRP
	Normal Flow	90000	262000	99000	190000	85300	332000	18200	282000
	JellyFish Flow	73000	251000	254000	193000	45900	361000	31800	290000
Media Access Delay (sec)	Protocols	AODV	DSR	TORA	GRP	AODV	DSR	TORA	GRP
	Normal Flow	5.4	1.92	1.34	1.08	5	10	36.6	1.7
	JellyFish Flow	5.4	1.95	1.97	1.18	1.13	7.1	32.8	1.75
Retransmission of Packets (Packets)	Protocols	AODV	DSR	TORA	GRP	AODV	DSR	TORA	GRP
	Normal Flow	0.81	0.77	0.76	0.75	0.819	1	1.03	0.94
	JellyFish Flow	0.79	0.77	0.77	0.72	0.78	1	1.04	0.94

In [10], the author observed the following results of their simulation .the measure the different performance metrics of network under a normal aloe and under a network under a JellyFish attack.

From above the authors in [10] concludes that if good time services and no loss of information needs then TORA is a good choice and if we want low delay produced during transmission and reception of information and data then go for AODV. In comparison with the protocol, DSR is poor. If we increase node density, forwarding rate of packets, use different protocol and introduced JellyFish periodic dropping attack the performance may vary.

6. Conclusion and Future Works

In this paper we have presented a brief introduction of MANETs and the different types of attacks on MANETs. Out of the many attacks on MANETs, we focus our studies on JellyFish Attack. We studied the JellyFish Attacks in and its different variants. The JellyFish attack is one of the most difficult to detect attack and cause decrease of the network performance. We also present a description of the JellyFish Attack and analyze the effect of the attack on different aspects of the network based on the different works done by different researchers. As it has been known that JellyFish attack is very difficult to detect due to its compliance with available protocol, we also bring into light one of the proposed method for detecting the JellyFish attack in paper[14]. Future work may include development of a much better and efficient detection system that can easily identify this attack and take measures to protect against this attack.

References

[1] C.K. Tok, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," *Pearson Education, pp. 28-30, 2002.*

[2] X. Cheng, X. Huang and D. Z Du, "Ad Hoc Wireless Networking,"*Kluwer Academic Publishers, ISBN: 1-4020-7712-2, pp. 319-364, 2006.*

[3] C. Siva Ram Murthy and B.S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," *Pearson Education, ISBN: 978-81-317-0688-6, 2006.*

[4] K. Sahadevaiah," Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks,"*ISSN 1943-3581 2011, Vol. 3, No. 4.*

[5] Prasant Mohapatra and Srikanth V. Krishnamurthy, "Ad Hoc Networks: Technologies and Protocols," *Springer International Edition, 2005.*

[6] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay," Different Types of Attacks on Integrated MANET-Internet Communication,"*IJCSS , Volume (4): Issue (3).*

[7] Hetal P. Patel, Prof. Minubhai. B. Chaudhari, "Survey: Impact of JellyFish On Wireless Ad-Hoc Network,"*in proceeding of INJCR'10, Volume.10, issue.5, no.2pp. 5-9, 2010.*

[8] Manjot Kaur, Malti Rani, Anand Nayyar ,"A Comprehensive Study of JellyFish Attack in Mobile Ad hoc Networks,*"IJCSMC, Vol. 3, Issue. 4, April 2014, pg.199 – 203.*

[9] Imad Aad, Jean-Pierre Hubaux, Senior Member, IEEE, and Edward W. Knightly, Senior Member, IEEE," Impact of Denial of Service Attacks on Ad Hoc Networks,*" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 4, AUGUST 2008.*

[10] Amandeep Kaur, Deepinder Singh Wadhwa," Effects of JellyFish Attack on Mobile Ad-Hoc Network's Routing Protocols,"*ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.1694-1700.*

[11] Mr. Hepikumar R.Khirasariya," Simulation study of Jellyfish Attack in Manet (mobile ad hoc network) using AODVRouting Protocol,"*ISSN: 0975 – 6760| Nov 2 To Oct 13 | Volume – 02, Issue – 02.*

[12] Hoang Lan Nguyen, Uyen Trang Nguyen," A Study Of Different Types Of Attacks In Mobile AdHoc Networks," *2012 25th IEEE CCECE*.

[13] Mohammad Wazid, Roshan Singh Sachan, R H Goudar," Measuring the Impact of JellyFish Attack on the Performance of Mobile Ad Hoc Networks using AODV Protocol," *Elsevier, 2012*.

[14] Fahad Samad, Qassem Abu Ahmed, Asadullah Shaikh, and Abdul Aziz," JAM: Mitigating JellyFish Attacks in Wireless Ad Hoc

Authors Profile

Dr Bobby Sarma, is a faculty member of Dept, Of Computer Science and Engineering & Information Technology of School of Technology, Assam Don Bosco University. Her subject of interest are Computer Network Security , Artificial Intelligence, Compiler Design

Usha Mary Sarma, is a faculty member of Dept, Of Computer Science and Engineering & Information Technology of School of Technology, Assam Don Bosco University. Her subject of interest are Image Processing, Computer Network

Abdul Kayum, is a MTech student of Dept, Of Computer Science and Engineering & Information Technology of School of Technology, Assam Don Bosco University. His subject of interest are Computer Network Security , Artificial Intelligence