MITIGATION FOR JELLY FISH ATTACK ON MANET

By

SHWETA SHAH * MADHU SHARMA ** ASHISH JAIN ***

* Postgraduate, Institute of Engineering and Technology, DAVV, Indore, India.
** Postgraduate, Institute of Engineering and Technology, DAVV, Indore, India.
*** Research Scholar, Institute of Engineering and Technology, DAVV, Indore, India.

ABSTRACT

Mobile Adhoc Networks have become a part and parcel of technology advancements due to its extraordinary technique. Open communication feature make it prone for various security threats. Subsequently, there are many security threats like DDOS, Wormhole, Black hole etc., which not only affect the network performance but also responsible for the leakage of sensitivity of information. Jelly-Fish attack is one of the routing disruption attack which lies in the series of wormhole and black hole attack at network layer. It attempts to compromise the network packet and store them for a period of time. It may try to introduce delay or partial capturing of packets during communication. Due to big impact of jellyfish attack, it has gained a big name in recently and most wide area for researchers. Jellyfish Attack exploits the end-to-end communication and creates congestion in transmission protocols. Arbitrary network failure or node failure is the natural phenomena and may vary as per real life deployment, but intentional failure or compromising network may lead to information leakage. Security in mobile networks is a challenging task. The complete study observes that the security threats not only capture the packets but also degrades the network performance. To overcome vulnerability problems, this work considers jellyfish attack as the study target and will derive a mechanism to identify and prevent mobile networks from security threats.

Keywords: MANETs, Security, Jellyfish Attack.

INTRODUCTION

Mobile Ad-hoc Network is a novel kind of wireless networks which is a collection of mobile nodes having infrastructure-less technology. Every mobile node has individual transmitter, receiver, processor and battery with self-configurable technology. Wireless communication link is used for connection establishment and communication purpose. An ad-hoc network doesn't use centralized controller like cellular network and establishes network without using third party device. Here, every mobile node is capable to work as transmitter, receiver and router for route discovery. Mobility gives a wide scale to mobile nodes to join or leave the network as they wish. Any node can change their network of position whenever they want. Due to limited transmission range and transmitter capability, intermediate nodes or multi-hops are required for information transmission to reach at another node. Here, every node is willing to forward packets to other node [1].

A better understanding of such ad-hoc network can be explained by considering a network of 5 nodes named as A, B, C, D and E. All are mobile nodes and can have limited transmission range. Suppose Node A wants to send a packet to E, it is necessary to involve other mobile nodes to establish a proper communication. Here, D will be an intermediate node to forward the packet to E. A will be the source node and E will be known as the destination node. A complete scenario is shown in Figure 1, which explains that the topological instability requires a set of policy to discover routes and transfer packet from one node to others. Figure 2 illustrates the classification of routing protocols.

The complete work observed that the mobile ad-hoc network is a very useful kind of wireless network and it has many advantages that can be explained as follows,

- Access to anywhere and services regardless of geographical location.

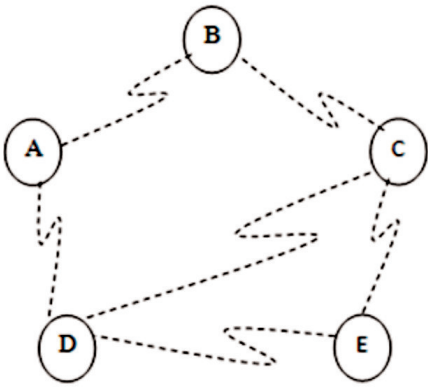

Figure 1. Mobile Ad-Hoc Networks

- No need of centralized control.
- Self configurable mobile node having special characteristics.
- Scalable topology.
- Enhanced flexibility.
- Robust administration.

The nodes involved in a MANET should co-operate with each other and are conversed among themselves and each mobile node acts as a relay as needed, to the implementation of specific functions such as routing and security.

- Multi-hop Routing

When source wants to forward packet to destination, it is communicated through intermediate nodes.

- Autonomous terminal

In MANET, every mobile node is an independent node, which could function as both a host and a router.

- Dynamic topology

Volatile methodology gives freedom to deploy an arbitrary shape node and node movement with variable speeds. Network topology may change with time of requirement but, performance will not be affected.

- Light-weight terminals

In maximum cases, the nodes in MANET are mobile with less CPU capability, low power storage and limited memory size.

- Shared Physical Medium

It uses wireless communication technology based on shared bandwidth concept to establish the communication.

- Distributed operation

Absence of central authority may give the distributed load balancing and communication sharing.

1. Related Works

Kaur and Rani [2] explored that the ad-hoc network is one of the leading solutions to establish temporary communication. Mobile ad-hoc networks are vulnerable, due to open nature and advancements of security threats. They observed various security threats in this paper and enlisted that jellyfish is the one of the most saviour security threats for various autonomous systems or ad-hoc networks. Shared bandwidth and intermediate node forwarding gives an opportunity to store packet for a period of time at attacker node. There are various attacks those affects the performance of network, but jelly-fish attempts to create kiosk between end-to-end communication and use TTL threshold to naturally drop packets.

Kaur and Sandhu [3] explored the study about AODV, OLSR and TORA routing protocols. The performance of network is also observed through OPNET 14.0 simulator. It is evaluated on the basis of data dropped due to buffer overflow or retry threshold exceeded or overload on bandwidth.

Sharma [4] et al. enlisted that the ad-hoc networks suffer with lot of challenges or limitations which gives a big impact on the performance of communication. Some of them are very serious like in resource capabilities due to infrastructure-less topology and small size of mobile nodes. Subsequently, absence of centralized authority require an intermediate node to forward packets which also increases the resource consumption for every node. The author also investigated that, this drawback may be an opportunity for jellyfish attack and the attacker can get benefit of vulnerabilities of routing protocols and hold the packets or drop as per the attacking strategy. Here, they give a brief introduction of all jelly-fish techniques and methodology for completion.

Marti et al. [5] addressed that the wired networks are the most secure solution for communication due to unicast

communication and temper proof links. But, due to infrastructure requirement and unavailability for mobility, they may become useless for certain applications. Attacks may be classified as routing disruption of resource draining attacks. Jellyfish is the combination of routing disruption and resource draining method that not only tries to exploit the vulnerabilities of routing protocols but also degrade the hardware performance. They observed that the jelly-fish is one of the variant of DDOS attacks, which may behave as a black hole attack.

The complete study concluded that the Jellyfish have three ways for implementation which can be enlisted as Jellyfish Reorder Attack, Jellyfish Periodic Dropping Attack and Jellyfish Delay Variance Attack [6]. The attacker node reorder the packets, reduces the high-quality put of destination to a sure level and increases the average End-to- End Delay. They consider ZRP routing protocols and implement the proposed solution with NS-2 simulator.

2. Ad-hoc On-Demand Distance Vector Routing (AODV)

Routing protocols identify how routers communicate with each other, disseminating in sequence that enables them to decide on routes between any two nodes on a computer network. Routing algorithms settled on the specific choice of route. Each router has a priori information only of networks attached to it straight. A routing etiquette shares this information first amongst immediate neighbors, and then right through the network. This way, routers gain acquaintance of the topology of the set-up [6].

There is a classification of routing protocols that are implemented in Wireless Sensor Network for secure routing.

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV, routes to connect two nodes are obtained only when it is required i.e. on-demand. AODV routing algorithm is especially suited for dynamic self-configured networks like MANET. AODV provides loop free routes along with route management for broken links. The bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements [7].

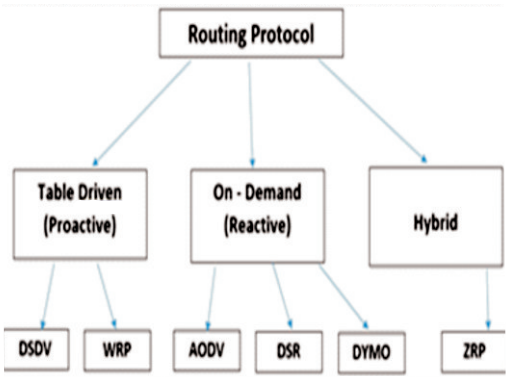

Figure 2. Classification of Routing Protocols

AODV uses symmetric links between communicating nodes. Nodes which are communicating or intermediate nodes on active route only maintain routing information. Nodes which do lie on active path need not maintain routing information and does not exchange routing table periodically. Furthermore, the routes are discovered and maintained between two nodes only when they need to communicate or if they are acting as the intermediate node supporting in communication.

The AODV algorithm's primary objectives are as follows [8,9],

- Initiate route discovery only when necessary.
- Periodic exchanges utilized only for local connectivity management and not for general topology maintenance.
- Sharing the local connectivity information with only those neighboring nodes which may need the information.

For route discovery, AODV uses the broadcast mechanism [4]. Instead of using source routing, the routing strategy used in AODV is to establish route entries dynamically at intermediate nodes. This kind of routing serves the network with large number of nodes by saving overhead required by source routes in each data packet.

There are three types of control messages in AODV, which are discussed below,

- Route Discovery
- Route Reply (RREP)
- Route Maintenance

Route discovery mechanism is one of the major

operations of this routing protocol, where route discovery happened at the beginning of the process. Here, Source node broadcasts RREQ packet and every intermediate node attempts to discover the ultimate destination. When it reaches to ultimate destination, the destination node generates the RREP message and unicast the reply from the same route. Here, in case of link failure or communication gap, it generates the route maintenance control packets. Route Error RERR messages are sent to inform about the error status of the current route broken. AODV uses the sequence numbers to ensure loop freedom.

3. Jellyfish Attack

Jellyfish is one of the variant of DoS attacks known as Denial of Service attack applied for resource draining. It is a passive kind of attack which produces delay in transmission and reception. Jelly-Fish attack disturbs the network for both TCP and UDP protocols to degrade the network performance. This attack is same as the black hole attack or wormhole attack but the dissimilarity is, it affects the network by bringing in delay. This attack can be classified into three grouping, which is planned below [10,11],

3.1 Jellyfish Reorder Attack

It is based on recorder concept and possible by exploring the vulnerabilities of TCP. It records the packets and diverts the transmission.

3.2 JF Periodic Dropping Attack

It timely drop packets by compromising the nodes. This kind of periodic dropping can be possible through relay node.

3.3 Jellyfish Delay Variance Attack

In this type of attack, the malicious node randomly delays packet without changing the order of the packets.

4. Problem Definition

The study of AODV routing protocols, challenges in MANET and vulnerabilities observations of routing protocols concluded that the wireless networks may get unsuccessful due to security weakness of routing protocols. Challenges in ad-hoc network are the major constraint for any development into the existing system. A little overhead may give a huge impact on network performance and lead to a reason for network collapse [8].

Furthermore, security is the one of the most important requirements nowadays, whereas breaching on security policy may harm a lot on network performance. The study of existing work and proposed solutions concluded that the security threats are the most danger activity applied through attacker either to compromise the network or to collapse the network. Jelly-fish is one of the severe security threat which not only compromise the network but also collapse the communication by draining the network.

The AODV routing protocol is a popular reactive routing protocol in wireless networks. AODV is the successor of AODV routing protocol developed with an aim to enhance the performance of ad-hoc network. AODV routing protocol has been designed for better performance of the network and not for security of the node. The major concern with such routing protocols is to retrieve best performance with minimum resource overhead. At the time of protocol designing, security was not the priority concern, but nowadays it is the most essential challenge.

The complete work generates a need to develop a solution which should integrate with routing protocols to reduce routing protocols vulnerabilities and avoid jelly-fish attack.

5. Methodology

The performance of the proposed solution will be done under three situations which are listed below,

- Ad-hoc network with normal situation.
- Ad-hoc network with Jelly-Fish attack.
- Ad-hoc network with preventive technique.

All the scenarios will be implemented and simulated with Qualnet 5.2 simulator and observed on basis of throughput, packet delivery ratio, and End-to-End delay.

- Simulation of AODV under various attacks is done to analyze the impact on performance metrics when malicious nodes are inserted in the network scenario.
- Analyze the impact of Jelly Fish attack on various

performance metrics for AODV.

- Implement the proposed technique in AODV for detection and prevention of Jelly Fish attack.
- Analyze the performance metrics for modified AODV under JellyFish attack.
- Compare the performance parameters for AODV under normal condition, JellyFish attack and Preventive JellyFish attack.

In short, following steps have been taken to detect and prevent Jelly Fish attack.

- Creation of normal node scenario.
- Deployment of Jelly Fish Attack.
- Deployment of Hello Packet mechanism to detect and prevent Jelly Fish attack.

6. Result Observations

A Qualnet 5.2 simulator has been used to simulate and evaluate the performance of the proposed solution. Qualnet is a licensed simulation tool developed by scalable networks. It gives a GUI based drag and drop environment for easy construction of network and simulation of the proposed solution. Five different scenarios have been constructed and simulated for three different conditions: Normal, attack and preventive approach. All these scenarios are simulated on basis of stationary and mobile condition of mobile nodes [12,13].

The complete work has been simulated into three steps,

Step 1: Mobile Ad-hoc Networks simulation with standard AODV routing protocol.

Step 2: Implementation of JellyFish attack with MANETs.

Step 3: Detection & Prevention of Jelly-Fish Attack in MANET with AODV routing during malicious node.

Property	Value
Traffic Generator Type	CBR (Constant Bit Rate)
MANET Scenario	5 Node, 10 Node, 15 Node, 20 Node, 25 Node
Source Node	Node 1
Destination Node	Node 5
Packet Size (byte)	512 Bytes
Packet to Send	2000 Packet
Time Interval	1 Seconds
Start Time	0 Seconds
End Time	2000 Seconds
Node Placement	Stationary Position / Mobile Position

Table 1. Scenario Configuration

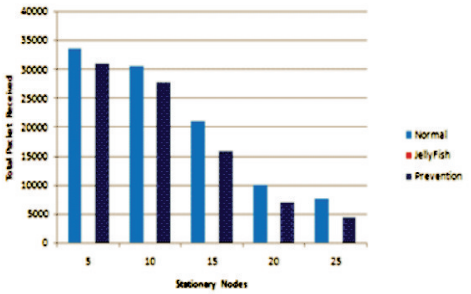

Figure 3. Total Packet Received Analysis of AODV with Stationary Nodes

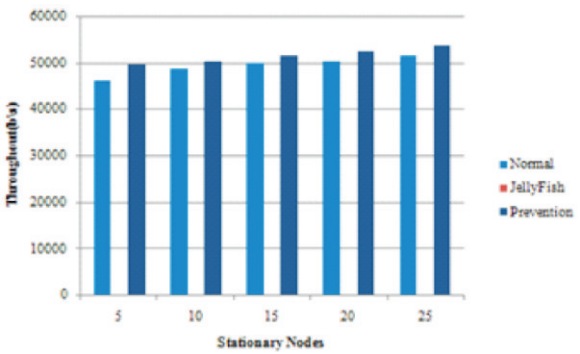

Figure 4. Throughput Analysis of AODV with Stationary Nodes

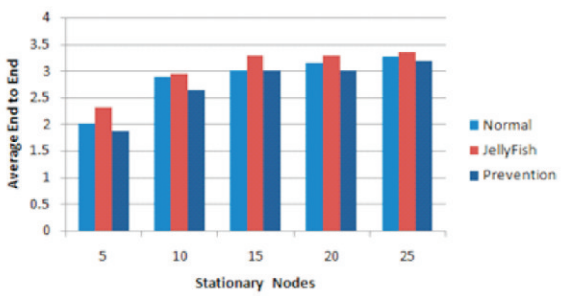

Figure 5. Average End-to-End Delay of AODV with Stationary Nodes

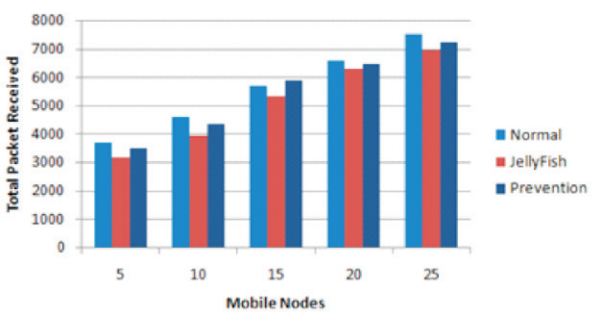

Figure 6. Total Packet Received Analysis of AODV with Mobile Nodes

All the above steps are implemented for 5, 10, 15, 20 & 25 node scenarios with stationary and mobile nodes.

The comparative study of the proposed solution has been represented in graph form. Figure 3 gives Packet Received Analysis, Figure 4 for Throughput Analysis, Figure 5 for Average End to End Delay of the stationary nodes

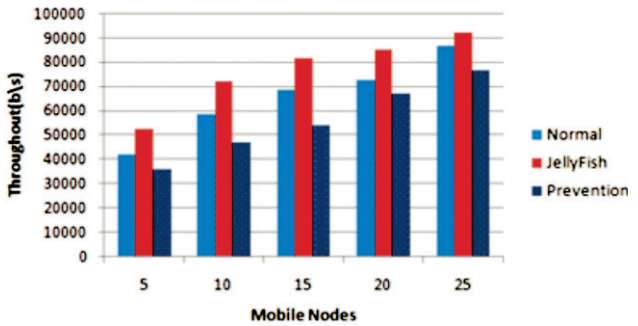

Figure 7. Throughput Analysis of AODV with Mobile Nodes

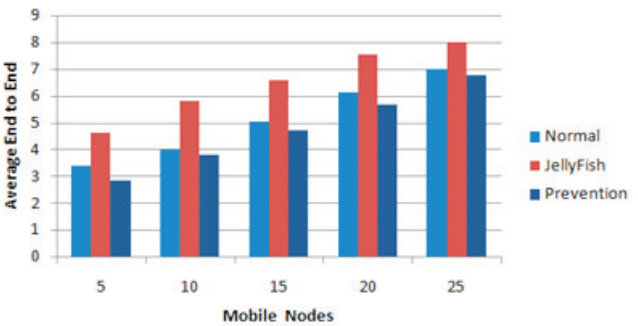

Figure 8. Average End-to-End Delay of AODV with Mobile Nodes

subsequently, Figures 6,7,8 gives same study for the mobile nodes.

Conclusion

This research paper investigates the importance of ad-hoc networks and also finds the impact of jelly-fish attack. It gives the brief details of jellyfish attack and its various classifications. The complete study observes that, jellyfish is one of severe security threats, which introduces delay during transmission. Thus the problems have been observed and a methodology has been proposed to overcome it.

References

[1]. Atul Kahate, (2003). *Cryptography and Network Security*, Second Edition-2003, Tata McGraw Hill N

[2]. Manjot Kaur and Malti Rani, (2014). "A Novel Defense Mechanism via Genetic Algorithm for Counterfeiting and Combating Jelly Fish Attack in Mobile Ad- Hoc Networks". *IEEE*.

[3]. Amneet Kaur and Prabhneet Sandhu, (2014). "Comparison of AODV, OLSR, and TORA in MANET Under Jelly Fish Attack". *IJISET - International Journal of Innovative Science, Engineering & Technology*, Vol. 1, No. 5.

[4]. Avani Sharma, Rajbir Kaur and Purnendu Karmakar†, (2014). "JFDV Attack: Influence on Workability of Mobile Ad-hoc Networks". *CICSYN'14 Proceedings of the 2014 sixth International Conference on Computational Intelligence, Communication Systems and Networks*, pp. 170-175.

[5]. S. Marti, T. Guili, K. Lai, and M. Baker, (2000). "Mitigating routing misbehavior in mobile ad hoc networks". In *Proceedings of MOBICOM 2000*.

[6]. H. Yang, J. Shu, X. Meng, and S. Lu, (2006). "SCAN: Self-organized network-layer security in mobile ad hoc networks". *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2.

[7]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, (2003). "Prevention of cooperative black hole attack in wireless ad hoc networks". In *Proceedings of 2003 International Conference on Wireless Networks (ICWN'03)*, pp. 570-575.

[8]. Piyush Agrawal, R. K. Ghosh, and Sajal K. Das, (2008). "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks". In *Proceedings of the 2nd international Conference on Ubiquitous Information Management and Communication*, pp. 310-314.

[9]. Nadeem and M. Howarth, (2011). "Protection of MANETs from a range of attacks using an intrusion detection & prevention system". *Springer Science and Business Media*, Vol. 146, No. 14.

[10]. H. Deng, H. Li, and D.P. Agrawal, (2002). "Routing security in wireless ad hoc networks". *IEEE Communications Magazine*, Vol. 40, No. 10.

[11]. M. Jackobsson, J. Hubaux, and L. Buttyan, (2003). "A micro-payment scheme encouraging collaboration in multi-hop cellular networks". In *Proceedings of Financial Crypto*, pp. 15-33.

[12]. Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., and Tolle, J. (2007). "Detecting black hole attack in tactical MANETs using topology graph". In *Proceeding of 32nd IEEE Conference on Local Computer Networks*.

[13]. Retrieved from www.Scalable-networks.com

[14]. Programmers Documentation of Qualnet by Scalable Networks version 5.2, 2012.

ABOUT THE AUTHORS

Shweta Shah has received her BE in Computer Science & Engineering from RGPV University and Master of Engineering in Computer Engineering from DAVV University. She has more than 6 Year Experience in education and research field. She has authored many research papers and research projects in National and International Journals. Her current research area is Security Issues in MANET.

Madhu Sharma has received her BE in Information Technology from RGPV University and Master of Engineering in Information Security from DAVV University. She has more than 6 Year Experience in education and research field. Her current research area is Wireless Networks and Security Attacks.

Ashish Jain has received his BE in Computer Science & Engineering from RGPV University and Master of Engineering in Computer Engineering from DAVV University. Currently he is pursuing his PhD from DAVV University in the field of Security Issues in Wireless Networks. He has more than 15 Years of Experience in education and research field. His current research area is MANET, WSN and Security Attacks.