Analysis of Jellyfish Reorder Attack on ZRP

Priya Maheshwari
M.Tech
Krishna Engineering College,
Ghaziabad, UPTU

Leenu Singh
Assistant Professor
Krishna Engineering College,
Ghaziabad, UPTU

ABSTRACT

MANETs are more susceptible to attacks than a wired network. High mobility, lack of central administration, etc. are some of the main causes. One of the DOS attacks known as Jellyfish Attack is difficult to analyze as well as to detect in MANETs as Jellyfisher nodes follow all the protocol rules. There are mainly three classes of jellyfish attacks named as a Jellyfish Reorder Attack, Jellyfish Periodic Dropping Attack and Jellyfish Delay Variance Attack. Jellyfish Reorder Attack is the most devastating attack amongst the three. The attacker node reorders the packet, and reduces the Goodput of destination to a certain level and increases the average End-to-End Delay. ZRP is the hybrid protocol in which each node forms its own zone. This paper is focused on analyzing the impact of the jellyfish reorder attack on the ZRP protocol by using NS2 as a simulator. The metrics used during the simulation are Goodput and End-to-End Delay.

Keywords

Mobile Ad hoc Network, ZRP, Jellyfish Reorder Attack, End-to-End Delay, Goodput.

1. INTRODUCTION

Security is one of the most important issues in MANETs. The routing protocols in MANETs have a breach at the level of security because the protocols do not have an inbuilt defense mechanism for the attacks. These networks often suffer from security attacks because of its characteristics like open medium, dynamically changing topology, lack of central management, and no clear inbuilt defense mechanism. As the topology changes continuously due to the random movement of the nodes, the malicious nodes may join the network and degrade its performance. Therefore, there is an alarming need to study the impact of various types of attacks on MANET routing protocols.

Many attacks do not follow the protocol rules, but the Jellyfish attacker follows all the rules. Acquiescence with all the data plane and control plane protocols is the main power of this attack; hence the detection of this attack is very difficult.

If the Jellyfish Reorder Attacker is reordering the packets that are sent from source to destination, it is very important to analyze the performance of ZRP protocol. After reordering if all the data received at destination are clubbed, then garbled data is obtained. It reduces the Goodput to a certain level. Hence, in this paper, simulation based impact is calculated to determine the performance of ZRP protocol due to Jellyfish Reorder Attack using two metrics named as Goodput and End-to-End Delay.

The rest of this paper is as follows. In Section 2, the literature review is given which mainly includes the summary of the work done by various researchers in the field of Jellyfish attacks and the ZRP protocol. In Section 3, problem definition is given. In Section 4, a brief overview of ZRP protocol is discussed. This section also includes the various types of jellyfish attacks that are encountered in MANETs. In section 5, various performance parameters along with the analysis results have been discussed. Key findings are also discussed in section 5. Section 6 describes the conclusion and future work.

2. LITERATURE REVIEW

Garg et al. have proposed enhancement in AODV protocol for defense against Jellyfish Delay Variance Attack in 2014 [1]. Kaur et al. in 2013 have compared performances of AODV, TORA, GRP (Geographical Routing Protocol) and DSR under Jellyfish Periodic Dropping Attack [2]. The paper has concluded that if good time services are required, then TORA is the best amongst three and if low delay between information flows is required then AODV should be preferred. Patel et al. in 2013 have inquired about congestion behavior of TCP and its variants under Packet reordering attack. The paper has also proposed a solution to packet reordering using hashing concept [3]. Wazid et al. have analyzed the performance of AODV, DSR and TORA under the Jellyfish Delay Variance Attack. The analysis has concluded that if the number of nodes are increased then end to end delay is more in case of the AODV protocol as compared to DSR protocol [4].

In 2012, Wazid et al. have also proposed Cluster and Super Cluster Intrusion Detection Techniques and prevention techniques for Jellyfish Reorder Attack [5]. This paper has proposed an algorithm based on buffer comparison for detecting and preventing a Jellyfish Reorder Attack. Ashish et al. have emphasized upon various types of DOS attacks that are encountered in MANETs and have given a brief overview of all the types of attacks [6]. Another approach has been proposed by kamaljit et al., which calculates the performance of ZRP protocol using different zone radius. The results have concluded that larger zone radius has advantages over smaller zone radius [7]. Jayasingh et al. have proposed an algorithm that detects the Jellyfish Attack at a single node and which can be effectively deployed on all other nodes [8]. The novel metric has also been proposed that detects the Jellyfish Reorder Attack based on the Reorder density, which is a basis for developing a metric. A comparison table is also drawn at the end, which shows the effectiveness of novel metric. It has also helped protocol designers to develop the counter strategies for Jellyfish Attack. Hoang et al. have worked on the most common types of attacks like Black Hole Attack, Neighbor Attack and Jellyfish Attack in MANETs and have simulated these attacks to calculate certain parameters like average End to End delay and average throughput [9]. Imad et al. have talked about Black Hole Attack and Jellyfish Attack and have calculated the impact of these attacks in MANETs using three factors: mobility, node density and system size

[10]. Kejun et al. have discussed about the detection strategies for mainly two types of attacks, Jellyfish Attack and Black Hole Attack [11].

3. PROBLEM DEFINITION

Many researchers have discussed about various types of Jellyfish Attacks. The researchers have also simulated various types of Jellyfish Attacks on various protocols to calculate the performance of the protocols under these attacks. They have also compared the performance of various protocols on the basis of various parameters like End-to-End delay, Throughput etc. But no one has discussed the performance of hybrid protocols like ZRP protocol during Jellyfish Reorder Attack. This paper focuses on analyzing the impact of the Jellyfish Reorder Attack on ZRP protocol using two metrics End-to-End Delay and Goodput.

4. RELATED TERMS

4.1 Jellyfish Attack

There are mainly three types of Jellyfish Attacks: Jellyfish Reorder Attack, Jellyfish Delay Variance Attack and Jellyfish Periodic Dropping Attack. This paper focuses on the first type of Jellyfish Attack. In this attack, the Jellyfish node delivers all the packets to the destination node but instead of forwarding them in FIFO order, it forwards them in random order from the queue. When all the data are clubbed at the destination, garbled data will be obtained. Jellyfish Delay Variance Attack misestimates available bandwidth. It also causes TCP to send traffic in bursts due to “self-clocking” leading to increased collisions and loss. The main drawback of Periodic Dropping Jellyfish Attack is that packet loss occurs periodically and end to end throughput becomes nearly zero.

4.2 ZRP Protocol

ZRP is a hybrid protocol that has advantages of both table driven and on demand driven protocol. The concept of zones is defined in ZRP that are local neighborhoods. Each node may be within diverse overlapping zones and may be of different size. The size of zone is given by the radius of length x where x is the number of hops to the perimeter of the zone. IARP shows the proactive protocol in ZRP and IERP shows the reactive protocol in ZRP.

Already stored routing table is used by proactive protocol immediately if the destination of the packet is in the same zone as that of the source which has generated the packet. If the source and the destination are not in the same zone, reactive protocol takes over to check each successive zone to find out the destination of the packet. Hence the processing overheads are reduced in ZRP.

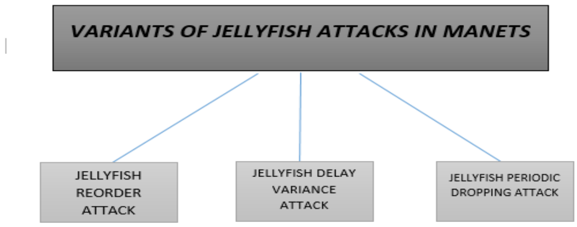
VARIANTS OF JELLYFISH ATTACKS IN MANETS
JELLYFISH REORDER ATTACK
JELLYFISH DELAY VARIANCE ATTACK
JELLYFISH PERIODIC DROPPING ATTACK

Fig 1: Variants of Jellyfish Attack

5. PERFORMANCE PARAMETERS AND SIMULATION RESULTS

NS2 is used as a simulator to carry out this analysis work. One node is taken as an attacker that is reordering the packets. NS2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. Various parameters that are used during this simulation are given in table 1.

Table 1: Simulation Parameters Used

Parameter	Value
Platform	Linux CentOS 5
Area	500 * 500 m
Protocols	ZRP, ZRP with jellyfish attack
Experiment Duration	10 Sec
Packet Interval	0.2 second
Traffic Type	CBR
Mobility Model	Random Way Point
NS Version	NS-2.33
Antenna Type	Omni Antenna
Packet Size	512 bytes

5.1 Performance Metrics Used

The metrics which are used to evaluate performance of MANETs routing protocols are as follows:

1. End-to-End Delay: It is the measured as the total time a data packet takes to reach the destination from the source. The delay time of all the successfully received packets is summed up, and then the average delay time is calculated.
2. Goodput: Goodput is the application level throughput. It is calculated as the number of valid information in bits received at the application layer per unit time.

These two metrics are analyzed in two different scenarios ZRP with an Attack and the ZRP without Attack.

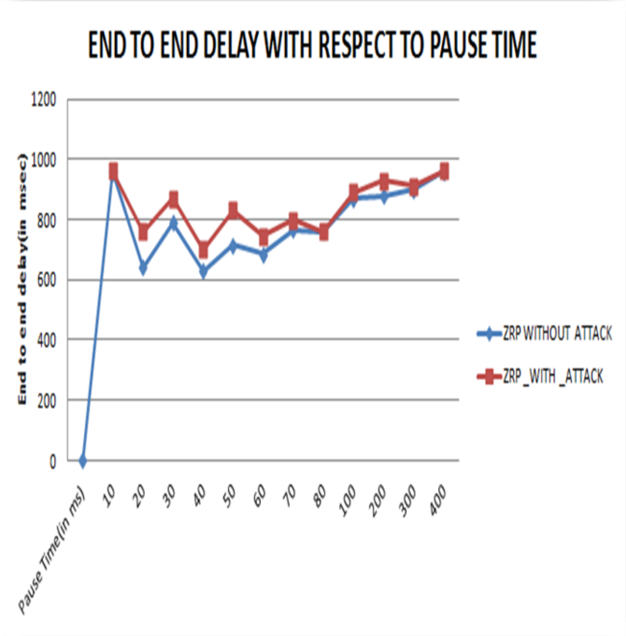

Fig 2 (a): End-to-End Delay v/s Pause Time

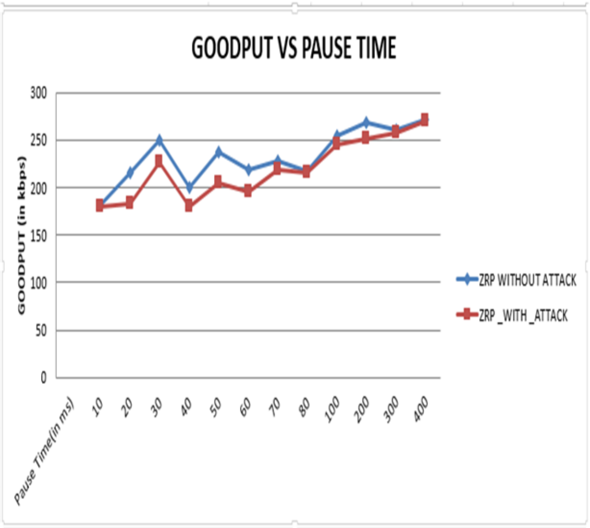

Fig 2 (b): Goodput v/s Pause Time

5.2 Simulation Results

1) Figure 2 (a) shows graph of the average End-to-End delay plotted against the various pause times. It is clear from the graph, after the attack, average End-to-End delay has increased. This is because some amount of time is wasted in reordering the packets by an attacker; hence End-to- End Delay is increased.

2) Figure 2 (b) shows a graph of average throughput v/s pause time. It is evident from the graph that Goodput increases with pause time, but after the attack it starts decreasing. This is because reordering of packets is done by Jellyfish Attacker due to which Goodput decreases.

6. CONCLUSION AND FUTURE WORK

Security is one of the major issues in MANETs. There are different types of attacks that can occur in MANETs and degrade the performance of the network. Hence it is very much necessary to analyze the impact of attacks on networks. In MANETs, there is no inbuilt provision for securing the network from various types of attacks. In their pure form, neither the infrastructure nor the communication protocols have capabilities to detect the attacks present in the network. Therefore, there is a need to work on those attacks which pose most dangerous threats to the network.

In this paper we have analyzed the impact of the Jellyfish Reorder Attack on ZRP using two parameters and it is concluded that, End to End Delay increases and Goodput decreases after the attack. The future work includes analyzing the impact of other types of Jellyfish Attacks like Jellyfish Delay Variance Attack and Jellyfish Periodic Dropping Attack on ZRP. Work can also be extended to propose a detection algorithm to detect Jellyfish Attack in MANETs having less complexity.

7. REFERENCES

[1] Garg, S., & Chand, S. (2014, September). Enhanced AODV protocol for defense against JellyFish Attack on MANETs. In Advances in Computing, Communications and Informatics ICACCI, 2014 International Conference on (pp. 2279-2284). IEEE.

[2] Kaur, A., & Wadhwa, D. S. (2013). Effects of jelly fish attack on mobile ad-hoc network's routing protocols. IJERA, 2248 (9622), 1694-1700.

[3] Patel, H. P., & Chaudhari, M. B. (2013, July). A time space cryptography hashing solution for prevention Jellyfish Reordering attack in wireless ad hoc networks. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[4] Wazid, M., Kumar, V., & Gaudar, R. H. (2012). Comparative Performance Analysis Of Routing Protocols In Mobile Ad Hoc Networks Under Jellyfish Attack. In International Conference on Parallel, Distributed and Grid Computing On IEEE.

[5] Wazid, M., Katal, A., & Goudar, R. H. (2012, December). Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack. In Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on (pp. 435-440). IEEE.

[6] Jain, A. K., & Tokekar, V. (2011, October). Classification of denial of service attacks in mobile ad hoc networks. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on (pp. 256-261). IEEE.

[7] Lakhtaria, K. I. (2010). Analyzing Zone Routing Protocol in MANET Applying Authentic Parameter. arXiv preprint arXiv:1012.2510.

[8] Jayasingh, B. B., & Swathi, B. (2010). A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network. Bharati Vidyapeeth's Institute of Computer Applications and Management, 164.

[9] Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6 (1), 32-46.

[10] Aad, I., Hubaux, J. P., & Knightly, E. W. (2008). Impact of denial of service attacks on ad hoc networks. Networking, IEEE/ACM Transactions on, 16 (4), 791-802.

[11] Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. Mobile Computing, IEEE Transactions on, 6 (5), 536-550.