Detection and Prevention of Jellyfish Attack in AODV Routing Protocol in MANET

Sanjay Kumar
Department of Information Technology
Rajkiya Engineering College, Azamgarh, India

Abstract

Research in the field of Mobile Ad-hoc Network (MANET) has been increasing over the years due to its various applications and the need of communication in mobile devices. Conversely, as compared to wired networks or infrastructure based wireless networks; MANET is mainly vulnerable to security attacks due to its principal characteristics such as no decided boundaries, changing topologies, finite bandwidth, energy constraint and absence of centralized administration. The JellyFish attack is one such security attack. The JellyFish attack is a denial of service attack and also a kind of passive attack that is hard to detect. It creates delay of data packets, before their transmission and reception in the network. In this paper, we propose a solution to the JellyFish delay variance attack in ad-hoc on demand distance vector (AODV) routing protocol for MANETs.
Keywords: AODV, Mobile Ad-hoc Network, JellyFish Attack

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is an infrastructure- less group of mobile nodes that can randomly change their physical positions in order to provide these networks a dynamic topology, thus forming wireless links with bandwidth constrains [5]. These wireless nodes have the capability of communicating with each other without any centralized administration. MANETS have the property that the nodes can move freely and can get organized randomly amongst themselves. Communication in mobile ad-hoc networks takes place by using multiple hops for establishing a path. In case two neighboring mobile nodes lie within the transmission range of each other, they communicate directly, otherwise, the nodes in between are involved in forwarding the packet. In MANET, every node has the liberty to move in or out of the network, independent of the other nodes in the network. Thus it is required that the nodes establish routing among themselves with dynamism and form the network as and when required. Routing Protocols such as Dynamic source Routing (DSR), Destination Sequenced Distance Vector Protocol (DSDV), Ad hoc on Demand Distance Vector (AODV) are used to forward the packets from one node to another node and to create connections in the network.

Due to the lack of a central administration of the network, the nodes themselves are responsible monitoring and management of the network. A number of routing protocols have been proposed for MANETs, which have different methods for finding a new route and also maintaining a route considering the mobility of the nodes. The routing protocols have been broadly classified [1] into (a) proactive routing protocols such as WRP [7], FSR, CGSR [9], DSDV [6], (b) on-demand routing protocols like AODV [8], DSR [10], TORA and hybrid routing protocols like ZRP [11]. Proactive routing protocols maintain the information of the network topology in routing tables which are updated. Whenever a node requires a path to a destination it runs a path finding algorithm as per its routing table. Reactive (on-demand) routing protocol searches for and establishes a path as and when needed. Hybrid routing protocols are a combination of the features of the proactive as well as reactive protocols. The hybrid protocols use reactive routing when the destination lies within the range of the nodes and employ proactive routing when the destination lies outside the range.

The basic characteristics of MANETs make them more exposed to attacks. These attacks are of two types, active attacks and passive attacks [12].

A passive attack does not affect the normal working of a network. An attacker aims to obtain the data without manipulating it. Hence, it is difficult to detect passive attack because the network functions ordinarily. The active attacks are classified into internal attacks and external attacks. When the attacker node belongs to external network it is called external attack while an attack from the node inside the network is known as an internal attack. Jelly fish attack is a passive attack as well as a denial of service attack. Denial of Service attack is an attack which limits the availability of the nodes of a network. In JellyFish attack, a malicious node intrudes into the network, after which it delays data packets pointlessly for some random amount of time before it forwards them [13]. As a result of this attack, increased end-to-end delay occurs in the network. So the network performance in terms of throughput decreases significantly. JF attack is further categorized as – JellyFish Periodic Dropping attack (dropping the data packets), JellyFish Reorder attack (changing the order of the data packets) and JellyFish Delay Variance attack (randomly delaying packet) [2].

In this paper we propose a solution to the JellyFish delay variance attack in ADOV routing protocol. Our paper is organized in the following manner. Section II presents overview of AODV routing protocol and JellyFish attack. The related literature survey is discussed in Section III. Section IV describes the proposed solution. We finally conclude in Section V.

II. AODV ROUTING PROTOCOL AND JELLYFISH ATTACK

The AODV routing protocol [8] is an on-demand routing protocol to discover routes. Only when it is required by a source node to send data packets, it finds a route to the destination. It identifies the most recent path using the destination sequence number. The biggest destination sequence number shows the newest route to the destination node, which is established by the source node for transmitting the data. The information of the next hop for each data transmission is stored not only by the source node but also the intermediate node. Initially, the source node broadcasts a RREQ packet in the network when it requires to establish a route to the destination node for transmission of data packets. On receiving a RREQ, an intermediate node may either forward it to the next node or it may prepare a RREP message provided there exists valid route to the destination node. The intermediate node or the destination node itself unicasts RREP message back to the source node following the already recorded path. When a RREP message from an intermediate node having valid route to the destination node or the destination node is received by the source node, a path is established. This is the route discovery process. Route Error (RERR) packets are used for route maintenance process in AODV.

AODV routing protocol may be affected by JellyFish attack. JellyFish attack exploits the vulnerability of (Transmission Control Protocol) TCP. A JellyFish attacker obeys all the rules of the protocol that is why it becomes difficult to detect. TCP is a reliable protocol and before it can send more packets it requires an ACK. In the JellyFish delay variance attack there is a delay before the packet is forwarded. As a result, TCP does not receive an ACK within a specific time period and resends each packet. Thus, the network congestion increases and the throughput decrease.

In this manner, a Jellyfish attacker node is not able to enter the transmission path.

III. LITERATURE SURVEY

Earlier the work in the realm of security issues in MANETs has been based on reactive routing protocols like Ad-Hoc on Demand Distance Vector (AODV). Several kinds of attacks have been studied and the ways to thwart these attacks have been devised. In Aad et al. (2008) [14], the authors propose protocol compliant attacks for closed loop flow and called them JellyFish attack. The authors present how these attacks detect the vulnerabilities in flow control and congestion control in TCP and use them to reduce the throughput of the network. Authors in Wazid et al. (2013) propose efficient TCP, a better version of TCP, to diminish the impact of JellyFish delay variance attack. It enables selective acknowledgement if jellyfish attacker is there and disables fast retransmission in TCP [4]. Although, not much improvement is there in performance under JellyFish attack efficiently because the selective ACK enhances the performance even in ordinary network with no attacker node present. Kaur et al (2015) propose a selective node participation approach for JellyFish delay variance by using temporarily ordered routing protocol (TORA) [3]. In Jaya Singh et al (2010), they develop a method that identifies the JellyFish attack at a node and that can be efficiently deployed at all the other nodes [15]. Kumar et al (2015) present an in depth study of JellyFish delay variance attack and its impact on the variants of TCP [16]. In Aad et al. (2004), the authors describe a denial of service structure for Jellyfish and black hole attacks [17].

Our Proposed solution detects the presence of a JellyFish attacker node, if any, in the network and removes it from the path connecting the source and destination nodes. Therefore the network throughput increases.

IV. PROPOSED SCHEME FOR THE JELLYFISH NODE DETECTION

We propose a procedure for AODV routing protocol, which is aimed at detecting the JellyFish delay variance attacker node in the path used to forward data packets. When the source node sends the first packet to the neighboring node, after the route discovery, it records the time of sending the packet and the sequence number. Then it records the time of receiving the ACK of that packet. The difference in the two values of time □ is given by Time of receiving ACK minus Time of sending the packet. This is compared to a maximum value of time which is ideally taken by the nodes. If the value of □□is greater than the maximum value then the receiver is a JellyFish attacker node and its flag value is set to 1. This maximum value is based on the propagation delay, link delay etc. This process is continued for every node until it is known that which node is causing a delay of the packet. Once the JellyFish attacker node is identified, a path that does not include this node is chosen for communication. In this manner, a Jellyfish attacker node is not able to enter the transmission path.

The Proposed Algorithm is as follows:

Finding JellyFish node

1) for source node:
2) Send first data packet.
3) Record the sending time and sequence number.
4) Record the time of receiving ACK of that packet
5) Calculate the difference in the two values of time:

$$\tau = \text{Time of receiving ACK} - \text{Time of sending the packet}$$

6) if (□ > maximum value)
7) Receiver is a JellyFish attacker node.
   Set flag = 1.

8) Repeat 2-6 for all other nodes until JellyFish node is found.

Prevention of the JellyFish attacker node from entering into forwarding path

- for RREP received from a node.
- if (flag == 1) for that node. Sender is a JellyFish attacker node.
- Reject RREP.
- Choose another path.

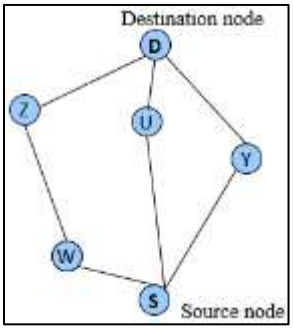

Fig. 1: Detection of JellyFish attacker node

Consider the scenario shown in Fig. 1; node *S* is the source node which wants to communicate to the destination node *D*. *S* broadcasts a RREQ packet in the network and recieves the RREP packet to establish a valid route to the destination node *D*. Suppose that node *S* sends a packet along node *U* which is the JellyFish attacker node. The source node records the value of sending time of first data packet to *U* and receiving time of acknowledgement from *U* and compares their difference with the maximum value. If it is found to be greater than the maximum value, node *U* is identified as JellyFish attacker node and its flag is set to 1. Now, node *S* will take an alternate path to communicate with *D* and detach node *U*. Node *S* starts a new route discovery process to *D* and rejects a RREP from a node with flag value 1.

V. CONCLUSION

In our paper, we have suggested a solution to the problem of JellyFish delay variance attack which is a security concern in MANETs. We have proposed a simple way to thwart this problem. In future, we will encompass our detection method's accuracy by using simulation observations. The simulation results will show effectiveness of the proposed mechanism.

REFERENCES

[1] Ashish Srivastava, Atul Mishra, Bikash Upadhyay and Akhilesh kumar Yadav "Survey and Overview of Mobile Ad-hoc Network Routing Protocols", IEEE International Conference on Advances in Engineering &Technology Research (ICAETR - 2014), August 01-02, 2014.
[2] M. Wazid et aI., "Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under JellyFish Attack", in 2nd IEEE Int. Conf. Parallel Distributed and Grid Computing (PDGC), Solan, H.P., 2012, pp. 147 -152.
[3] Amandeep Kaur, Deepinder Singh Wadhwa, "Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols", Sep-Oct 2013.
[4] Mohammad Wazid et aI., "E-TCP for Efficient Perfonnance of MANET under JF delay variance Attack" in IEEE Conf. Information & Communication Technologies (lCT), JeJu Island, 2013, pp. 145 -150
[5] Patroklos G. Argyroudis and Donal O'Mahony, "Secure Routing for Mobile Ad-hoc Network," IEEE Communication Surveys and Tutorials, 2005, pp. 2-21.
[6] C. K. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of ACM SIGCOMM 1994, August 1994, pp. 234-244.
[7] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, October 1996, pp. 183-197.
[8] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, February 1999, pp.
[9] C. C. Chiang, H. K. Wu, W. Liu and M. Gerla, "Routing in Clustered Multi-Hop Mobile Wireless Networks with Fading Channel", Proceedings of IEEE SICON 1997, April 1997, pp. 197-211.
[10] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Kluwer Academic
[11] Z. J. Hass, "The Routing Algorithm for the Reconfigurable Wireless Networks", Proceedings of ICUPC 1997, Vol. 2, October 1997, pp. 562-566.
[12] C. Siva Ram Murthy and B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall, 2004
[13] Amandeep Kaur, Deepinder Singh Wadhwa, "Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols", Sep-Oct 2013.
[14] Aad I, Hubaux J-P, Knightly E. Impact of denial of service attackson ad hoc networks. IEEE/ACM Trans. Netw 2008; 16(4):791e802.
[15] Jayasingh. B. B. and Swathi B "A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network." Bharati Vidyapeeth's Institute of Computer Applications and Management. pp. 164, 2013.
[16] S. Kumar, Implementation of delay variance attack using video streaming in MANET, Optik - Int. J. Light Electron Opt. (2015).
[17] Aad I, Hubaux J-P, Knightly EW. Denial of service resilience in ad hoc networksi. In: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, MobiCom '04; 2004. p. 202e15.