ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Defending Against Intrusion and Prevention of Jellyfish Attack Approach for Detecting Malicious Node in MANET

K. Naveeda[1], V. Nithya Poorani[2]

PG Student [CS], Dept. of ECE, Pavendar Bharathidasan College of Engg. & Tech., Tiruchirappalli, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, Pavendar Bharathidasan College of Engg. & Tech., Tiruchirappalli, Tamilnadu, India[2]

ABSTRACT: Mobile ad hoc networks (MANETs) are vulnerable to various types of attacks due to inherently in-secure wireless communication medium and multihop routing communication process. In this paper, we analyze the behavior and impact of JellyFish attack over MANETs. We have implemented and evaluated all three variants of JellyFish attack namely JF-reorder, JF-delay and JF-drop through simulation processes. These attacks exploit the behavior of closed loop protocols such as TCP and disturb the communication process without disobeying any protocol rules, thus the detection process becomes difficult. Consequently, traffic is disrupted leading to degradation in network throughput. Through extensive simulation results that are obtained using an industry standard scalable network simulator called NS2, impact of these attacks in terms of network throughput, overhead incurred and end-to-end delay is analyzed and used for devising detection and countermeasure. We have proposed a light-weight direct trust-based detection (DTD) algorithm which detect and remove a JellyFish node from an active communication route. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the existing and compared with proposed JF detection scheme in terms of packet delivery ratio and routing overhead.

KEYWORDS: CBDS, JellyFish attack, malicious node, mobile ad hoc network (MANET)

I.INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Many research works have focused on the security of MANETs.

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In blackhole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path to the destination,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. In grayhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network.

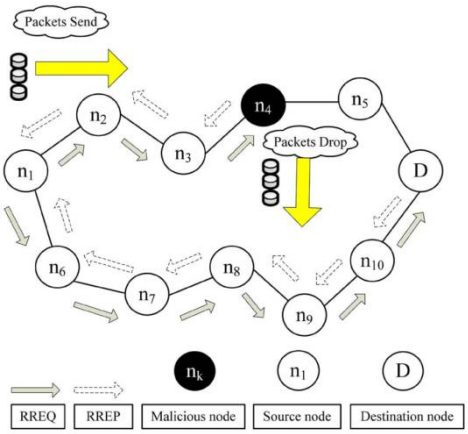

Fig.1: Blackhole Attack

It then selectively discards/forwards the data packets when packets go through it. In this paper, our focus is on detecting grayhole/collaborative blackhole attacks using a dynamic source routing (DSR)-based routing technique.

II. EXISTING SYSTEM

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks[6].

In MANETs, a malicious node in the network can lead to incorrect network behavior using following methods:

- Malicious node generates tremendous amount of junk packets in the network preventing legitimate nodes from gaining access to the communication channel for transmission of data or control messages.
- Malicious node generates control packets carrying incorrect topological information leading to false entries in other nodes' routing table.
- After receiving control messages, a malicious node can delay the dissemination process. As a result, the information in these control messages might become incorrect as it may not correspond to recent change in the network topology.

A large fraction of the existing MANET attacks uses one or more of the above three methods. Following is a comprehensive list of known MANET attacks.

Worm Hole attack [1] It is one of the most sophisticated and rigorous attacks in MANETs. Here, two attackers place themselves strategically in the network. Once strategically placed, the attacker pair advertises path through them as the shortest one. This is to ensure traffic diversion through these nodes. The attackers can eavesdrop the communication through them and record it for future use. The Worm Hole attacker creates a tunnel in order to record the ongoing communication and traffic at one network position and channels it to another position in the network.

Black Hole attack [2]: A malicious node (called blackhole) sends fake routing information, claiming that it has an optimum route and causes other nodes to route data packets through itself. For example, in AODV (Ad-hoc On-demand Distance Vector) [3], the attacker can send a fake RREP1 (including a fake destination sequence number equal to or higher than the one contained in the RREQ2) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Once paths have been established, blackhole simply drops all packets leading to a DoS attack.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Sybil attack: In this attack [4], the attacker assumes multiple identities and uses these identities to launch a distributed DoS attack, establish non-existent routes disrupting traffic, fabrication of control/data messages, etc. Multiple identities help the attacker in evading detection.
Grayhole attack: The attacker node drops some packets that pass through it.
Selfish Node Misbehaving: In MANETs, the nodes participate in a collaborative manner to forward packets to other nodes. A node refusing to forward packets in order to conserve its limited resources is termed a 'selfish node'. This selfishness causes network and traffic disruptions [5].
In addition, some of these methods require specific environments or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories.

1) Proactive detection schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage [7].

2) Reactive detection schemes are that trigger only when the destination node detects a significant drop in the packet delivery ratio.

Among the above schemes are the ones previously proposed, in which considered as benchmark schemes for performance comparison purposes. In 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received [8].
The disadvantage of the system are described as follows [10-12]: a) Lack of central point for authentication, network management and authorization facility, requirement of mutual trust based communication (i.e., multihop communication), dynamic topology, and limited resources i.e., hard to implement a countermeasure algorithm efficiently due to low processing power and battery life. b) The effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

III. PROPOSED APPROACH

A MANET topology can be viewed as an undirected graph G = {V,L}, where V = {v1,v2,v3…vn} is the set of nodes and L = {l1,l2,l3/lm} is the set of links in the network. A link between two nodes is active, if they are in each others' transmission range. In a multihop MANET, there may be k different routes between a source node (S) and a destination node (D). Let R(S->D,t) = R1 (S -> Dm,t) …. Rk (S ->D,t) be the set of routes from S to D at time t. For ith route Ri (S -> D,t) S[dzigrarr]n[dzigrarr]D, n being the intermediate node. Index t represents that for a given S and D, k, R(S -> D) and n change with time as the network topology is dynamic.
Let M= {m1, … mk, … ml}, mk, V, 1 < k < q represent a set of malicious nodes in the network. For attack to take place at any given time, M not equal to packets size, while q > 1. A JF-node always participates in the route discovery by forwarding the control messages during the route discovery process to increase its chances to become an intermediate node on as many selected routes as possible. Once a JF-node becomes an intermediate node on a selected route, it launches any JellyFish attack variant to degrade the network performance. Although, the JF-node is unable to distinguish the received packet type (i.e., TCP or UDP) as the packets are encrypted by upper layers, it can still perform the attack irrespective of this knowledge. According to the MAC 802.11 specifications, each data packet is transmitted to the next hop using RTS-CTS-DATA-ACK mechanism. At MAC layer, each node waits for the specified time for the ACK of recently sent data packet before transmitting the next one. A link for the next-hop towards destination is considered broken if no ACK is received for a data packet even after its re-transmission limit has been reached.
It is assumed that only protocol compliant attacks take place. JellyFish (JF) attacks are independent of routing layer and MAC layer protocols because they are targeted to disrupt the functionality of TCP protocol. Our simulations, however, use ad-hoc on-demand distance vector (AODV) as routing protocol and IEEE 802.11 as MAC protocol. Finally, it has been assumed that each node monitors the transmission of its neighbour nodes in promiscuous mode i.e., a node can overhear and process the transmissions not designated for it. This is required for our proposed detection mechanism.

Jellyfish Attack

JellyFish attack maintains compliance with both the control and data protocols to make its detection and prevention difficult. [12] Due to no functional distinction among mobile nodes in MANETs, an intermediate node can introduce a

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

critical vulnerability for TCP congestion control mechanism. Such a compromised/malicious node alters its forwarding behavior as described in following variants of JF attacks.

Jellyfish Reordering Attack

As the name suggests, an attacker node reorders some of the packets before forwarding them. As ACKs of some of reordered packets are not received in time, the sender need to retransmit them again. From receiver's perspective, each time a packet is received, an ACK is generated. For out-of-order packets, sender shall received duplicate ACK messages. TCP initiates its flow control mechanism if these duplicate ACK messages exceed a threshold (3 in our case). In our implementation of JF reordering attack, the JF node creates a reordering buffer of size k in its input queue as shown in Fig. 2. The data packets in this buffer are reordered before being forwarded. This attack can be implemented in following two ways:

1. Reorder packets in batches of k packets each. Algorithm includes three steps e
   (1) Reorder current batch of k packets,
   (2) Forward the reordered batch and
   (3) Wait for next batch. In our implementation of JF-reorder attack, we have used this method.
2. Reordering is done using a sliding window of k size and each time a packet is sent, this window is shifted by one packet. Reordering is initiated on available k packets each time a packet is about to leave the reordering buffer.

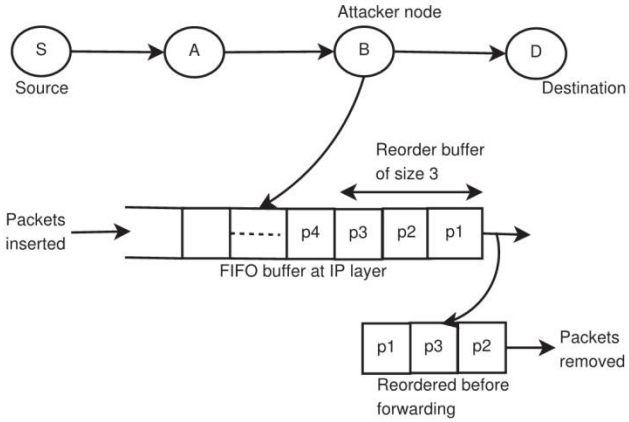

Fig. 2: Reordering Attack

The packet reordering results in an increase of duplicate ACK packets sent by the destination node. When the source receives three consecutive duplicate ACKs, it initiates flow and congestion control mechanism, which eventually decreases the network throughput leading to under utilization of available network resources.

Jellyfish Periodic Dropping Attack

In this attack, JF nodes randomly discard some packets over a specified period during communication process. In this way, incorrect route congestion information is conveyed to TCP, which uses dropping of packets as an indication of congestion on the route. The JF-node may either choose to discard a fraction of packets (e.g., 10 packets from every 100 packets) or may discard all the packets received during a slice of time (e.g., discarding data packets for few milliseconds every second near the TCP sender timeout). This forces TCP to enter the retransmission timeout (RTO) and to increase its RTO value. As the flow becomes stable, attacker repeats the above strategy to sustain the attack and keep the data flow rate low. An instance depicting the periodic drop attack is shown in Fig. 3.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

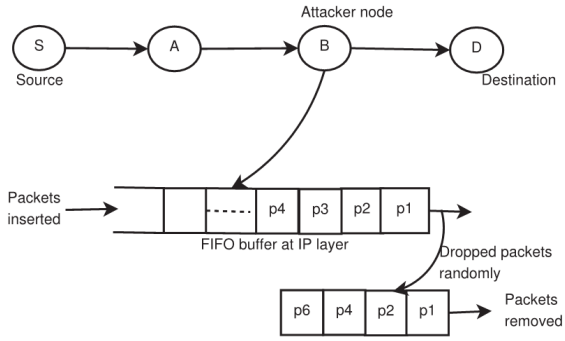

Fig. 3: Periodic Dropping

As JF-node starts discarding packets for some duration, the sender will eventually enter in timeout. TCP handles the timeouts by entering in slow start phase leading to decrease in the network throughput. The throughput decreases as the frequency of packets dropped by the attacker node increases. To maximize the impact of the attack, a JF-node will drop packets as soon as the TCP sender exits its slow start phase. Due to this, the flow will always be in a fragile slow-start state.

Jellyfish Delay Variance Attack

Round trip time (RTT) of data packets vary considerably due to congestion. Though TCP has a flow control mechanism to adapt to the changes, it cannot determine if the change in RTT is due to dynamic wireless topology, network congestion or JellyFish attack. Also, changes in RTT force TCP to increase RTO. By delaying packets randomly, a JF node can initiate this attack resulting in.

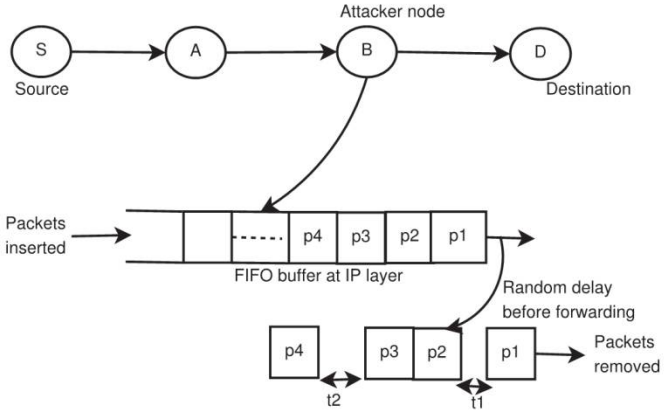

Fig. 4: Delay Variance

- Self-clocking of TCP leading to increased collisions and data packet loss,
- Wrong estimation of the available bandwidth for delay based congestion control protocols such as TCP Westwood and TCP Vegas,
- Very high RTO estimate thus decreases network throughput due to delayed detection of congestion in the network.

In delay variance attack, JF nodes are selfishly delaying packets. Resultant increase in RTT misleads the sender TCP, which increases its congestion window size and sends traffic in bursts. It will eventually result in more collisions. Fig. 4 shows an instance of our implemented delay variance attack.

IV. PERFORMANCE EVALUATION

A. Simulation Parameters

The NS-2 simulation tool is used to study the performance of our CBDS scheme. We employ the IEEE 802.11 MAC with a channel data rate of 11 Mb/s. In our simulation, the CBDS default threshold is set to 90%. All remaining

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

simulation parameters are captured below discussion. The network used for our simulations is depicted in [11-12] output screenshots; and we randomly select the malicious nodes to perform attacks in the network.

SIMULATION PARAMETERS

Parameter	Value
Simulator	NS2
Simulation time	10s
Area	1200X1200
Number of node	30
Physical Layer	IEEE 802.11
Routing protocol	AODV
Mobility model	Random way point
Radio type	802.11a/g
Transmission rate	10 packets/s
Packet Size	512/ 1024
Pause time	0s

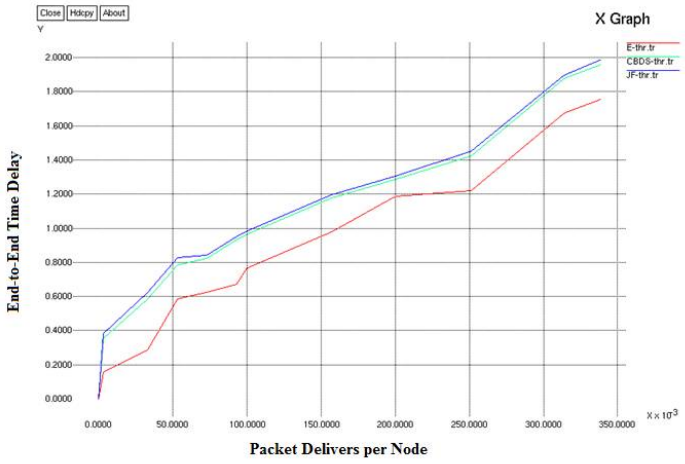

Fig. 5: Throughput ratio between time and data packets

The Fig.5 and Fig.6 shows the comparison of existing and proposed to shows the Packet Delivery Ration, End-to-Delay of simulation parameters.
Finally, the results obtained from this module is compared with previous results and comparison X-graphs are plotted. Form the comparison result, final RESULT is concluded.

V. CONCLUSION

In this paper, a detailed performance evaluation of JellyFish attack (JF-reorder, JF-delay and JF-drop) over AODV based MANETs is presented. Based on the simulation results generated over various MANET scenarios with varying number of attackers, intermediate hops and attack parameters, it has been observed that JellyFish attack causes network performance degradation in terms of network throughput, end-to-end delay and control overhead.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

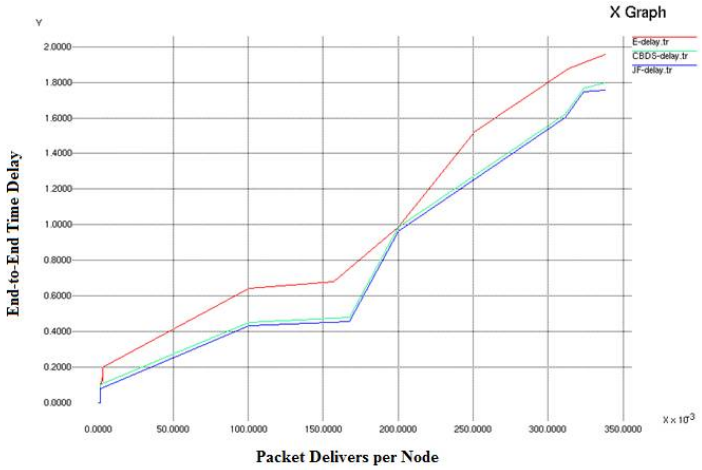

Fig. 6: Comparison graph of previous and proposed method

In this paper, there is analysis of performance of AODV protocol without jellyfish attack, with jellyfish attack and the proposed prevention scheme against jellyfish attack. Ad-hoc network play very critical role in many fields ranging from military applications to other house hold applications. It is very vital to handle security in data transmission in such cases which is very much challenging due to their infrastructure less behavior. It is very much clear that the performance of the proposed work — Defending against Intrusion and Prevention of Jellyfish Attack Approach for Detecting Malicious Node in MANET performs better.

REFERENCES

[1] Hu Y-C, Perrig A, Johnson D. "Wormhole attacks in wireless networks". IEEE J Sel Areas Commun 2006; 24(2):370e80.
[2] Mishra A, Jaiswal R, Sharma S. "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network". In: IEEE 3rd International Advance Computing Conference (IACC); 2013.
[3] Perkins C, Royer E. "Ad hoc on-demand distance vector routing". 1999.
[4] Abbas S, Merabti M, Llewellyn-Jones D, Kifayat K. "Lightweight sybil attack detection in MANETs". IEEE Syst J 2013;7(2):236e48.
[5] Dasilva MVL, Eltoweissy M. "A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In: International Conference on Mobile and Ubiquitous Systems". Networking and Services; 2005.
[6] Nguyen HL, Nguyen UT. "A study of different types of attacks in mobile ad hoc networks". In: 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE); 2012.
[7] Wazid M, Katal A, Sachan R, Goudar R. "E-TCP for efficient performance of MANET under JF delay variance attack". In: IEEE Conference on Information Communication Technologies; 2013. p. 145e50.
[8] Nadeem A, Howarth M. "A survey of MANET intrusion detection & prevention approaches for network layer attacks". IEEE Commun Surv Tutor 2013;15(4):2027e45.
[9] Jayasingh BB, Swathi B. "A novel metric for detection of jellyfish reorder attack on ad hoc network". BVICAM Int J Inf Tech 2010;2(1):20.
[10] Abdelaziz A, Nafaa M, Salim G. "Survey of routing attacks and countermeasures in Mobile ad hoc networks". In: 15th International Conference on Computer Modelling and Simulation (UKSim); 2013.
[11] Mishra A, Jaiswal R, Sharma S. "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRItable in ad hoc network". In: IEEE 3rd International Advance Computing Conference (IACC); 2013.
[12] Mani P, Kamalakkannan P. "Mitigating selfish behavior in mobile ad hoc networks: A survey". Int J Comput Appl 2013;73(22):1e7.