IJMRT: Volume (1), Issue 1, May 2019

ISSN (Print) : 2663-2381
ISSN(Online) : 2663-4007

International Journal of Multidisciplinary Research Transactions

(A Peer Reviewed Journal)

www.ijmrt.in

An Efficient Trust-Based Detection System for Defending Intrusion and JF Attack in MANET

P Subramanian

PG Student, Department of Electronic and Communication Engineering, Anna University, BIT Campus, Tiruchirappalli, Tamil Nadu, India

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 IDS outperforms the existing and compared with proposed JF detection scheme in terms of packet delivery ratio and routing overhead.

Keywords: Grayhole attacks, malicious node, mobile ad hoc network (MANET), Instruction detection.

1. 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.

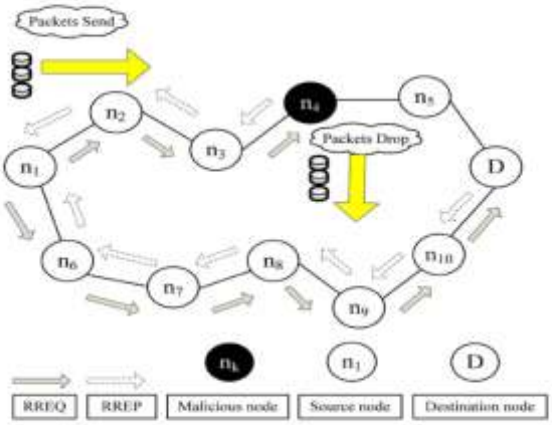

Fig.1 Blackhole Attack

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole (known as variants of black hole attacks). In black hole attacks a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. 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. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, 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.

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, a node transmits a malicious broadcast informing that it has the shortest path to the destination, 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.

2. Related Works

With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results in the rapid development of the technology. Due to the reason that MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention. In the [5] C. Tsou, J.-M.Chang and H.-C.Chao present the common routing protocols in current such as DSR AODV and so on almost take account in performance. They don't have the related mechanism about detection and response. Aiming at the possible attacks by malicious nodes, based on the DSR protocol, this paper presented a mechanism to detect malicious nodes launching black/grayhole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node.

I. Rubin, A. Behzad, introduce an ad hoe wireless mobile network that employs a hierarchical networking architecture. The network uses high capacity and low capacity nodes. We present a topological synthesis algorithm that selects a subset of high capacity nodes to form. The latter consists of interconnected backbone nodes that intercommunicate across high power links, and also makes use of (airborne, ground and underwater) Unmanned Vehicles (Uvs). We introduce the TBONE protocol to implement the key networking schemes for such a Mobile Backbone Network (MBN). It includes combined network layer operation, i.e. mobile backbone net-work topological synthesis, and MAC layer resource allocation schemes. The TBONE protocol serves to allocate resources across the network to ensure that user applications are granted acceptable quality-of-service (QoS) performance, while striving to ensure a highly survivable and robust backbone-oriented networking architecture. [10]

A mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In the [1] H. Deng, W. Li D. Agrawal study the routing security issues of MANETs, and analyze in detail one type of

attack-the “black hole” problem-that can easily be employed against the MANETs. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.
The effects of jelly fish attack on MANET’s routing protocols. Here four protocols AODV, DSR, TORA and GRP are used. Performance of the network has been evaluated in terms of Data dropped by buffer overflow, Data dropped due to threshold exceeded, Load, Media access delay, Retransmission attempts. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme. [7]

3. Proposed Approach

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 transmit traffic in bursts because of 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.

3.1. Jellyfish Attack in Mobile Ad Hoc Networks

Jellyfish attack maintains compliance with both the control and data protocols to make its detection and prevention difficult. Due to no functional distinction among mobile nodes in MANETs, an intermediate node can introduce a critical vulnerability for TCP congestion control mechanism. Such a compromised/malicious node alters its forwarding behavior as described in following variants of JF attacks.

3.2. 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 receive duplicate ACK messages. TCP initiates its flow control mechanism if these duplicate ACK messages exceed a threshold. 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. 1. 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.

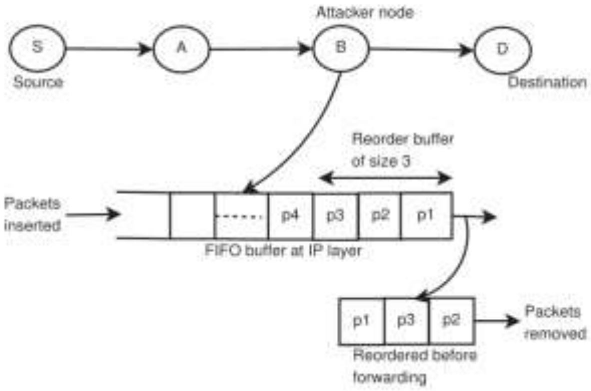

Fig.1 Reordering Attack

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.

3.3. 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.

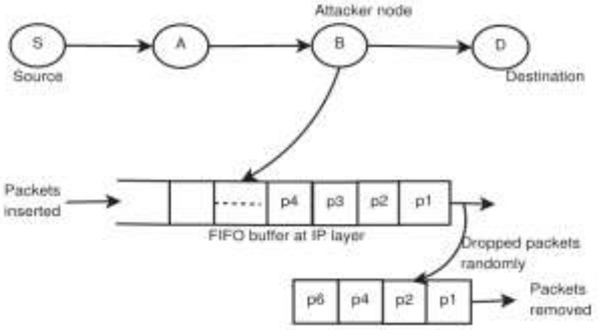

Fig.2 Periodic Dropping

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.

3.4. 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.

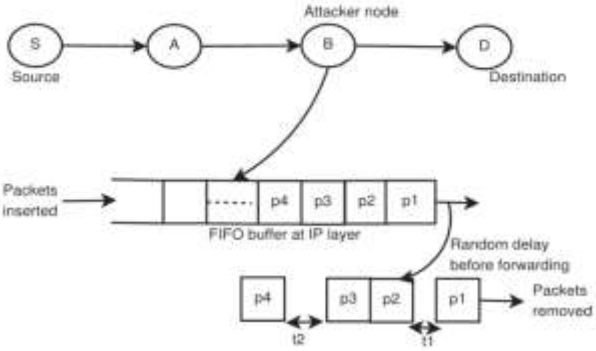

Fig. 3 Delay Variance

- 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. 3 shows an instance of our implemented delay variance attack.

4. Performance Evaluation

4.1. Simulation Parameters

The NS-2 simulation tool is used to study the performance of our jellyfish scheme. In this section, we will present the performance analysis of TCP-SACK under various variants of Jellyfish attack over MANETs. Simulation results using EXata-Cyber3 are obtained on various scenarios; each scenario investigated for changes in performance metrics with increase in number of JF-attackers and hop-length (i.e. intermediate nodes) en-route. In this work, we have used two MANET scenarios for evaluating performance.

4.2. Modules

4.2.1. Implementation of Wireless Network

In this module, a wireless network is created. All the nodes are configured and randomly deployed in the network area. Since our network is a wireless network, nodes are assigned with mobility (movement). A routing protocol is implemented in the network. Sender and receiver nodes are randomly selected and the communication is initiated. All the nodes are configured to CBDS and reverse tracking among all the nodes.

4.2.2. Performance Analysis

In this module, the performance of the network after CBDS is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters are considered here and X-graphs are plotted for these parameters.

4.2.3. Implementation of CBDS *coding scheme*

In this module, to enable all the nodes to get the global AODV, we propose a dynamic threshold algorithm, with an emphasis on calculation the total node packet delivery ration and reverse tracking the node information. The proposed encoding strategy is based on CBDS default threshold coding which has very low complexity. CBDS scheme involves misbehavior nodes in the MANET

4.2.4. Performance analysis

In this module, the performance of the proposed network coding method is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these 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.

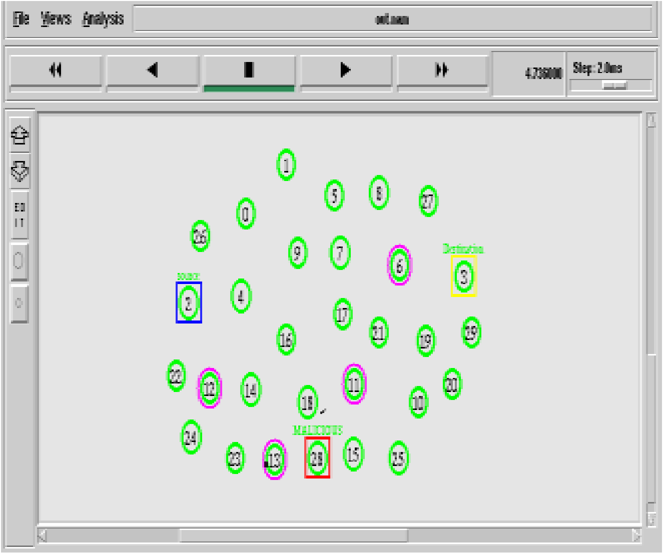

Fig.4 Reroute and Communication Started

Simulation Parameters

Parameter	Value
Application Traffic	*10 CBR*
Transmission rate	*10 packets/s*
Packet Size	*512 bytes*
Channel data rate	*10Mbps*
Pause time	*0s*
Simulation time	*10s*
Number of node	*30*

Area	*1200X1200*
Threshold	*Dynamic*

4.3. Performance Metrics

4.3.1. Packet Delivery Ratio

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, pkt di is the number of packets received by the destination node in the ith application, and pktsiis the number of packets sent by the source node in the ith application.

4.3.2. Routing Overhead

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpkiis the number of control packets transmitted in the ith application traffic and pkti is the number of data packets transmitted in the ith application traffic.

4.3.3. Average End-to-End Delay

This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is di, and the number of packets received by the destination node is pktdi.

4.4.4. Throughput

This is defined as the total amount of data (bi) that the destination receives them from the source divided by the time (ti) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second.

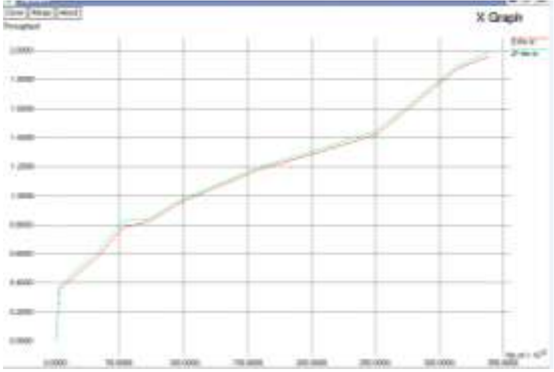

Fig.5 Performance Response

5. Conclusion

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. 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 — Impact of Jellyfish Attack and Approach for Detecting Malicious Node in MANET

REFERENCES

[1]. Deng H, Li W, and Agrawal D (2002), "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10.

[2]. Baadache A. and Belmehdi A. (2010) "Avoiding black hole and cooperative black Hole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1.

[3]. Chang C, Wang Y, and Chao H (2007), "An efficient Mesh-based core multicast Routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239.

[4]. Po-Chun Tsou, Jiann Ming Chang, Han-Chieh Chao and Jiann.-Liang Chen, (2011) "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun, VITAE.

[5]. Wang W, Bhargava B, and Lindeman M,(2009) "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009

[6]. Corson S and Macker J (1999), RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations.

[7]. Johnson D and Maltz D (1996), "Dynamic source routing in ad hoc wireless networks," Mobile Compute., pp. 153–181.

[8]. Rubin I, Behzad A, Zhang R, Luo H, and Caballero E (2002), "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf. vol. 6, pp. 2727–2740.

[9]. Weerasinghe H and Fu H, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.

[10]. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[11]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[12]. H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.

[13]. Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun. vol. 29, pp. 367– 388, 2004.

[14]. W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, 2009, pp. 103–110.

[15]. W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[16]. IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications, pp. 1-445.