Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks

1Syed Atiya Begum  
Assistant professor, CSE Dept  
Adam’s Engineering College  
Paloncha-507115, India  
atiyaice@gmail.com

2L.Mohan  
Assistant professor, CSE Dept  
Adam’s Engineering college  
Paloncha-507115, India  
lavmohan@gmail.com

3B.Ranjitha  
Assistant professor, CSE Dept  
Adam’s Engineering college  
Paloncha-507115, India  
ranjitha.bandi@gmail.com

Abstract-A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless links. 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.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. A Denial-of-service attack is a type of security breach that prohibits a user from accessing normally provided services. The denial of service (DOS) does not result in information theft or any kind of information loss but can nonetheless be very dangerous, as it can cost the target person a large amount of time and money. Denial-of-service attacks affect the destination rather than a data packet or router.

Significant progress has been made towards making ad hoc networks secure and DoS resilient. In this paper, we study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. The first attack we study, called the JellyFish attack, is targeted against closed-loop flows such as TCP; although protocol compliant, it has devastating effects. The second is the Black Hole attack, which has effects similar to the JellyFish, but on open-loop flows. The interesting point to note here is DoS attacks can increase the capacity of ad hoc networks, as they starve multi-hop flows and only allow one-hop communication, yet clearly undesirable situation. Later in this paper we study different techniques to protect our ad hoc networks against these denial-of-service attacks.

Key Words - DoS attacks, TCP, UDP, ad hoc networks, Jelly Fish, Black hole.

I. INTRODUCTION

A mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing and service discovery without the help of an established infrastructure. Nodes of an Ad Hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host’s wireless transmissions. An Ad Hoc network uses no centralized administration.

Significant progress has been made in securing ad hoc networks via the development of secure routing protocols [Destination-sequence Distance Vector (DSDV) protocol, Cluster-Head Gateway Switch Routing (CGSR) protocol, Wireless Routing (WRP) Protocol, Dynamic Source Routing (DSR) Protocol, and Associate Based Routing (ABR) Protocol]. Yet, there remains an indefinite “arms race” in system and protocol design: attackers (or researchers anticipating the moves of attackers) will continually introduce increasingly sophisticated attacks, and protocol designers will continually design protocol mechanisms designed to thwart the new attacks.

The goal of this paper is to quantify via analytical models and simulation experiments the damage that a successful attacker can have on the performance of an ad hoc network and to secure our ad hoc networks against these attacks.
II JELLYFISH AND BLACK HOLE DOS ATTACKS

Security Requirements in MANETs

- Availability
- Authorization and Key Management
- Data Confidentiality
- Data Integrity
- Non-repudiation

A. JellyFish Attack

The key principle that JF use to facilitate the attack is targeting end-to-end congestion control. In particular, many applications such as file transfer, messaging, and web will require reliable, congestion controlled delivery as provided by protocols such as TCP.

JF Reorder Attack:

In this attack JF nodes maliciously re-order packets. In this attack, JF deliver all packets, yet after placing them in a re-ordering buffer rather than a FIFO buffer. Consequently, we will show that such persistent re-ordering of packets will result in near zero goodput, despite having all transmitted packets delivered.

Impact of JF reorder attack:

![Figure 2: JF-reorder effect on throughput](image)

**JF Periodic Dropping Attack:**

The JF attacking nodes drop all packets for a short duration (e.g., tens of ms) once per RTO. Thus, JF are
passive and generate no traffic themselves; like non-malicious nodes, JF drop for only a small fraction of time; yet, with this dropping pattern during a maliciously chosen period, the following behavior results.

**JF Delay Variance Attack:**

Variable round-trip-times due to congestion are an inevitable component of TCP’s operation. Yet, ensuring high performance in the presence of random and high delay variation due to an attacker was clearly not incorporated into TCP’s design. Such a high delay variation can (i) cause TCP to send traffic in bursts due to “self-clocking,” leading to increased collisions and loss, (ii) cause mis-estimations of available bandwidth for delay-based congestion control protocols such as TCP Westwood and Vegas, and (iii) lead to an excessively high RTO value. Indeed, enhancing TCP to combat the effects of non-malicious delay variation to wireless links has been the focus of intense research, as has the development of tools for available bandwidth estimation. Consequently, malicious manipulation of packet delays by the JF delay variance attack has the potential to significantly reduce TCP throughput. Such attackers therefore wait for a variable amount of time before servicing each packet, maintaining FIFO order, but significantly increasing delay variance.

**B. Black hole Attack**

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In a flooding-based protocol such as AODV the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

**III TECHNIQUES TO PROTECT AD HOC NETWORKS AGAINST DOS ATTACKS**

The research effort, funded by DARPA/ATO's Fault Tolerant Networks (FTN) program, developed a ground breaking approach for protecting ad hoc networks against denial of service (DoS) attacks. We present a set of design techniques to protect ad hoc networks against denial of service attacks. These techniques seek to limit the damage sustained by ad hoc networks from intrusion attacks and allow for continued network operation at an acceptable level during such attacks.

- Different proposed techniques are:
  - Flow-Based Route Access Control (FRAC)
  - Multi-Path Routing
  - Source-Initiated Flow Routing
  - Flow Monitoring
  - Fast Authentication
  - Sequence Numbers

**Flow-Based Route Access Control (FRAC):**

A flow is a sequence of packets from a source node to a destination address. With FRAC, each router in an ad hoc network maintains an access control rule base that defines the list of authorized flows that may be forwarded by the router. Packets belonging to unauthorized flows are simply dropped by the router.

**Multi-Path Routing:**
Multi-path routing refers to the ability of ad hoc routing algorithms to discover and maintain all legitimate routes (or paths) for a data flow. This is essential if an ad hoc network is to be able to tolerate intrusion induced path failures of the type described earlier.

**Source-Initiated Flow Routing:**

Each of these alternate paths between the source and the destination is associated with a path label that identifies the path. The source inserts the path label in each data packet. Routers examine the path label in each data packet to determine the next hop.

**Flow Monitoring:**

Flow monitoring enables the detection of path failures resulting from the various types of intrusion attacks. The routing function in the source node of an information flow periodically sends flow status messages to the routing function on the destination node. The flow status message includes within it, the number of packets associated with this flow that has been transmitted by the source since the last status message. Status messages also carry sequence numbers. The flow status is encrypted and protected by a digital signature to protect the integrity of the message.

**Fast Authentication:**

Fast authentication is a lightweight mechanism for authenticating data packets flowing through a wireless router that relies on placing the path label of a packet at a node specific secret location within the packet. Fast authentication periodically changes the per node secret location of path labels to reduces the susceptibility of this mechanism to traffic analysis.

**Sequence Numbers:**

Fast authentication and FRAC are not sufficient to counter replay attacks. Sequence numbers provide a counter measure for this. Similar to the technique used for embedding path labels within the data packet, the source inserts sequence numbers within the data packet at node-specific secret locations for the nodes in the path between the source and the destination.

**IV RELATED WORK**

Throughout the exhaustive research and readings in the field of mobile Ad Hoc networks and the many security challenges and issues related to their routing protocols, analysis of various secure routing protocols proposed in the literature has been performed.

As a result, in the table 2, a comparison between some of the most established secure routing protocols with respect to some performance and security parameters is given so that to facilitate the choice of one of them to work on.
MANETs have several significant characteristics and challenges. They are as follows:

- Dynamic topologies: Nodes are free to move arbitrarily. Thus, the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- Bandwidth-Constrained, Variable Capacity Links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications, after accounting for the effects of multiple access, fading, noise, and interference conditions, is often much less than a radio’s maximum transmission rate.
- Energy-Constrained Operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation.
- Security: Mobile wireless networks are generally more prone to physical security threats than fixed-cable nets. The increased possibility of eavesdropping, spoofing, selfish behavior and denial-of-service attacks should be carefully considered.

These characteristics and challenges create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet.

V CONCLUSION

In this paper, we studied a novel DoS attack perpetrated by JellyFish: relay nodes that stealthily misorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. We studied different techniques to protect our ad hoc networks against DOS attacks. It seeks to limit the damage sustained by ad hoc networks from intrusion attacks and to allow for continued network operation at an acceptable level during such attacks. These techniques are designed to handle attacks on the routing traffic as well as the data traffic in ad hoc networks thereby providing a comprehensive defence against intrusion attacks. Since these techniques are routing algorithm independent, this approach may be viewed as providing general design principles and techniques that can be incorporated within a number of existing ad hoc routing algorithms to make them robust to Denial-of-Service attacks.

REFERENCES

