ISSN 2229-5518

Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks

Syed Atiya Begum

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, a capacity-maximizing, yet clearly undesirable situation.

Later in this paper we study different techniques to protect our ad hoc networks against these denial-of-service attacks. The mechanisms described here 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. These mechanisms are designed to handle attacks on the routing traffic as well as the data traffic in ad hoc networks thereby providing a comprehensive defense against intruders. These techniques are routing algorithm independent. These mechanisms may be viewed as providing general design principles and techniques the can be incorporated within a number of existing ad hoc routing algorithms to make them robust to intrusion attacks.

Index Terms— DoS attacks, Resilience, TCP, UDP, ad hoc networks ,Jelly Fish, Black hole.

1. 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.

Significant progress has been made in securing ad hoc networks via the development of secure routing protocols [Destination-sequenced 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.

Techniques for protecting the routing infrastructure in global Internet that have been proposed in recent years are not adequate for ad hoc network environments. As described later, ad hoc networks face threats that are not encountered in traditional network environments. These unique threats induce types of network failure modes that cannot be handled by security services designed for the global Internet infrastructure. This paper presents a set of design Techniques for resilience of DoS attacks, to protect ad hoc networks against denial of service attacks.

A MANET Example:

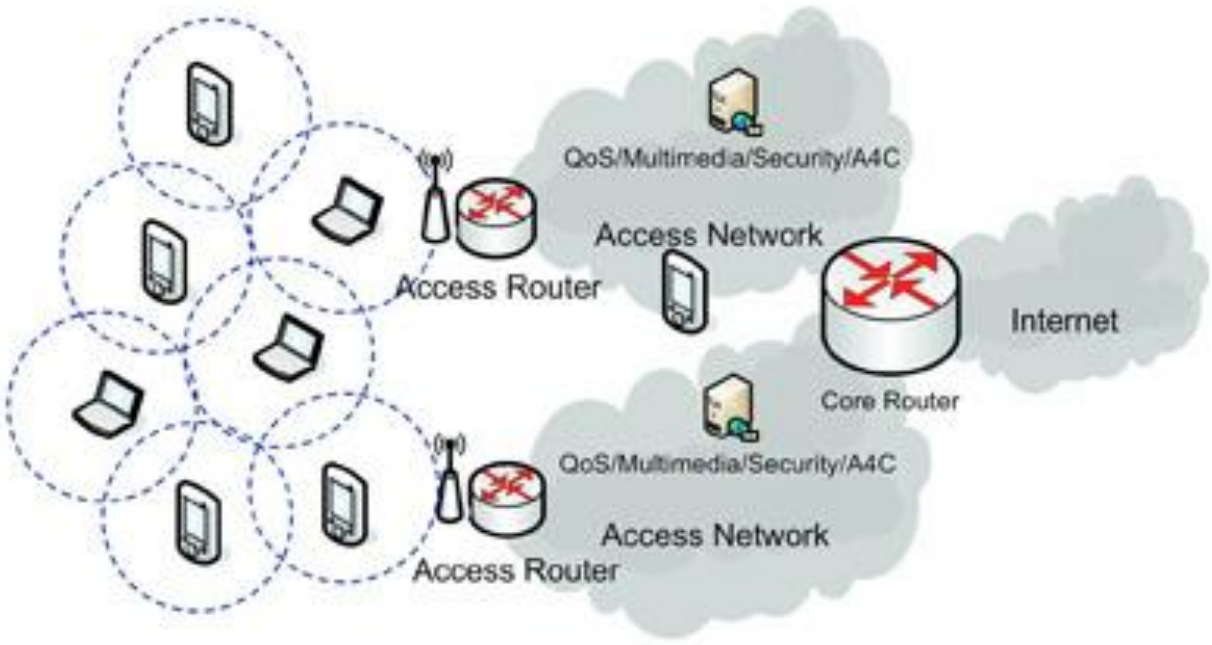

Figure 1. Mobile Ad Hoc Network

2. Jellyfish And Black Hole Dos Attacks

Security Requirements in MANETs

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

2.1 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:

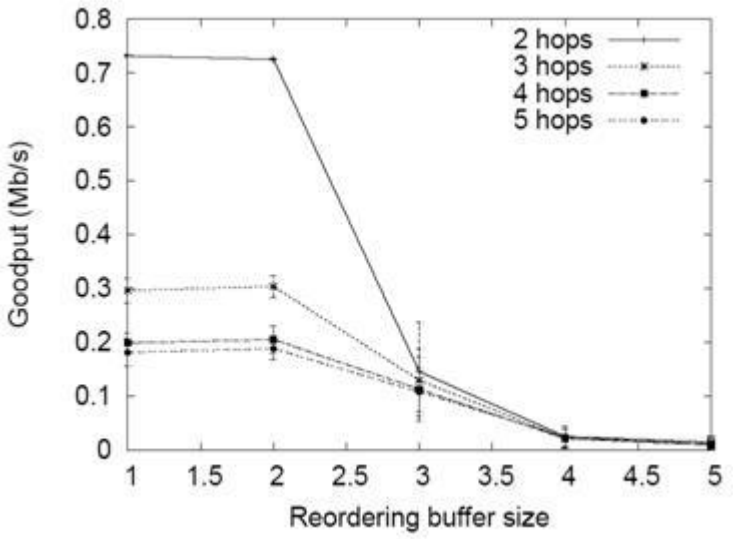

Figure 2. JF-reorder effect on throughput

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.

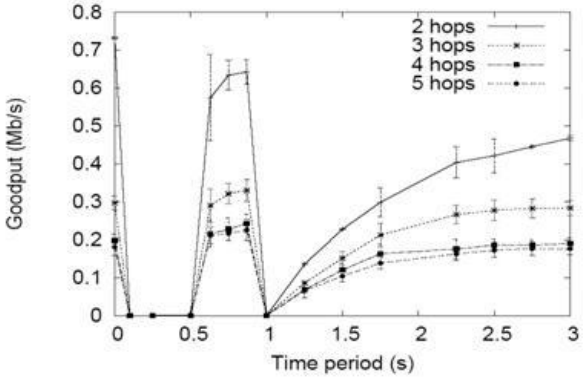

Figure 3. JF-drop effect on throughput

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 nonmalicious 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.

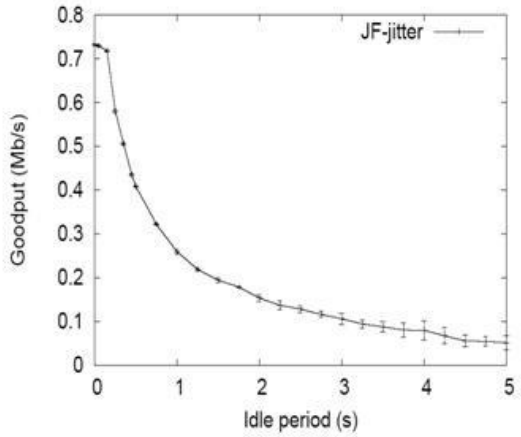

Figure 4. JF-jitter effect on throughput

2.2 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.

3. 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):

This design technique provides a first line of defense against resource depletion attacks by restricting data traffic passing through a router to authorized flows.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.

The access control rule base need not maintain an exhaustive list of authorized flow identifiers. Instead it may define access control in terms of general rules or policies.

The incorporation of FRAC within existing algorithms requires modifications to the route construction components of the algorithms so that the routing tables are indexed by the flow identifiers as opposed to destination addresses. Furthermore, the packet forwarding function must be modified to ensure that packet forwarding decisions are made on the basis of the flow-id as opposed to the destination address. This even applies to source routing ad hoc algorithms such as Dynamic Source Routing (DSR) . Of course, in this case the routing table need not maintain the next hop information since each packet contains the source route.

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.

A number of existing routing algorithms are inherently incapable maintaining multiple paths. They can only maintain the current path, usually the shortest path between the source and the destination. They will only initiate discovery of an alternate path when notified of the failure of the current path. However, in the case of intrusion attacks on data traffic, this would result in rediscovery of the faulty path again. Since routing control traffic is unharmed on the path, this path still remains the shortest path between the source and the destination and is therefore selected again by the routing algorithm. Table driven ad hoc routing algorithms, such as DSDV, fall into this category.

To incorporate multi-path routing, the route discovery and maintenance functions of these algorithms must be modified. Specifically, the routing tables needed to support multi-path routing must maintain the next hop information not only on a per flow basis but also on a per path basis for each flow.

Source-Initiated Flow Routing:

When multiple paths exist between the source and the destination, source-initiated flow routing enables the source to specify which of these paths must be used by the data flow originating from it to reach the destination. 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.

To incorporate source initiated flow routing, existing ad hoc routing algorithms must implement mechanisms for selecting path labels for each alternate path between the source and destination and to convey this information to the source node so that it is aware of all these paths.

Flow Monitoring:

For source-initiated flow routing to work effectively, it is essential to detect path failures resulting from intrusion induced faults. We rely on the flow monitoring mechanism to detect the failure of a path and to notify the source of the information flow. The source then switches the information flow to an alternate path to circumvent the intruder-induced fault in the previous path.

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.

The routing function at a destination node continuously monitors each flow received by it and tracks the number of packets successfully received by it (i.e., uncorrupted) between flow status messages for each flow. It signals a path failure for a flow if one of the following events occurs:

1. It has not received a flow status message for a predetermined interval (potentially indicating a simple route failure or a denial of service attack on the path).
2. The number of packets successfully received by it falls below a present threshold fraction of the packets transmitted by the source (indicating a potential flow disruption attack).
3. The number of packet received by it is much above that transmitted by the source (indicating a potential resource depletion attack on the path).

The path failure message is sent from the destination to the source of the information flow over all the alternate paths that exist between the two nodes.

Fast Authentication:

The effectiveness of TIARA mechanisms such as FR4C rests upon the efficacy of the authentication mechanism. Traditional packet authentication techniques used with IPSEC, such as MD5 based message authentication codes (MAC), are prohibitively expensive to be used in the route forwarding path.

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. The location might be different for different nodes in the path between the source and the destination of the data flow. The information on the node specific secret location of the path label is conveyed to each routing node in a secure fashion by the route establishment function of the ad hoc routing algorithm. Existing ad hoc algorithms must be modified to incorporate this functionality.

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.

Similar to fast authentication, the incorporation of this mechanism in existing ad hoc routing algorithms requires changes in the route establishment function as well as the packet forwarding function within the wireless router.

4. Related Work

TABLE I. SECURE AD HOC ROUTING PROTOCOLS COMPARISON

Protocol	ARAN[35]	ARIADNE[34]	SAODV[40]	SEAD[37]	SRP[38]
Type	Reactive	Reactive	Reactive	Proactive	Reactive
Encryption Algorithm	Asymmetric	Symmetric	Asymmetric	Symmetric	Symmetric
MANET Protocol Synchronization Central Trust Authority	AODV/DSR No Certificate Authority (CA) Required	DSR Yes Key Distribution Center (KDC) Required	AODV No CA Required	DSDV Yes CA Required	DSR/ZRP No CA Required
Authentication	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	No	No	No	No
Integrity	Yes	Yes	Yes	No	Yes
Non Repudiation	Yes	No	Yes	No	no
Arti-Spoofing	Yes	Yes	Yes	No	Yes
Dos Attacks	No	Yes	No	Yes	Yes

Authenticated Routing for Ad-Hoc Networks (ARAN) is an on-demand, ad-hoc routing protocol that uses certificates to ensure authentication, message integrity, and non-repudiation of routing messages in an ad hoc networking environment. Based on logical route metrics and certificates, ARAN is immune to modification, impersonation, and fabrication of routing messages.

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.

5. 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

[1] http://web.informatik.uni-bonn.de/IV/Mitarbeiter/mp/paper/secure_routing/routing security in ad hoc networks - lundberg.pdf
[2] http://www.cs.purdue.edu/homes/ninghui/readings/TruSe_fall04/aran.icnp02.pdf
[3] http://web.informatik.uni-bonn.de/IV/Mitarbeiter/mp/paper/secure_routing/routing-security in ad hoc networks- lundberg.pdf
[4] R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, K. Thurber, Techniques for intrusion-resistant ad hoc routing algorithms (TIARA), in: Proceedings of MILCOM, October 2000.
[5] http://www.yuvaengineers.com/?p=699
[6] http://www.authorstream.com/Presentation/Gulkund-17377-secure-routing-ad-hoc-wireless-networks-Requirements-Protocol-AODV-SAR_SEAD-ARAN-Security-Aw-in-as-Entertainment-ppt-powerpint/