On the Survivability of Routing Protocols in Ad Hoc Wireless Networks

Baruch Awerbuch, Reza Curtmola,
David Holmer and Herbert Rubens
Department of Computer Science
Johns Hopkins University
Baltimore, MD 21218 USA
{baruch, crix, dholmer, herb}@cs.jhu.edu

Cristina Nita-Rotaru
Department of Computer Science
Purdue University
West Lafayette, IN 47907 USA
crisn@cs.purdue.edu

Abstract

Survivable routing protocols are able to provide service in the presence of attacks and failures. The strongest attacks that protocols can experience are attacks where adversaries have full control of a number of authenticated nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. This work examines the survivability of ad hoc wireless routing protocols in the presence of several Byzantine attacks: black holes, flood rushing, wormholes and overlay network wormholes. Traditional secure routing protocols that assume authenticated nodes can always be trusted, fail to defend against such attacks. Our protocol, ODSBR, is an on-demand wireless routing protocol able to provide correct service in the presence of failures and Byzantine attacks. We demonstrate through simulation its effectiveness in mitigating such attacks. Our analysis of the impact of these attacks versus the adversary's effort gives insights into their relative strengths, their interaction and their importance when designing wireless routing protocols.

1 Introduction

The wide-spread adoption of portable computing devices combined with the recent advances in wireless technology has lead to increases in productivity in the corporate and industrial sectors. While these recent advances have enhanced existing business processes, they have also introduced new security vulnerabilities.

Traditionally, networks have strongly relied on physical security. The concept of a network firewall is an example of this approach. A firewall is intended to provide an access control division between the insecure public network (the Internet) and the seemingly secure private internal corporate network. However, in the context of wireless networks, the assumption about the physical security of the network infrastructure is unrealistic. The wireless shared medium is exposed to outsiders and susceptible to a wide range of attacks such as: jamming of the physical layer, disruption of the medium access control layer, attacks against the routing protocols, targeted attacks on the transport protocols, or even attacks intended to disrupt specific applications.

In addition to the vulnerabilities of the wireless communication to outside attacks, the ultra portability of modern devices provides an increased susceptibility to theft. In 2003, 59% of companies surveyed in the CSI/FBI Computer Crime and Security Survey [1] reported that laptops had been stolen. The likelihood of devices being captured is even higher for military devices operating in a battlefield environment. Once captured, these devices can be used to attack the network from inside. Therefore, there is a need for protocols able to operate correctly not only in the presence of failures and outside attacks but also when part of the network is under the control of the adversary. Attacks denoted by arbitrary (malicious) behavior are also known as Byzantine [2] attacks and protocols able to provide service in the presence of attacks and failures are often referred to as survivable protocols.

Many secure routing protocols focus only on providing authentication and integrity of messages. Authentication and data integrity mechanisms, although needed in order to prevent injection, modification and impersonation attacks, do not provide protection against Byzantine attacks since they cannot force a node to behave as specified by the protocol. Below, we outline several Byzantine attacks that are considered in this work. We believe they are representative of the types of attacks that are likely to be mounted against ad hoc wireless routing protocols, and they cover a wide range of adversarial strengths. Individual techniques were proposed [3, 4, 5, 6, 7] to mitigate each of these attacks, but ODSBR [8] is the only full-fledged protocol that can withstand all of them.

A *Black Hole Attack* is a basic Byzantine attack where the adversary drops entirely or selectively data packets,

while still participating in the routing protocol. As a result, whenever an adversarial node is selected on a path, data will be lost partially or entirely on that path.

A *Flood Rushing Attack* exploits the flood duplicate suppression technique used by many wireless routing protocols. If an attacker succeeds in rushing an authenticated flood through the network before the flood traveling through a legitimate route, then the legitimate version will be ignored and only the adversarial version will be propagated. This attack may result in establishing many adversarial controlled paths. Authentication techniques can not prevent the attack, since adversaries are authenticated nodes.

A *Byzantine Wormhole Attack* is an attack in which two colluding adversaries cooperate by tunneling packets between each other in order to create a shortcut (or wormhole) in the network. This tunnel can be created by using a private communication channel, such as a pair of radios and directional antennas, or by using the existing ad hoc network infrastructure. The adversaries can use the low cost appearance of the wormhole in order to increase the probability of being selected on paths, and then attempt to either disrupt the network by selectively dropping the data packets, or to perform traffic analysis. Note that for a Byzantine wormhole, the wormhole link exists between two compromised (adversarial) nodes, while in a traditional wormhole two honest nodes are tricked into believing that there exists a direct link between them.

A *Byzantine Overlay Network Wormhole Attack* is a more general (and stronger) variant of the previous attack, which occurs when several nodes are compromised and form an overlay network. By tunneling packets through the overlay network, the adversaries make it appear to the routing protocol that they are all neighbors, which considerably increases their chances of being selected on routes and facilitates further attacks.

In this work we study the survivability of ad hoc wireless routing protocols in the presence of failures and Byzantine attacks. Our contributions are:

- We present a detailed description of several Byzantine attacks (black hole, flood rushing, wormhole and overlay network wormhole) and analyze their mechanisms and interaction. We analyze the techniques used to mitigate these attacks by ODSBR [8], our ad hoc wireless routing protocol designed to defend against a wide range of Byzantine attacks performed by possibly colluding adversaries.
- We developed a protocol independent Byzantine attack module for the NS2 [9] simulator in order to simulate these attacks. We believe the module is a helpful tool for the secure routing research community.
- We demonstrate through simulation the effects of the considered attacks on the AODV [10] routing protocol. Our results quantify the damage caused by the attacks and provide insights into identifying those which result in the greatest network disruption while requiring the least number of adversarial participants.

  We emphasize the reason we chose to compare ODSBR only with AODV; we consider the performance of AODV to be representative of both insecure routing protocols and authentication-based secure routing protocols (such as Ariadne [11], SEAD [12], ARAN [13] and SRP [14]) that do not provide protection against the considered Byzantine attacks.
- We implement our protocol, ODSBR [8], and show through simulations how ODSBR mitigates the above identified attacks. Analysis of the results gives insights into the survivability of the routing service while under attack and indicates what are the main factors contributing to the effectiveness of the attacks: flood rushing and strategic adversarial positioning.

The rest of the paper is organized as follows. Section 2 surveys related work. We present an overview of the ODSBR protocol and discuss the mechanisms it uses to detect failures and mitigate Byzantine attacks in Section 3. We demonstrate through simulations the impact of these attacks on AODV and show how ODSBR mitigates them in Section 4. We conclude in Section 5.

2 Related Work

Many vulnerabilities in network protocols are caused by the lack of integrity and authentication mechanisms, which allows an attacker to alter or fabricate packets. Significant research in securing wired [15, 16, 17] or ad hoc wireless [11, 12, 13, 14] routing protocols focused on this aspect. Below we present only work that specifically addressed Byzantine attacks. None of the protocols we overview below are able to deal with a wide range of Byzantine attacks, but are rather focused on a particular attack.

Black Hole. The technique presented in [3], referred as *Watchdog*, exploits the fact that a node can overhear its neighboring nodes forwarding packets to other destinations. If a node does not overhear a neighbor forwarding more than a threshold number of packets, it concludes that the neighbor is adversarial. The scheme does not require any explicit network overhead or cryptography and is effective against the basic black hole attack in single rate fixed transmission power networks. However, it does not perform well when either power control or multi-rate (i.e. 802.11abg [18, 19]) are used, since their use will violate the assumption that the forwarding transmission is successfully overheard. In addition, the method is vulnerable to attacks from two consecutive and colluding adversaries where the first

adversarial node does not report that the second did not forward the data.

An alternate technique for avoiding black hole attacks is the Secure Data Transmission (SDT) protocol [4]. SDT uses authenticated destination-to-source acknowledgments as proof that the packets reached their destination. The approach taken in SDT to avoid the black hole attack is to disseminate a packet across several node-disjoint paths. The method has relatively low overhead, converges quickly, and works effectively in a well connected ad hoc wireless network, where the number of disjoint paths is large. The disadvantage is that in a sparsely connected network, where the number of available disjoint paths is small, all of the discovered paths may contain an attacker and thus, the scheme will be less effective.

Flood Rushing. Rushing Attack Prevention (RAP) [5] prevents the rushing attack by waiting for up to k flood requests and then randomly selecting one to forward, rather than only forwarding the first one. To prevent an attacker from bypassing the scheme by simply sending k requests, the RAP protocol incorporates secure neighbor discovery and secure route delegation schemes. However, these schemes have significant network overhead because multiple rounds of communication are required for every hop the route request propagates. In addition, RAP will be ineffective if the adversary has compromised k or more nodes.

Byzantine Wormhole. A technique proposed to prevent wormholes is *Packet Leashes* [6]. The authors suggest restricting the maximum transmission distance by using either a tight time synchronization (temporal leash) or location information (geographic leash). Temporal leashes require additional hardware, such as accurate clocks or GPS receivers. The protocol is effective at preventing the traditional wormhole attack, but is ineffective against the Byzantine variant because preventing the wormhole is the responsibility of its end points. In this case the end points are adversarial and cannot be trusted to follow the protocol correctly.

A more recent method, proposed for ad hoc wireless sensor networks relies on directional antennas [7]. The approach prevents wormholes by having each node maintaining accurate information about its neighbors. Messages coming from a node that is not perceived as a neighbor are ignored. The protocol is appropriate for sensors networks which in general have low mobility. However, maintaining neighbor information in mobile networks is more challenging and expensive. In addition, the protocol that maintains information about neighbors can itself be subjected to wormhole attacks, particularly because it requires cooperation among nodes.

3 ODSBR

ODSBR is an on-demand source routing ad hoc wireless routing protocol, designed to cope with a wide class of Byzantine attacks. In previous work [8] we laid out the design principles and theoretical analysis for ODSBR. In this paper we focus on providing details about the techniques employed by ODSBR to detect faults and to mitigate Byzantine attacks, and on presenting simulations which show the protocol's effectiveness under several attack scenarios. The task required us to implement ODSBR, design several modifications to the original protocol motivated by practical considerations, and implement an NS2 [9] module that generates Byzantine attacks. Below we present an overview of the protocol and discuss implementation details and mitigation techniques.

3.1 Overview

The design of ODSBR is centered around the impossibility of distinguishing between failures and malicious behavior. Thus, ODSBR addresses both failures and attacks within an unified framework. A fault is defined as any disruption that results in significant loss or delay. It can be caused by Byzantine behavior, external adversaries, lower layer influences, or simply by bursting traffic. As long as a non-adversarial path exists between source and destination, ODSBR finds that path and uses is to deliver data. ODSBR assumes that while all network nodes can be authenticated, only the source and destination can be fully trusted.

At the highest level, the protocol operates using three phases: least weight *route discovery*, Byzantine *fault localization* and *link weight management*. The route discovery is based on a reliability metric capturing past history. The metric is represented by a list of link weights where high weights denote low reliability. Each node maintains its own list, dynamically updating it when faults are detected. Faulty links are identified by an adaptive probing scheme in the fault localization phase, and are then avoided when selecting a new path (since their weight is increased). Individually, these phases provide several security guarantees:

- *Route Discovery.* Double flooding, per node flood verification, and forwarding rules guarantee that the route discovery process will always find the lowest cost path. However, this path is not guaranteed to be adversarial-free until the weight of adversarial links has been increased sufficiently that the lowest cost path is fault free.
- *Fault Localization.* The source uses an adaptive probing technique to locate faults along the path down to the nearest link. The source requires secure acknowledgements from intermediate nodes (*probes*) along the