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

route. The secure acknowledgements represent cryptographic proof that packets are delivered successfully and uncorrupted to the destination. Due to the structure of the probing scheme, an adversarial node can only cause a fault to be localized to one of its adjacent links, and does not have the power to arbitrarily incriminate other links in the network. Also, as the list of probes is cryptographically coupled to every data packet, it is impossible to escape detection without delivering the majority of packets correctly (dropping less than an allowable threshold).

- *Link Weight Management.* The increased weight assigned to a faulty link is maintained until a sufficient number of correct secure acknowledgements are received from the destination. This amortizes the number of lost packets caused by adversaries over enough successful packets, and bounds the overall loss rate even in the case of dynamic adversaries that alternate between good and bad states.

When combined together, as long as a fault free path from the source to the destination exists, these three phases bound the number of losses caused by adversaries, even when a majority of the nodes are colluding Byzantine adversaries. We refer the reader to [8] for a more detailed description and the theoretical analysis of ODSBR.

3.2 Implementation

We implemented the protocol using the NS2 [9] network simulator. We assumed the protocol uses RSA [20] with 1024-bit keys for public key operations, AES [21] with 128-bit keys for symmetric encryptions and HMAC [22] with SHA1 as the message authentication code. The impact of these cryptographic operations is represented by adjusting the packet size and by introducing packet delay accordingly, as if the packet actually contained authenticating data (e.g. digital signatures or MACs), and as if CPU time was spent performing cryptographic operations[1].

For practical reasons, we implemented a simplified adaptive probing scheme for fault localization. Instead of our originally proposed binary search probing technique [8], we use only two states: a "non-probing" state where only the destination returns acknowledgments, and a "probing" state where all intermediate nodes also return acknowledgments. The protocol operates in the non-probing state until a loss threshold violation occurs and a fault is detected. If, in probing state, the source node successfully delivers enough packets and the loss rate goes below a specified threshold, then the source node returns to the non-probing state. Preliminary experiments we conducted showed that when the total number of hops is relatively small, the cost of enabling all the probes at once is low. In this case the two-state technique reduces the amount of time necessary to identify a link and considerably simplifies the protocol implementation.

The performance of the implementation is influenced by the values of several parameters: the loss threshold rate, the timeout allowed for a packet to traverse a link and the size of the sliding window necessary to keep track of the packet loss history. After conducting a series of experiments with different sets of parameters, the values were chosen as follows: loss threshold rate – 10%, link timeout – 250 milliseconds and sliding window size – 100 packets. We tuned these parameters conservatively in order to ensure that the protocol will operate in a wide range of environments. Although the simulations in this work were conducted with 50 nodes, these values were tuned for efficient operation with up to 100 nodes.

3.3 Attacks Mitigation

To the best of our knowledge, ODSBR is the only protocol that can withstand all of the attacks described below.

Black Hole The ODSBR protocol uses end-to-end acknowledgments from the destination to detect the presence of a black hole attack. Upon detection of the attack (the number of lost packets becomes higher than a threshold value), ODSBR enters a probing mode with the goal of discovering the attack location. As a result of this probing procedure, the location of the adversary can be narrowed down to a link (the guilt is assigned to a link, since it is theoretically impossible [23] to indicate a node). The weight of a blamed link is doubled, which ensures that the protocol will avoid selecting paths containing that link during future route discoveries. As a result, if there exists an adversarial-free path to the destination, ODSBR will eventually find it within a bounded amount of packet loss. In addition, ODSBR can deal with a mobile adversary along the path, since probes once started are not retired immediately. In the worse case, all nodes may act as probes.

An adversary can drop packets just below the threshold in an attempt to avoid detection. However in this case the protocol has successfully "scared" the adversary into predominantly behaving correctly. In addition, randomized threshold selection can help reduce the effectiveness of this adversarial strategy. One of the main advantages of ODSBR's approach to mitigating black holes is that the locations of the attackers are learned, thus enabling adversary avoidance in arbitrary network configurations.

Flood Rushing The route discovery phase of the ODSBR protocol has several features which help mitigate the effects of flood rushing. The protocol performs hop-by-hop authentication and integrity checking of route discov-

[1] We have adjusted the time delays to approximate the performance of a 1.5 GHz Intel Pentium M processor.

ery flood packets. This prevents an invalid variant of the flood from propagating through the network. Using only end-to-end authentication (source and destination only) will not prevent an invalid variant from propagating and blocking the valid flood.

In addition, ODSBR processes all duplicate flood packets and if a valid flood packet with a lower metric is received, an additional re-broadcast is scheduled. The advantage of this technique is that even if an adversary performs a successful "rush" in an attempt to be selected on the path, the adversarial variant of the flood will be shortly overridden by the legitimate flood with a lower path cost. The method will increase the protocol overhead because nodes affected by the rushing adversary need to re-broadcast the flood packet more than once. Finally, any adversary that manages to bypass these two protection mechanisms and starts creating damage, will be detected by the fault location algorithm and then avoided when a new path is selected.

Byzantine Wormhole ODSBR's approach to mitigating Byzantine wormholes is motivated by the observation that the primary attack when a wormhole exists is the dropping of packets that attempt to travel through the wormhole, rather than the wormhole formation. A wormhole attack will appear to ODSBR as a faulty link existing between two nodes. ODSBR mitigates the attack not by preventing the formation of the wormhole, but by detecting it and increasing its weight. Once the wormhole's link weight has been increased sufficiently, ODSBR will avoid it and select the next best alternate path. This strategy does not require any additional hardware or capabilities to function, and it works equally well for both Byzantine and traditional wormholes. The number of packets lost and the amount of time taken to find an adversarial-free path, will be proportional to the number of wormhole links that create paths shorter than the legitimate route. As a result, ODSBR's ability to mitigate the wormhole attack will be reduced if many wormhole links are present.

Byzantine Overlay Network of Wormholes The convergence of ODSBR is slowed if many adversaries exist in the network and cooperate to create an overlay of Byzantine wormholes. However, the amount of damage that the attackers can create is bounded. More specifically, for a network of n nodes of which k exhibit adversarial behavior, the bound is given by $q^- - \rho \cdot q^+ \leq b \cdot kn \cdot \log^2 n$, where q^- and q^+ are the total number of lost packets and successfully transmitted packets, respectively, ρ is the transmission success rate, slightly higher than the original threshold, and b is the number of lost packets per window. Note that kn represents the number of links controlled by an adversary. If there are no adversarial nodes, the above equation becomes the ideal case where $q^- - \rho \cdot q^+ \leq 0$. More details about the analysis can be found in [8].

4 Experimental Results

In this section we show how AODV [10], a well-known routing protocol for ad hoc wireless networks, reacts under several Byzantine attack scenarios. In addition, we conducted simulations of the same attacks against ODSBR in order to show its effectiveness in mitigating the attacks. We chose to compare ODSBR with AODV because we consider the performance of AODV to be representative for both insecure and authentication-based secure routing protocols (such as Ariadne [11], SEAD [12], ARAN [13] and SRP [14]). These secure routing protocols do not provide additional resilience over the insecure AODV protocol under the considered Byzantine attacks.

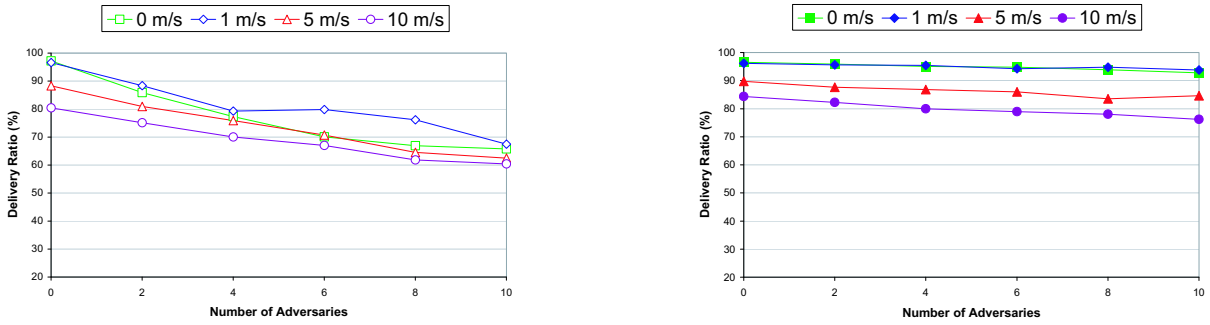
We also conducted experiments to compare ODSBR with the DSR [24] routing protocol. The results were similar to the ones in which the baseline was AODV. Due to space constraints we chose to include only the measurements for AODV.

Each data point in the figures of this section is the mean result of 30 different random environments. AODV and ODSBR are simulated in the same set of random environments in order to generate paired statistics (a standard method of statistical variance reduction). A paired T-test analysis of all our data shows that the largest p-value for any set is .0083. Therefore, we can be over 99% confident in saying the observed performance differences between AODV and ODSBR are statistically significant.

4.1 Simulation Setup

We performed simulations using the NS2[9] network simulator. Nodes in the network were configured to use 802.11 radios with a bandwidth of 2 Mbps and a nominal range of 250 m. 50 nodes were randomly placed within a 1000 by 1000 meter square area. In addition to these 50 nodes, up to 10 adversarial nodes were added to the simulations, depending on the considered attack configuration. A traffic load of 10 constant bit rate (CBR) flows was used to simulate data communication through the ad hoc network. An aggregate load of 0.1 Mbps was offered to the network by having each flow send 256 byte packets (≈4.9 packets per second). The simulated time was 300 seconds.

We used a modified random way-point mobility model that addresses the concerns raised in [25] about the validity of the standard random way-point model. Nodes select a speed uniformly between 10% and 90% of the given "max" speed to achieve more steady mobility and ensure that the average speed does not drop drastically over the course of the simulation. In addition, 300 virtual seconds of mobility are generated before the start of the simulation such that when the simulation starts, nodes are already in motion. This allows the average speed and node distribution to stabilize before the simulation starts.



(a) AODV (b) ODSBR

Figure 1. Black Hole Attack: Random Placement

In order to simulate the considered Byzantine attacks, we developed a protocol-independent Byzantine attack simulation module for NS2. This module provides the capability to simulate the black hole, Byzantine wormhole, and Byzantine overlay network wormhole attacks without modifying the routing protocol.

4.2 Black Hole Attack

We simulate a black hole attack by dropping any data packet sent by the routing agent. Routing protocol control packets are unaffected. On a real device, depending on the routing protocol implementation, performing a black hole attack may be as simple as deactivating IP forwarding.

We evaluate the delivery ratio by using as a baseline the case where no black holes exist in the network. We then increase the number of adversarial nodes, randomly placed in the network, and evaluate the effect this has on the delivery ratio. Figure 1 shows the delivery ratio of the AODV and ODSBR protocols as a function of the number of adversarial nodes, for different levels of mobility. We note that the delivery ratio of AODV does decrease as the number of adversaries increases, but a large number of adversarial nodes is required in order to cause a significant network disruption. For example, approximately 10 adversarial nodes are required to drop the delivery ratio of AODV below 70%. This happens because there is no effort by the adversary to get itself selected on paths and although a number of compromised nodes exist in the network, there is no coordination between them when performing the attack. We conclude that AODV can sustain attacks consisting of a small number of uncoordinated black holes.

ODSBR remains basically unaffected by attacks at low mobility, maintaining a delivery ratio of about 95%, even in the presence of 10 adversarial nodes. At higher mobility, we see a slight decrease in the delivery ratio because node mobility causes some paths to be broken, and some packets will be lost before ODSBR reacts and readjusts the path.

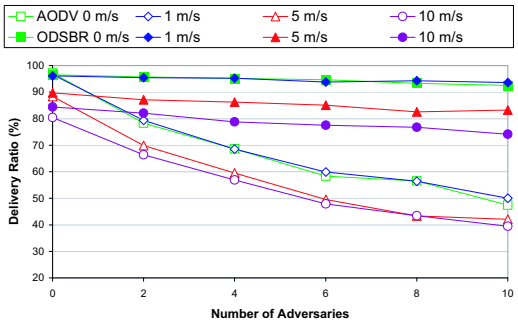


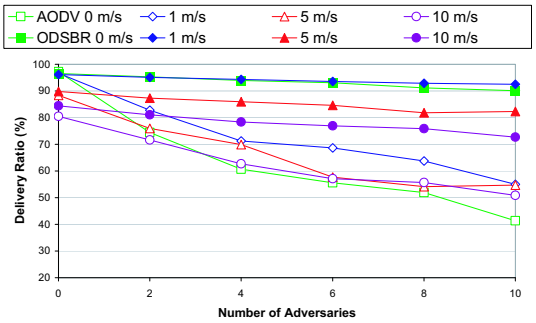
Figure 2. Flood Rushing Attack Combined with Black Hole Attack

4.3 Flood Rushing Attack

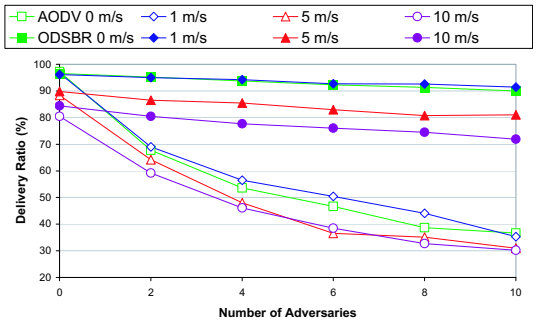
If an adversary is selected on many routing paths, it can cause more disruption. Therefore, any additional attack that helps a node to be selected on many paths can increase the impact of a regular black hole attack. The flood rushing attack is an example of such an attack. We performed simulation examining the impact of black hole attacks when combined with flood rushing.

We simulated flood rushing attacks as follows. During the propagation of a normal flood packet, each node waits a small randomized delay before re-transmitting it. These delays are designed to reduce the number of collisions and in some protocols to help ensure that the shortest paths are selected. Eliminating the extra delay is the simplest mechanism available to provide an adversary a time advantage over the normal flood.

Figure 2 shows the delivery ratio of AODV and ODSBR as a function of the number of adversarial nodes randomly placed within the simulation area, at different mobility values. It can be observed from Figures 1(a) and 2, that the delivery ratio for AODV is significantly affected by flood rushing. The intensity of the attack is due to the greater number of paths that an adversary succeeds in getting se-



(a) Without Flood Rushing



(b) With Flood Rushing

Figure 3. Wormhole Attack: Random Placement

lected on. No coordination exists between the attackers. The attack is very effective and lowers AODV's delivery ratio to about 40% when 10 adversaries are present in the network (as opposed to about 70% when no flood rushing was present).

The impact of flood rushing on ODSBR is almost unnoticeable. At low mobility, ODSBR delivers over 90% of the packets (as opposed to 95 % when no flood rushing was present), even in the presence of 10 adversaries. This indicates that the technique used by OSDBR to process lower path cost floods instead of discarding them is effective against flood rushing.

4.4 Byzantine Wormhole Attacks

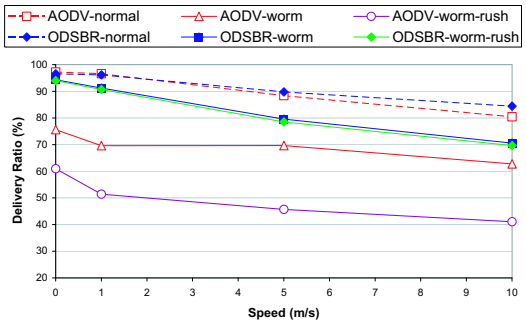
Previous attacks we examined do not use any coordination between the attackers. A coordinated attack can be much stronger, particularly if adversaries have knowledge of the network topology and/or traffic patterns. This can allow them to select strategic locations that can increase the effectiveness of an attack. For example, an adversary may locate itself in the vicinity of a specific target, or between two nodes that communicate frequently, or position itself such that it can hear all the communication on the network. A Byzantine wormhole attack, or simply a *wormhole*, is an example of an attack that requires coordination between the attackers. A wormhole can be used either to increase the effectiveness of a black hole directly, or as an effective tool in conducting flood rushing attacks, by allowing an adversary to jump several hops ahead of the legitimate flood through the wormhole. In addition, the placement of the wormhole in the network can increase the number of adversarial controlled paths.

Below we examine coordination among attackers and placement of attackers as possible strategies for increasing the effectiveness of an attack. We simulated the most effective wormhole attack by assuming that communication through the wormhole tunnel has no latency and has unlimited bandwidth. Several wormholes are placed in the network, but no coordination exists between them (coordinated wormholes are studied in Section 4.5). We examine the effect of wormhole placement by considering three configurations which we refer to as *random placement*, *central wormhole* and *cross of death*. In all cases, we evaluated the impact of the wormhole attack both by itself, and when combined with flood rushing.

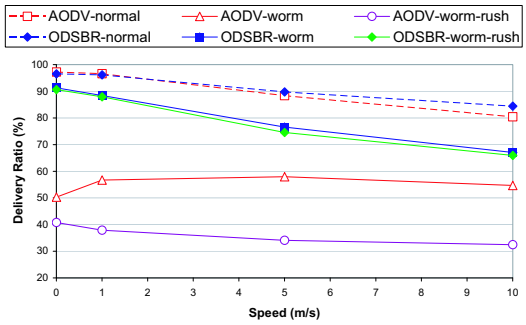
Random Placement. The first configuration we consider is a set of wormholes randomly placed in the network. Figure 3(a) presents results for AODV and ODSBR in the presence of the wormhole attack, while Figure 3(b) presents results for the wormhole attack combined with flood rushing. When compared to the black hole attack with randomly placed adversaries (Figure 1 and Figure 2), the same number of adversaries placed randomly, but now forming wormholes, can mount a more effective attack against AODV. This result is due to the fact that by using wormhole tunneling, the adversaries are selected as part of more routes and are thus able to drop more traffic and create more damage. When combined with flood rushing, the delivery ratio for AODV goes as low as 30% to 40%, depending on the mobility of the nodes.

In the case of ODSBR, the presence of wormholes has very little impact when compared with the black hole attack conducted by a number of attackers randomly distributed in the network (see Figures 1(b) and 3(a)). This indicates that ODSBR uses an effective mechanism in dealing with mobile adversaries that coordinate to create wormholes. The second observation is that adding flood rushing to increase the effectiveness of the attack does not make a difference for ODSBR, as expected from previous results (see Figures 1(b) and 3(b)).

Central Wormhole. Pictured in Figure 5(a), this configuration contains only two adversaries placed at coordinates (300,500) and (700,500) in the 1000 x 1000 m^2 area considered for our simulations. Since the nominal range is 250 m, this placement gives the wormhole a good coverage of the communication in the network.

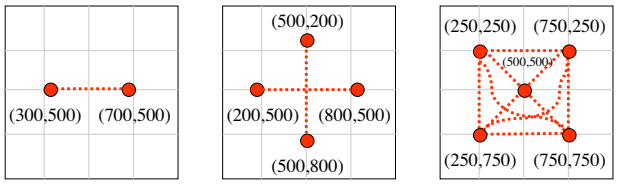


(a) Central Wormhole Configuration



(b) Cross of Death Configuration

Figure 4. Wormhole Attack: Central Wormhole and Cross of Death



(a) Central Wormhole (b) Cross of Death (c) Complete Coverage

Figure 5. Wormhole Network Configurations

The results presented in Figure 4(a) show the delivery ratio as a function of the mobility of the nodes, for AODV and ODSBR. In addition, the normal delivery ratios in the case of no adversaries are shown for reference. Although only one wormhole is present, the attack is considerably more effective than the black hole attack (see also Figures 1 and 2). For example, when flood rushing is enabled and two attackers coordinate to form a *central wormhole*, AODV's delivery ratio can drop as low as 41%, which is similar in strength to 10 randomly placed adversaries performing the black hole attack. This indicates that strategic positioning plays a significant role in the impact of an attack. The attacker needs to compromise only 2 nodes and then coordinate the attack.

For ODSBR, the wormhole at the specified location has a small effect, dropping the delivery ratio from about 80% in the case of 10 randomly placed adversaries, to about 70% in the case of the central wormhole, when nodes have a mobility of 10 m/s in both cases. This indicates that the placement of the wormhole did not allow it to control all the paths, so adversarial-free paths existed in the network. Since there was only one wormhole, ODSBR found it and used alternative paths to successfully perform data forwarding.

Cross of Death. As seen in Figure 5(b), this configuration contains four adversaries placed at coordinates (200,500), (800,500), (500,200), (500,800). They form two wormholes, in the shape of a cross. There is no coordination between the two wormholes.

The results presented in Figure 4(b) show the delivery ratio as a function of the mobility of the nodes, for AODV and ODSBR. As we expected, this is a more effective attack against AODV than the *central wormhole* attack, since the adversarial nodes are covering a larger area and are able to draw in (and drop) more traffic.

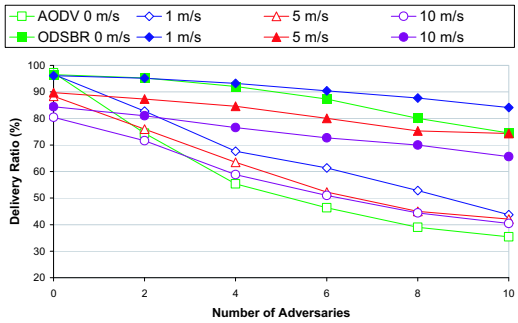
For ODSBR, the addition of one more wormhole was not problematic. Although each of the two wormholes had a good coverage, because of the lack of coordination among the four attackers, adversarial-free paths still exist in the network, so ODSBR manages to find them and use them as alternate paths.

Figures 3 and 4 allow us to analyze the number of randomly placed adversaries required to inflict the same amount of damage as a strategically placed attack. It can be noted that for AODV, with mobility > 0 m/s, the *central wormhole* configuration inflicts slightly more damage than 4 randomly placed adversaries (2 random wormholes) and the *cross of death* inflicts slightly more damage than 8 such adversaries (4 random wormholes). For ODSBR, both the *central wormhole* and the *cross of death* cause more damage than 10 randomly placed adversarial nodes (5 wormholes). This indicates that the wormhole attack is more effective if the adversaries are strategically placed, rather than randomly placed.

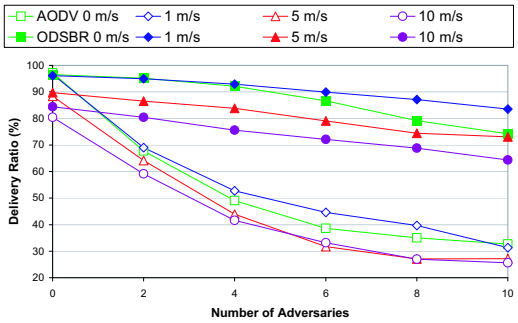
4.5 Byzantine Overlay Network Wormhole Attack

In Section 4.4 we analyzed the case where the wormholes were just point-to-point tunnels between two adversaries. While this attack is strong and effective, an even stronger variant exists, when the attackers also coordinate the wormholes. More specifically, the attacker compromises a number of nodes and organizes them in an overlay network wormhole, or a *super-wormhole*. In a super-wormhole attack with n adversaries there exist essentially n^2 point-to-point tunnels between the adversaries.

In the following set of simulations a static wormhole configuration is placed within the network. We investi-

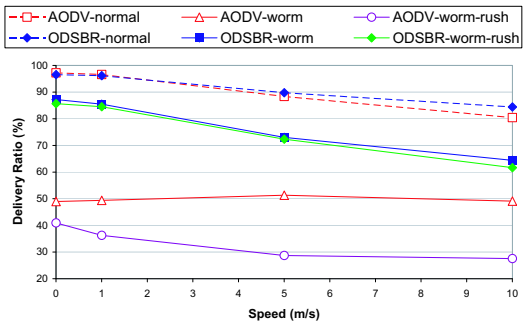


(a) Without Flood Rushing

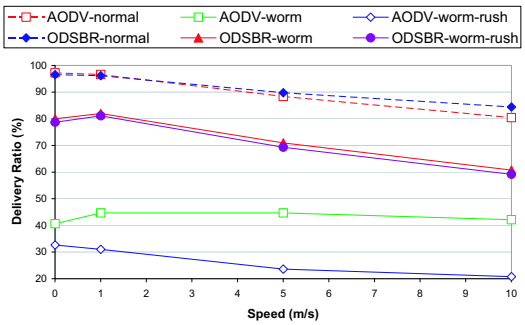


(b) With Flood Rushing

Figure 6. Super-Wormhole Attack: Random Placement



(a) Cross of Death Configuration



(b) Complete Coverage Configuration

Figure 7. Super-Wormhole Attack: Cross of Death and Complete Coverage

gated three configurations which we refer to as *random placement*, *cross of death*, and *complete coverage* (see Figure 5). In all cases, we first evaluate the effect of the super-wormhole attack on the delivery ratio. We then combine the super-wormhole with flood rushing and examine the impact of the combined attack. We assume that communication through the super-wormhole tunnels is instantaneous.

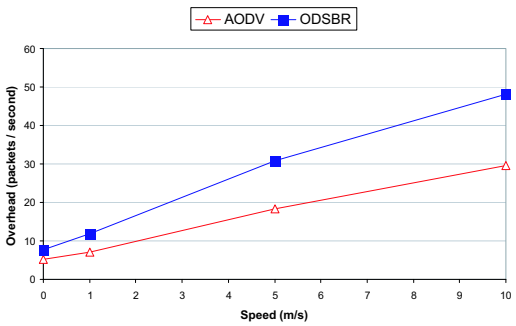
Random Placement. In this configuration a set of up to 10 adversarial nodes are randomly placed in the network and form a super-wormhole. Figure 6 presents results for AODV and ODSBR for the super-wormhole attack, with and without flood rushing. In this case, both for AODV and ODSBR, the super-wormhole attack is more effective than the regular wormhole, though not by much. This leads us to believe that a super-wormhole created by randomly placed adversaries gives them little advantage over the case when the same number of adversaries create regular 1-to-1 wormholes.

Cross of Death. The same configuration as the *cross of death* in Section 4.4 was used, but with all four adversarial nodes connected in a super-wormhole configuration. The results presented in Figure 7(a) show the delivery ratio as a function of the mobility of the nodes, for AODV and ODSBR, both with and without flood rushing. In addition, the normal delivery ratios in the case of no adversaries are shown for reference.

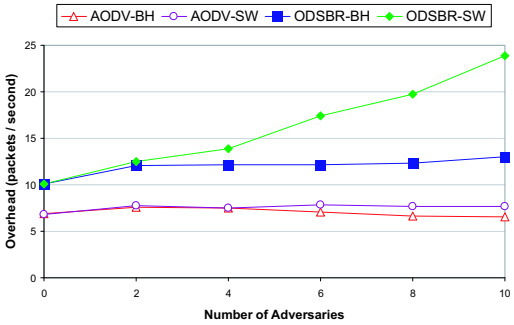
Figures 7(a) and 6 help us determine the number of randomly placed adversaries required to inflict the same amount of damage as a strategically placed attack. We conclude that for AODV, with mobility > 0 m/s, the *cross of death* configuration inflicts slightly less damage than a super-wormhole created by 8 randomly placed adversaries. For ODSBR, if mobility > 0 m/s, the *cross of death* causes about the same damage as a super-wormhole created by 9 randomly placed adversaries if flood rushing is not used, or 10 adversaries if flood rushing is enabled. Observe that the attack is slightly more effective than the *cross of death* with regular wormholes (Figure 4(b)). This is because the additional tunnels created in the super-wormhole scenario are of limited strategic value in comparison to the primary tunnels.

Complete Coverage. The strength of the super-wormhole attack can be increased significantly if the adversaries are able to position themselves throughout the network such that they can hear any transmission that takes place in the network. We simulated the configuration shown in Figure 5(c), with five adversarial nodes placed at coordinates (250,250), (250,750), (500,500), (750,250), (750,750).

Observe the devastating effect of this attack in Fig-



(a) Non-adversarial Scenario



(b) Attack Scenario

Figure 8. ODSBR overhead

ure 7(b). When combined with flood rushing, the delivery ratio of AODV drops as low as 20% in the presence of five adversaries, while ODSBR still delivers 60% of the packets. Since the five adversarial nodes almost completely cover the entire ad hoc network, adding more adversaries will not significantly increase the effectiveness of the attack. A set of only five colluding adversaries strategically placed and launching a coordinated attack practically paralyze the considered ad hoc network when an insecure routing protocol is used. It may seem that a super-wormhole attack is not feasible in practice because it may require a large number of point-to-point tunnels established between the adversaries. However, our simulations show that only five adversaries can cause a major disruption in a network of 50 nodes, making this attack practical and easy to mount.

4.6 Protocol Overhead

Simulations were conducted to compare the overhead of ODSBR with that of AODV, in order to evaluate the cost of security. In addition to route discovery overhead, ODSBR requires a protocol acknowledgment for each successfully delivered data packet. In real implementations, ODSBR acknowledgments can be piggy-backed on TCP acknowledgment packets, thus we only consider routing packets in the overhead measurements.

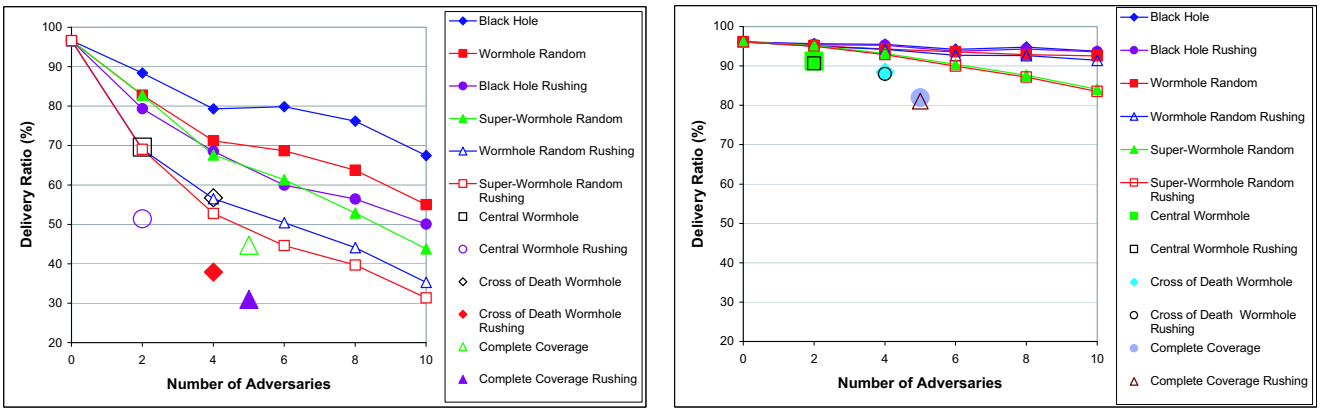
Figure 8(a) illustrates the overhead in a non-adversarial scenario. At all simulated levels of mobility, ODSBR transmits more routing packets per second than AODV. This is due to the fact that ODSBR floods both the route request and the route reply, while AODV floods only the route request. ODSBR requires bidirectional flooding to guarantee route establishment in the presence of Byzantine adversaries. If the route reply was unicast, then an adversary on the reverse path could forward the request but drop the reply, thus preventing a route from being established, although a correct path existed in the network.

Next we present the overhead while under adversarial attack. Figure 8(b) depicts the overhead of the routing protocols as a function of the number of adversaries, when the adversaries execute a black hole and a super-wormhole attack. The nodes are under random way-point mobility with a maximum speed of 1 m/s. Observe that the routing overhead of ODSBR increases with the number of adversaries. This occurs as a result of the protocol actively detecting faults and readjusting the path to avoid them. The overhead of ODSBR increases proportionally to the number of faulty links in the network. Since a super-wormhole attack results in a larger number of faulty links than a black hole, we see a considerable difference in the routing overhead of ODSBR when detecting a super-wormhole. On the contrary, the overhead of AODV decreases slightly as the number of adversaries increases. Since the adversaries forward the AODV control packets successfully and only drop data packets, AODV is unable to detect that a fault is occurring. This results in a massive reduction in AODV's delivery ratio, while no additional routing messages are generated.

4.7 Discussion

In this section we compare the previously presented simulation results in order to determine the relative strength of the Byzantine attacks (see Figure 9). To evaluate the effects of these attacks in a mobile ad hoc network, we selected scenarios where the mobility of the nodes was 1 m/s. This value was chosen in order to better isolate the damage caused specifically by the Byzantine attacks as opposed to losses due to node mobility. Analysis of these results indicates that two main factors contribute to the effectiveness of the attacks at disrupting the AODV routing protocol: flood rushing and strategic adversarial positioning.

Flood Rushing. In Figure 9(a), the line labeled "Black Hole Rushing" shows the results of a random placement black hole attack with flood rushing enabled. Observe that by enabling flood rushing, this attack resulted in a much greater reduction in the delivery ratio as compared to the same attack without flood rushing. In addition, the flood rushing made this attack strong enough that it caused more



(a) AODV (b) ODSBR

Figure 9. Attacks Comparison

damage than the random wormhole attack and comparable damage to the random super-wormhole attack. Note that the black hole attack (a non-colluding attack and simpler to execute), combined with flood rushing can create more damage than the wormhole attack (a colluding attack and harder to mount). This motivates the need to design routing protocols which are able to mitigate the flood rushing attack.

Strategic Positioning. The results indicate that the strength of the attacks can be significantly increased if the adversaries are strategically positioned. The point labeled "Complete Coverage" in Figure 9(a) illustrates the effectiveness of strategic positioning. This is the result of a super-wormhole with adversaries arranged in a dominating set configuration. By being strategically placed, five adversaries are able to reduce the delivery ratio of AODV to just 45%, without using flood rushing. In comparison, six randomly placed adversaries executing a super-wormhole attack, are only capable of reducing the delivery ratio of AODV to 61%. This demonstrates the power of strategic positioning in crippling the performance of the AODV routing protocol.

When used together, flood rushing and strategic positioning can cause substantial damage to the routing protocol. To quantify the most effective attack, we define the relative strength of a particular attack configuration σ as:

$$\sigma = \frac{DR_{norm} - DR_{adv}}{DR_{norm} \cdot Num_{adv}} \quad (1)$$

where DR_{norm} and DR_{adv} are the delivery ratios in the absence and in the presence of adversaries respectively, and Num_{adv} is the number of adversaries. Intuitively, σ represents the amount of damage an attack can cause per adversary. The higher σ is, the greater the relative strength of the considered attack, since this indicates that a larger amount of damage can be inflicted by a smaller number of adversaries.

Note that in the "Complete Coverage Rushing" case the delivery ratio drops to 30%, while $\sigma = 13.6$. Although this point corresponds to an attack that results in the greatest reduction of AODV's delivery ratio, it is not the most effective attack from the adversary's perspective because five nodes need to be compromised. Alternatively, we can consider the point referred to as "Central Wormhole Rushing" in Figure 9. This attack is able to lower AODV's delivery ratio from 96.6% to 51.4%, while requiring only two colluding adversaries, thus $\sigma = 23.4$. In fact, this is the highest σ observed out of all the considered attacks. This colluding attack executed by only two adversaries combines both flood rushing and strategic positioning, inflicting the highest amount of damage with the least number of adversaries.

Figure 9(b) presents a summary of the 1 m/s simulation results for the ODSBR protocol. The first observation is that at this level of mobility, the ODSBR protocol was able to successfully deliver over 80% of the packets under all simulated attack scenarios. This validates the protocol's overall strategy for operation in a Byzantine environment. In particular, the results show that ODSBR is resilient against flood rushing attacks which we have shown are devastating to other existing on-demand protocols.

5 Conclusions

In this paper we focused on analyzing the ability of ad hoc routing protocols to provide correct service in the presence of failures and Byzantine attacks. Our experiments showed that the state-of-art insecure routing protocol AODV is highly vulnerable to a wide range of Byzantine attacks. This is particularly significant considering that authentication-based secure routing protocols (such as Ariadne, SEAD, ARAN and SRP) do not provide additional resilience to these attacks. We conclude that flood rushing and strategic positioning of adversaries are the two most

important factors for an effective attack against on-demand protocols, particularly when adversaries collude. The flood rushing attack amplifies any attack it is combined with because it allows an attacker to have control on the route selection. Ad hoc routing protocols must be designed to take into consideration this attack.

After examining several types of attacks, we conclude that according to our metric, the most effective attack was the central wormhole combined with flood rushing: only two colluding adversaries were able to reduce AODV's delivery ratio to 51%. We showed that ODSBR was able to mitigate a wide range of Byzantine attacks; in particular, it was not significantly affected by flood rushing. Its performance only decreased when it needed to detect and avoid a large number of adversarial links.

References

[1] "CSI/FBI computer crime and security survey," *CSI Computer Security Institute*, vol. 8, 2003.

[2] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Advances in Ultra-Dependable Distributed Systems, N. Suri, C. J. Walter, and M. M. Hugue (Eds.), IEEE Computer Society Press*, 1995.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *The 6th ACM International Conference on Mobile Computing and Networking*, August 2000.

[4] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in 2^{nd} *ACM Workshop on Wireless Security (WiSe)*, 2003.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *ACM Workshop on Wireless Security (WiSe)*, 2003.

[6] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," in *Proceedings of the* 22^{nd} *Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, April 2003.

[7] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *NDSS 2004*, 2004.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in *ACM Workshop on Wireless Security (WiSe)*, September 2002.

[9] "The network simulator - ns2." http://www.isi.edu/nsnam/ns/.

[10] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, 1994.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *The 8th ACM International Conference on Mobile Computing and Networking*, September 2002.

[12] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *The 4th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[13] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *10th IEEE International Conference on Network Protocols (ICNP'02)*, November 2002.

[14] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, pp. 27–31, January 2002.

[15] R. Hauser, T. Przygienda, , and G. Tsudik, "Reducing the cost of security in link-state routing," in *Symposium of Network and Distributed Systems Security*, 1997.

[16] B. R. Smith, S. Murthy, and J. Garcia-Luna-Aceves, "Securing distance-vector routing protocols," in *Symposium on Networks and Distributed Systems Security*, 1997.

[17] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (s-bgp)," *IEEE Journal on Selected Areas in Communication*, vol. 18, no. 4, 2000.

[18] *IEEE Std 802.11a-1999*. http://standards.ieee.org/.

[19] *IEEE Std 802.11b-1999*. http://standards.ieee.org/.

[20] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[21] *Advanced Encryption Standard (AES)*. No. FIPS 197, National Institute for Standards and Technology (NIST), 2001. http://csrc.nist.gov/encryption/aes/.

[22] *The Keyed-Hash Message Authentication Code (HMAC)*. No. FIPS 198, National Institute for Standards and Technology (NIST), 2002. http://csrc.nist.gov/publications/fips/index.html.

[23] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[24] D. A. M. David B. Johnson and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (dsr)," August 2003.

[25] J. Yoon, M. Liu, and B. D. Noble, "Random waypoint considered harmful," in *INFOCOM '03*, (San Francisco, CA), April 2003.