Denial of Service Attacks in MANETs

by

Lucy R. Lee

S.B. Electrical Engineering and Computer Science
Massachusetts Institute of Technology, 2021

Submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2021

© Massachusetts Institute of Technology 2021. All rights reserved.

Author: .....
Department of Electrical Engineering and Computer Science
May 27, 2021

Certified by: .....
Dr. Karen Sollins
Principal Research Scientist
Thesis Supervisor

Accepted by: .....
Katrina LaCurts
Chair, Master of Engineering Thesis Committee

Denial of Service Attacks in MANETs

by

Lucy R. Lee

Submitted to the Department of Electrical Engineering and Computer Science
on May 27, 2021, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

Denial of service (DoS) attacks are one problem threatening the networks in the Internet of Battle Things (IoBT) world. Since devices move often in this world, the type of network most commonly used in the IoBT world is the Mobile Ad hoc Network (MANET), which dynamically re-configures itself to update the stored paths from one device to another. Routing protocols are used to update these paths. This paper describes two routing protocols designed specifically for use in MANETs - AODV and OLSR. We compare the performances of these two protocols during simulations of an IoBT scenario, and also analytical compare how they respond to two specific DoS attacks - black hole and flooding.

Thesis Supervisor: Dr. Karen Sollins
Title: Principal Research Scientist

Acknowledgments

I would like to thank my advisor, Karen Sollins, for her support throughout this thesis project and paper. I would also like to thank Samuel DeLaughter, for attending all of my meetings as well. Together, both of you always gave me excellent suggestions, explained concepts clearly, and guided me well as I progressed through this project.

I would also like to thank my parents and sister for their support throughout this process. Thank you for accompanying me along this journey and always providing positive encouragement.

Finally, I would like to thank my friends for also providing motivation and accompanying me through the late nights as we worked towards finishing our theses and graduation.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Denial of service (DoS) attacks are commonplace today, as defenses grow to meet attacks, and new attacks are formed to combat those defenses. One area in which these attacks are especially prevalent is the Internet of Things (IoT) space. This space is consisted of different objects communicating through the Internet. Many of these devices are small and insecure, making them attractive targets for attackers seeking to compromise them [3]. In fact, many IoT systems lack even basic security.

The Internet of Battle Things (IoBT) space resides within the IoT space, but is tailored especially for military applications. As the military begins to incorporate more advanced technologies into its equipment, the battlefield of the future will also evolve to become more densely populated with a variety of technological devices [12]. However, the IoBT space faces the same security problem that IoT systems face with regards to DoS attacks.

The network type that IoBT systems use is the mobile ad-hoc network (MANET), a type of network that is decentralized and wireless. Each device in the network is free to move independently, resulting in links between devices changing frequently. Each device is also a router, since it must forward other traffic as well as manage its own communication [6].

Two specific routing protocols that are commonly used within MANETs are AODV and OLSR. In this paper, we focus on these two protocols since they represent different categories of routing protocols - AODV is a distance vector and reactive protocol,

while OLSR is a link state and proactive protocol.

For our evaluation, we analyze the performance of both protocols in a simulation with IoBT characteristics, and also analytically compare how each protocol would react to specific DoS attacks such as black hole and flooding attacks. Depending on the situation, different routing protocols have different trade-offs, and making a choice about which routing protocol to use in a network should heavily depend on the deployment conditions of the network and what characteristics of the protocol are important to the user.

For the simulation, we use NS-3 [18], and change parameters such as environment size, transmit power, and mobility models to incorporate distinctive characteristics from the IoBT space. Then, we measure metrics such as end-to-end delay, hop count, and packet type ratios to determine the strengths and weaknesses of both routing protocols. We find that in the IoBT situation we are studying with high mobility nodes, OLSR performs better. However, in a different situation where links between nodes are more stable, AODV may be the better choice.

The two DoS attacks we use to compare the protocols are black hole attacks and flooding attacks. Black hole attacks are a type of routing disruption attack [4], while flooding attacks are a type of resource consumption attack [10]. Based on our analytical comparison, both attacks will be detrimental to AODV and OLSR, but the attacks can have more drastic effects on networks using the AODV routing protocol.

1.1 Summary

In Chapter 2, we explain the challenge associated with this problem space. Following that, Chapter 3 contains general background information on the IoBT space, DoS attacks, MANETs, and other related work. Chapter 4 dives deeper into the background of routing protocols, and introduces two specific protocols. We then describe our simulation results in Chapter 5, before following that with a comparative analysis of the effects DoS attacks have on our protocols in Chapter 6. Finally, we conclude this paper in Chapter 7.

Chapter 2

The Problem

The IoT space describes the network of "things", which are physical devices, and how they are all connected through the Internet. This space is rapidly expanding, as more and more technologies continue to evolve and grow [23]. Any physical object could be a "thing", as long as it can connect to the Internet to receive or send information. Examples range from small objects, such as a light bulb that can be switched on and off with a phone application, to large ones, such as a driver-less vehicle. As opposed to any random object, these technological "things" are more useful since they can communicate with other "things".

One area that IoT is expanding into is the military. When "things" can communicate with each other, they can also benefit humans involved in warfare. This new problem space is known as IoBT, but also has other names such as the Internet of Military Things, or Internet of Battlefield Things. Nevertheless, they all represent the same problem space - the problem space of IoT systems used in military applications.

As mentioned in Chapter 1, the MANET is a type of network that is very suitable for IoBT systems. Military missions involve constant movement of soldiers, vehicles, and other devices, so networks must be able to re-configure easily and allow the topology to be changed often. Since soldiers, vehicles, drones, and other devices all move at different speeds and with different paths, they each need to be represented by a separate mobility model. MANETs are able to provide this ability.

All devices in a MANET can be both an edge (destination) node, or an infras-

tructure node, which helps forward packets for other nodes. In addition, all or most devices are in motion, so the connectivity model and routes in between nodes will continuously change. However, although MANETs provide us with the ability to adjust to high mobility scenarios, they tend to be insecure, and are susceptible to DoS attacks.

The problem we address in this thesis is to explore the impact and vulnerabilities of two key representative routing protocols, whose responsibility is to provide valid routes for traffic between different edge nodes. We will compare the performances and characteristics of these two protocols, as well as how different DoS attacks can affect these routing protocols.

Chapter 3

Background

In this chapter, we introduce the background relevant to this problem space. We first describe the IoBT space. Next, we describe the problem of DoS attacks within this space. Finally, we narrow in on the type of network most commonly used in this space - MANETs.

3.1 Internet of Battle Things

The IoBT space is a unique space where the military meets the IoT space. The world of military battles has grown to be populated by a variety of devices, and successful communication between these devices is paramount to ensuring victory on the battlefield. These devices include a diverse set of "things", such as sensors, vehicles, robots, and more [12]. By being able to communicate with each other, they can better serve humans in combat.

However, such a large problem space will inevitably meet with challenges. These challenges include adapting to the heterogeneity of devices, achieving a proper balance between a user-friendly interface and displaying enough information, and preventing adversarial interference [12]. In this paper, I focus in on the challenge presented by enemies. Adversaries can threaten the confidentiality, integrity, and availability of information through electronic eavesdropping and malware.

3.2 Denial of Service Attacks

DoS attacks are a common method used by adversaries to disrupt networks. They are a rapidly growing problem, and pose an immense threat since the multitude and variety of them in the Internet are constantly growing [14]. These attacks prevent legitimate use of a service. General examples of DoS attacks include flooding systems by sending more traffic than the service can handle, and exploiting vulnerabilities in the target system that causes the service to crash.

Similarly, in the IoBT problem space, adversaries may launch DoS attacks to disrupt military operations. These attacks could prevent military equipment from functioning properly, or prevent communication between devices, both of which are vital to the success of a mission. Other ways adversaries can threaten network operations include acquiring friendly information from the network, inserting rogue things into the network, or intercepting and corrupting other information [12].

3.2.1 Victim Type

One way to group DoS attacks into different categories is based on the victim of the attack. An attack could target the destination node directly. One example of this type of attack is one that floods the receiver node with packets, preventing it from functioning properly.

Besides targeting the destination node directly, a DoS attack could also be indirect. If the attack is on other nodes within the network, the second order effects can still indirectly affect the destination node. For example, an attack on the infrastructure could prevent routing from working properly, thereby affecting other nodes besides the ones directly targeted by the attack.

3.2.2 Attack Type

Another way to partition DoS attacks is by grouping them based on the mechanism they use to attack victim nodes. There exists a large multitude of ways a DoS attack could be executed, so there are many categories within this partition, such

as overwhelming, dropping, and corrupting attacks. An overwhelming attack could flood the victim node until it can no longer perform its legitimate tasks. A dropping attack can occur if a malicious or malfunctioning node drops packets rather than forwarding them. A corrupting attack can happen when a malicious node corrupts packets before forwarding them, thereby changing the data within packets.

3.3 Mobile Ad-hoc Networks

To prevent attacks such as DoS ones from threatening the IoBT network, we must first understand the layout and structure of the network, and how devices currently communicate with each other. In the IoBT space, both humans and pieces of equipment have high mobility, since military missions involve constant movement. The network must dynamically reconfigure itself in response to this mobility in order to maintain communication between different devices. This type of network is called a mobile ad-hoc network, or MANET.

As introduced in RFC 2501 [6], MANETs are a type of decentralized wireless network that don't rely on pre-existing infrastructure. Instead, devices are free to move independently in any direction, and the links between devices must be updated frequently in order to maintain connections.

MANETs have the same distinctions as static networks between informing each router of the best route from it to each destination, called routing, and the act of using that information to forward the traffic toward the destination. To update these paths through routing, there needs to be a routing protocol, which specifies how information is distributed among the devices in the network. It also ensures that all the devices agree on what the routes are. In Chapter 4, we will describe routing protocols in more detail and explain the differences between some of them.

Security is a major vulnerability for MANETs. Since MANETs are constantly re-configuring and changing, they face challenges related to trust, verification, and adequate authentication [6]. DoS attacks are able to exploit these vulnerabilities to prevent the network from operating correctly.

3.4 Related Work

In the IoBT space, DoS attacks are already considered a potential problem. The overview on this problem space in Section 3.1 comes from the paper by Kott et al. from 2016 [12].

The background of DoS attacks and methods to analyze them is described in detail in two of Mirkovic's papers. The first describes taxonomies for distributed DoS attacks, and defense mechanisms against them [14]. The attack taxonomy covers both known attacks as well as those that are realistic potential threats. The defense system taxonomy covers both published approaches as well as commercial ones that are sufficiently documented. These two proposed taxonomies provide a background from which to understand and further analyze DoS attacks. The second paper by Mirkovic expresses the importance of using user and application-level metrics to judge DoS attacks [13].

In the work done by Greenberg et al. on 4D [9], they present a general framework for separating routing from routers. This framework consists of four planes: decision, dissemination, discovery, and data. When this paper was introduced in 2005, it introduced the novel idea that network control and management could be designed as a set of logically-centralized nodes that held a view of the entire network state. These centralized nodes would perform the calculations needed for each node, and then send that information out to each specific node. This idea has now become a recognized concept within routing protocols, and is further discussed in Section 4.1.1.

There is prior work completed on MANET routing protocols as well. In the paper by Gandhi et al., they evaluate and compare the performances of reactive, proactive, and hybrid protocols in MANETs [8]. A different paper by Alslaim et al. provides an overview of the MANET routing protocol problem space before comparing three specific protocols in terms of both characteristics and performances [2].

Finally, besides comparing MANET routing protocols themselves, there has also been work completed regarding the threat of DoS attacks in MANETs. Jain et al. introduces a way to classify these attacks [10], much like Mirkovic's DoS taxonomy

paper [14], except specifically tailored for MANETs. In this paper, the authors specify numerous DoS attacks, as well as multiple ways to classify them. Although Mirkovic's paper is not particularly applicable to the work described in this paper, Jain's paper is informative about DoS attacks that are specific to MANETs, and therefore more applicable to this paper.

Chapter 4

Routing Protocols

Routing protocols are necessary to find specific paths between the source and the destination. More specifically, for MANETs, the protocol must be able to adapt to changes in the network topology while maintaining routing information.

MANETs are not limited to any one particular routing protocol. Nodes must behave as routers and maintain their own routes to other nodes. The dynamic topology of MANETs shapes how these routing protocols can function. Another challenge these nodes face is that resources such as battery, bandwidth, and transmission power are limited [12].

4.1 Categories

There are many different routing protocols used in networks today, and it is important to pick a routing protocol that will work well based on the characteristics of the network it is used in. In the following subsections, we walk through three different ways to categorize these protocols.

4.1.1 Centralized vs. Distributed

Routing protocols can be categorized as centralized protocols, and distributed ones. In a centralized routing protocol, there exists a central node that gathers network

information from all other nodes in the network. This node is also responsible for calculating the best routes between all pairs of nodes, and then broadcasting that information out to each specific node [22].

In a distributed routing protocol, nodes receive information from other nodes in the network, and path computation is done at each node instead of at one central node. The kinds of information shared and styles to accomplish this differ from one protocol to another. All nodes are responsible for maintaining and updating their own routing tables separately [22].

Since MANETs are reconfigured often, distributed routing protocols are more effective than centralized ones. Each device should be responsible for its own movement and also for calculating its own routes to other destinations. Instead of having one central node that has to directly communicate with all the other nodes, it is more efficient to just send routing information to neighbors.

As an example, in a military environment, there may be a small group of soldiers that venture away from the main group, and get disconnected from the original network. In this case, these few soldiers should still be able to communicate with each other even though they are too far away from the others. In a centralized model, these soldiers would be completely disconnected from both the original network and from each other, since the central node wouldn't be able to send any routing information to them. On the other hand, in a distributed model, the small group could establish their own network even after being disconnected.

4.1.2 Distance Vector vs. Link State

Another way to partition routing protocols is by looking at the type of information sent during routing. Three primary categories include distance vector, link state, and path vector. In this paper, we focus on distance vector and link state protocols and pick one of each in Section 4.2 to analyze further.

Distance vector routing protocols choose the best path to a destination based on distance, usually measured using hop counts. The information shared by each node consists of the node's distance from other nodes. Each node shares information with

only its neighbors, and also updates its own distance table using information from its neighbors.

On the other hand, link state protocols share information through flooding and nodes generally try to maintain knowledge of the full network topology. The information shared consists of a node's links to other nodes.

4.1.3 Reactive vs. Proactive

Routing protocols specifically for MANETs can be grouped into three main types - reactive, proactive, and hybrid. In this paper, we discuss the reactive and proactive types in more depth, since hybrid is just a way to incorporate advantages from both.

Reactive protocols are also often called on-demand protocols, since nodes find routes to other nodes only when they need to. Only after a source node has a packet to send to a destination node does it begin determining the route to the destination [8].

In contrast, proactive routing protocols are also known as table-driven protocols. Each node maintains its own internal information about the entire topology of the network. This information is usually in the form of tables, and must be updated regularly in order to maintain up-to-date information on the routes to all other possible destination nodes [8]. When a node needs to send a packet, routes should be available from the source node immediately.

While MANET routing protocols are all distributed, both reactive and proactive ones are used because they each have their own positives and negatives. Proactive protocols have routes ready to use at nodes when they need it, while reactive protocols may need to take the time to find a route after a packet needs to be sent. However, this is done at the expense of more network overhead.

4.2 Routing in MANETs

Now that we've described how different routing protocols can be partitioned into categories, there are two particular protocols we focused on in this paper - AODV and

OLSR. Both are frequently used in the MANET environment, and are representative of some of the categories mentioned earlier. AODV is a distance vector and reactive protocol, whereas OLSR is a link state and proactive protocol.

4.2.1 Ad-hoc On-demand Distance Vector

Ad-hoc On-demand Distance Vector (AODV) is a reactive routing protocol. As introduced in RFC 3561 [7], this protocol uses three types of messages - route request (RREQ), route reply (RREP), and route error (RERR).

In AODV, nodes use request and response cycles to discover routes. When a node wants to send a packet, it first broadcasts a RREQ message to its neighbors. If the neighbor doesn't have a valid route to the destination, it in turn broadcasts the RREQ message to its own neighbors. This request process repeats until the RREQ message reaches either the destination node or a node that has a valid path to the destination. In Figure 4-1, we see an example of this with Node B as the source node and Node D as the destination node.

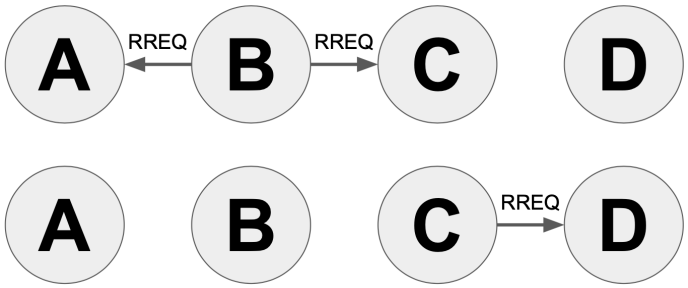

Figure 4-1: RREQ message broadcast from Node B, then forwarded by Node C

Now that the request to find a route has been satisfied, the node that has a valid path to the destination or the destination node itself sends back a RREP message to indicate that a route has been successfully found. This RREP message is unicast instead of broadcast back along the path the original RREQ took. In this way, a bi-directional path is established between the source and the destination, and the nodes along the path store the next hop node they should take to reach both the source and destination nodes.

In Figure 4-2, we see the continuation of our example after Node D, the destination node, receives the RREQ message. The RREP message is unicast back to the source node, Node B, and afterwards, Nodes B and D will store a valid path to each other.

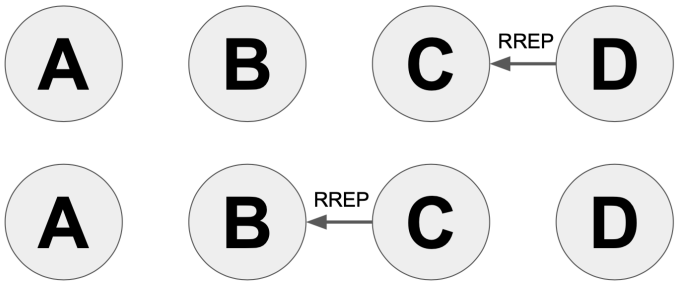

Figure 4-2: RREP message unicast back from Node D to Node B

The RERR message is used when a node loses connectivity to one of its neighbors. When this happens, the node invalidates the route between itself and that neighbor in its own stored routes, and then sends a RERR message to any other neighbors that may have that invalidated route in their saved routes.

4.2.2 Optimized Link State Routing

Optimized Link State Routing (OLSR) is a proactive routing protocol. As introduced in RFC 3626 [5], the two types of messages it uses to discover and disseminate link state information are hello and topology control (TC) messages.

The core functionality of this protocol is made up of neighbor detection, multipoint relay (MPR) selection, topology control message diffusion, and route calculation. During neighbor detection, each node uses hello messages to discover its neighbors and 2-hop neighbors.

Afterwards, the node uses this information to select its set of MPRs from its list of 1-hop neighbors. An important feature of OLSR is MPRs. MPRs are selected nodes which forward broadcast messages during the flooding process. They are the minimum set of nodes needed by a particular node in order to reach all of its possible destinations. MPRs are useful because they help control message overhead by limiting the number of times a message is passed around throughout the network during

flooding. By eliminating duplicate paths, they reduce the total amount of traffic on the network.

The set of MPRs for a node is selected from its set of 1-hop neighbors, and this set must be able to reach all of the node's 2-hop neighbors. This way, when a node sends information to be broadcast, only the selected MPRs for that node re-transmit those packets, while the other 1-hop neighbors process the packets but don't forward them.

In Figure 4-3, a sample network is shown. We use Node A to illustrate our example on selecting MPRs.

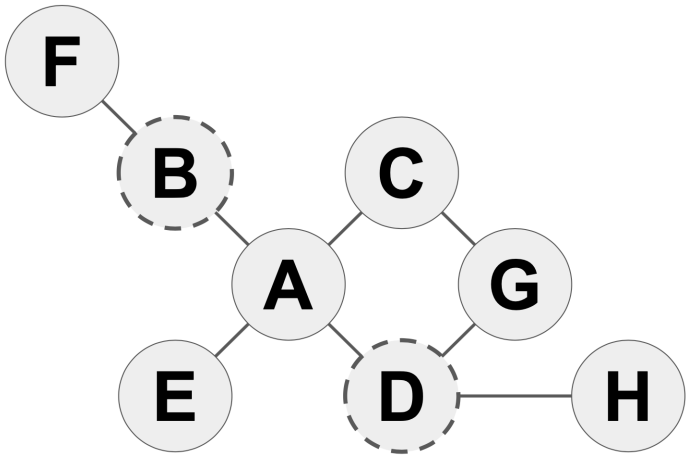

Figure 4-3: Nodes B and D are selected as MPRs for Node A

Node B is selected as a MPR for Node A because it is the only 1-hop neighbor of Node A that can reach Node F, a 2-hop neighbor. Both Nodes C and D can reach Node G, but only Node D can reach Node H. Node D is selected as a MPR, and since it covers Node G as well as Node H, Node C is no longer needed and is therefore not selected. Node E is also not selected because it doesn't connect to any further 2-hop nodes from Node A. Table 4.1 summarizes the relationships between Node A and the other nodes in this network.

Node	**1-Hop Neighbors**	**2-Hop Neighbors**	**MPRs**
A	B, C, D, E	F, G, H	B, D

Table 4.1: Node A's 1-hop neighbors, 2-hop neighbors, and MPRs

During topology control diffusion, each MPR node maintains a MPR selector set, which is the set of nodes that selected said node as an MPR node. The MPR periodically broadcasts TC messages to advertise the links between itself and the nodes in its MPR selector set. TC messages are flooded to all nodes in the network, and they take advantage of MPRs to enable better scalability in the distribution of topology information.

If we look back at Figure 4-3, we established earlier than Nodes B and D are Node A's MPR nodes. During topology control diffusion, when Node A receives the broadcast link information from other nodes, it will forward that information to all of its 1-hop neighbors. However, Nodes B and D know that Node A has selected them as its MPR nodes. After Node A's 1-hop neighbors received the broadcast link information, Nodes B and D will continue forwarding the information as well as incorporating it into their own routing tables, while Nodes C and E will only incorporate it into their routing tables and not forward it.

Finally, route calculation happens at each node. The route to each node is calculated based on the link state information acquired from both hello and TC messages. Each node stores its next hop node for all nodes they can possibly reach in the network, as well as the distance.

Chapter 5

Protocol Evaluation

To simulate a MANET running in an IoBT environment using the different routing protocols, we used a network simulator. The simulator we used is NS-3, a discrete-event network simulator for Internet systems, targeted primarily for research and educational use. NS-3 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use [18].

In this chapter, we perform a comparative evaluation of the performances resulting from a simulated MANET using AODV and OLSR protocols. We first discuss how we set up the simulation, and then describe the results by comparing different characteristics of the simulations.

5.1 Simulating MANETs

To simulate a MANET in an IoBT environment, we experimented with different parameters within NS-3, such as environment size, number of nodes, and transmission power, among others. Besides changing those, we also designed new mobility models to fit the requirements of the IoBT space.

5.1.1 Network Parameters

Table 5.1 below displays the network parameters set in NS-3 for this simulation. For this experiment, the total time is set to be 70 seconds, with 10 seconds of start-up time, which is when no data packets are sent and only routing traffic is propagated throughout the network. The 20 people and 5 vehicle nodes are set in a 400m by 400m square.

The WiFi parameters are set to the default ones in the program, which is ad hoc mode with a 2 Mb/s rate and a Friis propagation loss model [17]. However, the transmit power is changed to 10 dBm to simulate the range of radios and other communication devices used in military missions.

10 of the people nodes send UDP data at an application rate of 1.024 Kb/s each to the other 10 people nodes. This translates to a rate of 2 64-byte packets per second each, with 1200 data packets sent over the course of the entire simulation. This parameter means that the 20 people nodes are both edge nodes (source/destination), as well as infrastructure nodes, while the 5 vehicle nodes are only infrastructure nodes that help forward other nodes' packets. While vehicles may have communication abilities, it is more likely for people to be carrying individual devices and communicating with each other, with the vehicles helping forward messages when needed.

Parameter	**Value**
Simulation Time	70 seconds total, 10 seconds start-up time
Simulation Area	400m x 400m
Number of Nodes	25 total: 20 people, 5 vehicles
WiFi Mode	Ad hoc mode
WiFi Rate	2 Mb/s
WiFi Loss Model	Friis Propagation Loss Model
Transmit Power	10 dBm
Number of Source/Sink Pairs	10
Sent Data Rate	1.024 Kb/s
Packet Size	64 bytes
Protocols	AODV, OLSR

Table 5.1: NS-3 Simulation Parameters

5.1.2 Mobility Models

Besides changing some of the parameters in the simulation, we also developed new mobility models to model how a soldier or vehicle might move. The mobility models are one of the main characteristics of the simulation that distinguish it as an IoBT environment.

For the people nodes, we used the random waypoint mobility model built in to NS-3 [20]. In this mobility model, the object will pick a new waypoint and a new random speed, and then will begin moving towards the waypoint at that constant speed. When it reaches the destination, the process repeats. The new waypoints are picked using the random rectangle position allocator, which essentially picks any random point within a rectangular space [19]. The new speed is a random variable between 0m/s and 3m/s.

This mobility model is suitable for soldiers in an IoBT scenario, because soldiers are likely to be moving constantly on foot. Furthermore, soldiers aren't restricted in where they can move to, and should be able to move freely within the rectangular area.

On the other hand, since vehicles can only travel on roads instead of being able to travel anywhere, we built a grid of roads over the base rectangular area. At any time, a vehicle node has a 4/5 probability of remaining stationary, and a 1/5 probability of beginning to travel down a road. Vehicle speed is set as 14.8m/s.

For the vehicle nodes, we used the waypoint mobility model [21]. This model is similar to the random waypoint model used for the people nodes, except the waypoints are deliberately set, instead of being randomly chosen. This way, we can set the exact waypoints of where a vehicle will travel to, and limit it to only traveling on the grid of established roads.

Table 5.2 below contains a summary of the comparison between the two mobility models.

	People Node	Vehicle Node
Mobility Model	Random Waypoint	Waypoint
Speed	0m/s - 3m/s	14.8m/s
Position	Anywhere	Only on roads
Stationary	Never	Often

Table 5.2: People and Vehicle Mobility Models

5.2 Results

To evaluate the results from the simulation, we used multiple metrics that looked at different aspects of how each routing protocol performed. These metrics can be split into two categories - metrics related to the delivery of data packets, and metrics related to the routing traffic itself.

5.2.1 Data Packet Delivery

The first metric we measured is the number of data packets sent, received, and dropped by the 2 protocols. In Figure 5-1, we see that both routing protocols attempt to send 1200 packets. However, AODV is only able to send around 500 of those while OLSR sends almost all of them. Out of the packets that are sent, only around 100 of the AODV ones are actually received by the destination, while almost 400 are dropped. In contrast, almost all packets are successfully sent and received by OLSR, and only a very small amount are dropped.

OLSR clearly performs better than AODV for this metric. Since OLSR is a proactive and link state protocol, during the start-up time of 10 seconds, each node will obtain a view of the entire network. Once data packets start being sent, all nodes should already have paths to all other nodes in the network already, even though they may be outdated.

On the other hand, since AODV is a reactive protocol, only when a data packet needs to be sent will a valid route be looked for. When a route cannot be found, the packet just won't be sent at all, resulting in the low number of AODV packets that are actually sent. On top of that, many of them are dropped, which may be a

result of high mobility. If the AODV nodes cannot update their routes to be valid soon enough after the mobility causes routes to change, then packets will be dropped when they reach a node that does not hold a valid path to the destination.

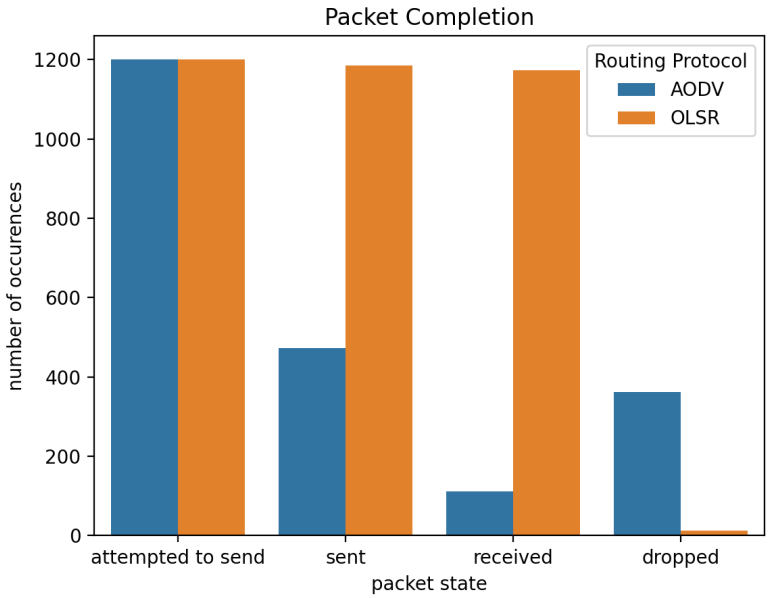

Figure 5-1: Number of data packets sent, received, and dropped for AODV and OLSR

The second metric we measured is the end-to-end delay, which is the amount of time it takes a data packet to reach its destination node after it is sent by its source node. As shown in Figure 5-2, the simulation using the OLSR protocol performs better for this metric. This figure is cumulative and the x-axis is a logarithmic scale. The figure only accounts for packets that are successfully delivered to the correct destination. Over 90% of those data packets in the OLSR simulation are sent in less than a millisecond, while only less than 30% of packets in the AODV simulation are sent in that time frame.

One explanation for why OLSR performs much better than AODV for this metric is that it takes longer for an AODV node to process an incoming packet and then forward it than it takes for OLSR. This might be because the AODV simulation has much more traffic in general, as we will see later in Figure 5-5, and is overwhelmed by the load, or because the AODV protocol requires additional time to calculate the

route at a forwarding node even after a packet is sent.

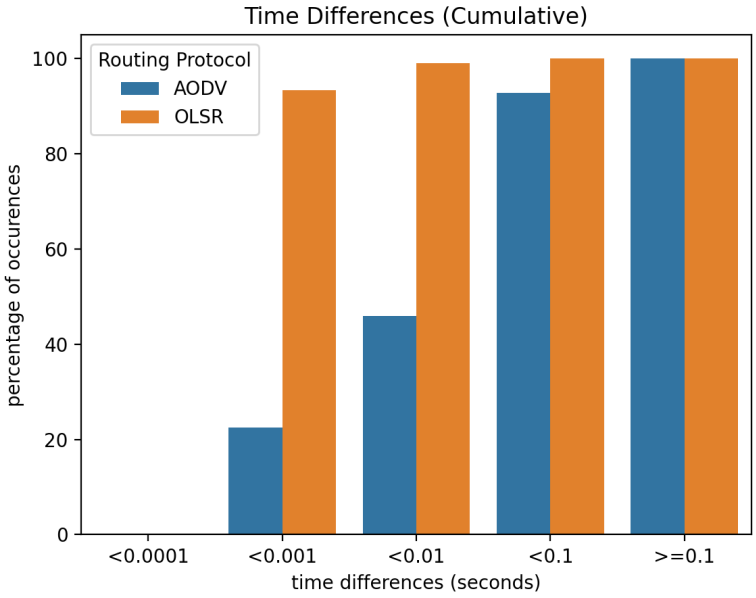

Figure 5-2: Amount of time from when a data packet is sent to when it is received for AODV and OLSR

The final metric we measured in this packet delivery category is the hop count from source to destination. As seen in Figure 5-3, also cumulative, AODV performs better than OLSR in terms of hop count. This figure, like Figure 5-2, only accounts for packets that are successfully delivered. Around half of the data packets in the OLSR simulation are sent using over 10 hops, while that same percentage in the AODV simulation are sent using only 3 or less hops.

This metric seems to contradict the previous metric we measured, since AODV seems to take more time but less hops to send its packets. However, as we saw earlier in Figure 5-1, AODV does not successfully deliver all of its data packets. A possible explanation for the result of this metric is that of the AODV packets that are actually sent, the ones that are received are the ones that are from shorter paths because the longer paths have a higher probability of changing in the middle due to the high mobility of nodes, which would result in the packet being dropped.

In contrast, packets may also be sent along outdated routes in OLSR, but instead of being dropped, they may just end up taking a longer path than needed or even

looping before arriving at the destination. This explains the high hop count from the OLSR simulation.

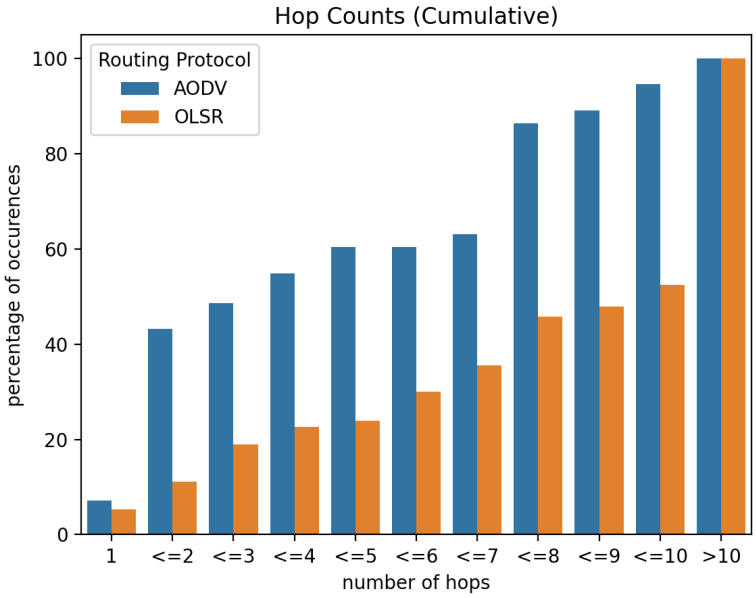

Figure 5-3: Number of hops it takes for a data packet to reach its destination for AODV and OLSR

5.2.2 Traffic Ratios

Besides measuring packet delivery metrics, we also measured metrics related to the amount of traffic sent for each routing protocol. The first metric we measured is the percent of total traffic that is made up of routing traffic. The routing traffic consists of RREQ, RREP, or RERR messages for AODV, and HELLO or TC messages for OLSR. As shown in Figure 5-4, almost all of the traffic seen in the AODV simulation is AODV routing traffic, whereas less than half of OLSR traffic is for routing.

Since the total traffic is made up of routing traffic and data packets, and the number of data packets sent is comparable between the two protocols, Figure 5-4 shows that AODV needs much more routing traffic to handle this type of high mobility traffic than OLSR does. OLSR sends routing traffic periodically, with a set time in between each message, while AODV reacts to changes in the network. Since

the MANET changes often, AODV requires more routing traffic than OLSR to handle the same amount of data packets.

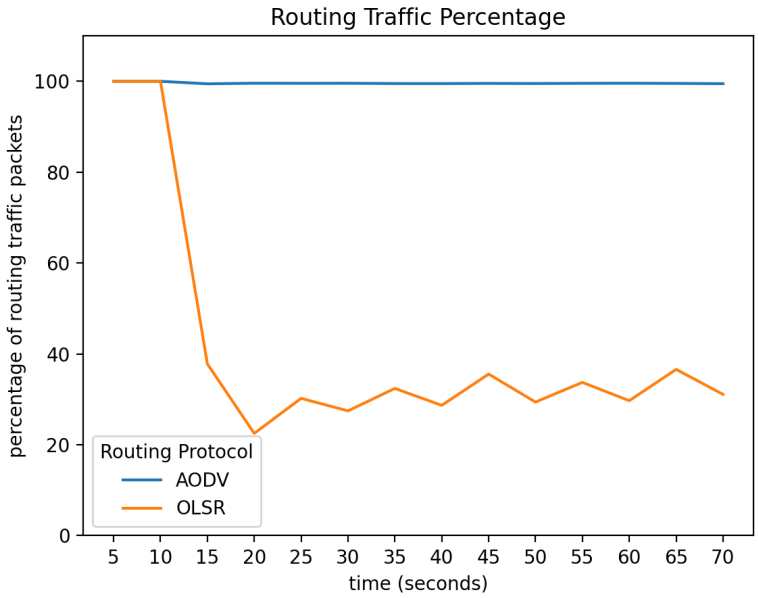

Figure 5-4: Percentage of routing traffic out of total traffic over time for AODV and OLSR

Besides looking at the percentage of total traffic that is made up of routing traffic, we also look at the actual number of packets being sent over time. In Figure 5-5, the actual number of routing messages sent for AODV completely dwarfs that of OLSR. Although it seems like OLSR doesn't send routing traffic at all from the figure, we know from the previous figure that around 30% of total OLSR traffic is routing packets, which further displays the enormous difference between AODV routing traffic and OLSR routing traffic.

The results of the previous graphs showed that AODV needs a large amount of routing traffic to handle this IoBT scenario. However, both simulations attempt to send the same amount of data packets, so the number of RREQ and RREP messages shouldn't result in as large of a difference from the number of OLSR routing messages as it does.

In Figure 5-6 below, we analyze the ratio of RREQ, RREP, and RERR messages sent in the AODV simulation. After 15 seconds in the simulation, RERR messages

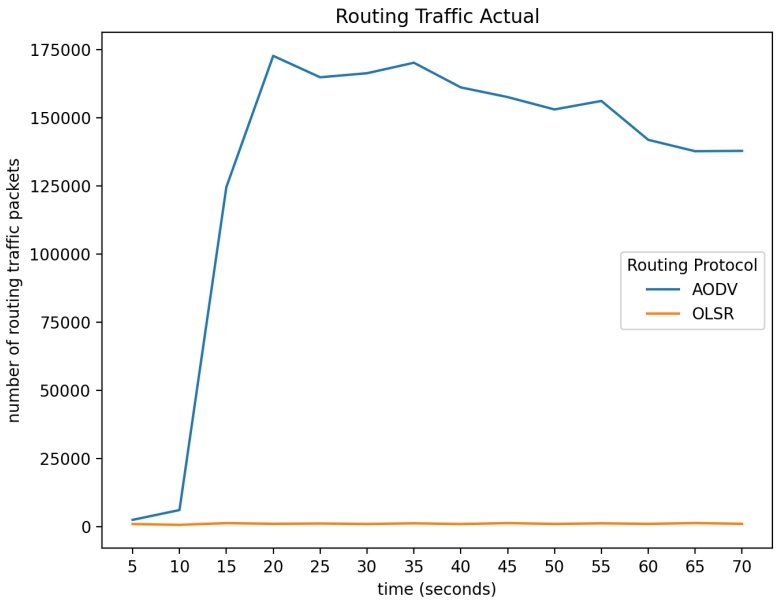

Figure 5-5: Actual numbers of routing traffic packets over time for AODV and OLSR

make up almost all of the routing messages, and RREQ and RREP messages are rarely sent in comparison. This is in line with our earlier deduction that just RREQ and RREP messages shouldn't result in the enormous difference we end up seeing.

Instead, the difference is caused by the RERR messages, which entirely takes over the AODV traffic. The large amount of RERR messages results from constant link changes between nodes, since after a link between two nodes no longer exists, nodes must flood the RERR message regarding this link to all other nodes in the network. This constant re-configuring and flooding causes the large amount of RERR messages, as well as the large amount of AODV routing traffic in general.

5.3 Summary

In summary, each protocol has its strengths and weaknesses. The OLSR simulation had more data packets sent, more packets received, and less packets dropped. Out of the packets sent, OLSR also had packets reaching their destination faster. However, the AODV simulation had lower hop counts out of the packets it sent.

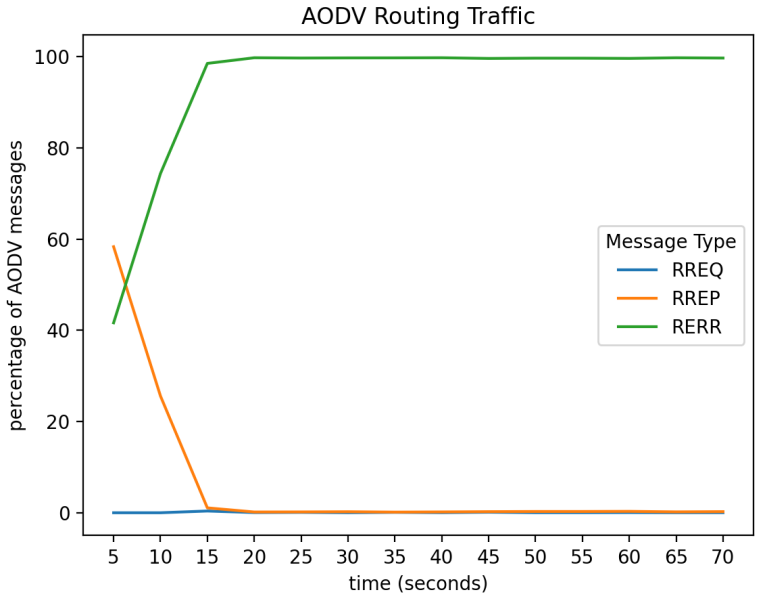

Figure 5-6: Ratio of AODV routing message types over time

In terms of total traffic within the network, OLSR needed less routing traffic than AODV to process the same amount of data packets. Within AODV, the traffic in general was dominated by the routing traffic, and the routing traffic was dominated by RERR messages.

In a situation such as this IoBT scenario with high mobility nodes and constant link re-configuration, OLSR will perform better. However, for networks where paths remain generally constant between nodes, AODV may be the better choice of routing protocol.

Chapter 6

DoS Evaluation

In Section 3.2.2, we introduced a way to categorize DoS attacks on networks by partitioning based on the type of attack. In this chapter, we introduce two of these categories - routing disruption attacks and resource consumption attacks. We also describe specific attacks within these categories and describe the effects they have on both AODV and OLSR.

6.1 Routing Disruption

Routing disruption attacks take advantage of the security vulnerability in MANET routing protocols by attempting to route legitimate data packets in a dysfunctional way [4]. They target the actual routing messages exchanged between nodes using techniques such as sending forged packets, corrupting the information, or just dropping the packets. After the victim node is deceived, the route calculations done at the node will be affected as well.

A black hole attack is a specific type of routing disruption attack in which a malicious node drops data packets instead of forwarding them [11]. The most basic version of this attack occurs when the malicious node takes part in the routing protocol as if it were a normal node, and establishes itself as an intermediate node in some of the paths found within the network. Then, when a data packet is forwarded through any of those paths, the malicious node drops that packet so that it never reaches its

intended destination.

One variation of the basic black hole attack occurs when a malicious node will actively advertise itself as having the shortest path to all destinations within the network. Instead of passively becoming an intermediate node for some paths, it actively tries to become an intermediate node for all the paths. By creating these fake routes, the attacking node ensures that data packets will be sent to it, and it can then drop all of those packets. This variation more heavily affects the network than the basic version does, since a larger amount of packets will end up getting dropped and never reaching their destinations.

Another variation of this attack is when multiple malicious nodes collaborate, rather than only a single node attacking the network. This version is also more dangerous than the basic version, since it is more difficult to detect and prevent.

A black hole attack could target the entire network, or just a single node. If it only targeted a single node, the malicious node would only drop data packets from that node. However, by targeting the entire network, the malicious node can extend its reach to all of the data packets being sent throughout the network, thereby increasing its effectiveness.

6.1.1 AODV

In AODV, black hole attacks are implemented by taking advantage of the RREQ and RREP message types [15]. To implement the version of black hole attack where the malicious node actively promotes itself as always having the shortest path, the malicious node will respond to RREQ messages with a false RREP message saying that the hop count to the destination node is a low enough number such that the node will definitely be chosen as an intermediate node in the path. Usually, this hop count number will be one to represent a short route, and the attacking node will further ensure it succeeds by using a high sequence number, which represents the freshness of the route.

Then, because of this deception, the source node issuing the RREQ will choose the path containing the malicious node as it believes that path to be the shortest

path to the destination. However, when the source node sends data packets through this malicious node, the packets will be dropped. Through this method of responding to RREQ messages, the malicious node is able to take over most routes within the network, and therefore drop most, if not all, data packets that are sent.

The black hole attack is highly dangerous to the AODV routing protocol. A malicious node has the possibility of becoming an intermediate node within all the paths in the network. If that occurs, the node could drop every single data packet sent within the network, which would cause the network to cease operation completely.

6.1.2 OLSR

In the OLSR routing protocol, black hole attacks are implemented differently. Instead of taking advantage of RREQ and RREP messages, the malicious node uses the MPR selection to advertise itself instead. The malicious node will first send false hello messages to its 1-hop neighbors, saying that it has a direct connection to multiple other nodes [16].

During the MPR selection process, the malicious node will be selected as a MPR node for its 1-hop neighbors because of its advertised false connections. The malicious node can include other nodes in the network or even imaginary nodes in its hello messages to be definitely selected as a MPR node. To go one step further, if the malicious node wants to be the only MPR node selected by a node, it needs to include all of that node's 2-hop neighbors in the hello messages it sends out, as well as an imaginary node. The reason an imaginary node is included is because the malicious node will be the only node in the entire network that has a valid path to this imaginary node, so it will definitely get selected as a MPR node.

Once the malicious node has been selected as a MPR node, it will receive both routing messages and data packets from its victim nodes. It can then drop the data packets it receives.

The black hole attack is also extremely dangerous to the OLSR routing protocol. Like in AODV, a malicious node has the ability to slowly integrate itself into the entire network. By sending false hello and TC messages, it can eventually become a

MPR node for all of its 1-hop neighbors, and any data packets forwarded by those 1-hop neighbors will go to the malicious node.

6.1.3 Comparison

In AODV, the malicious node becomes an intermediate node within any paths for which they received RREQ messages. If the malicious node is centrally located within the network, it has the possibility of dropping all packets in the network. However, if the attacking node is on the outside, it may not receive all the RREQs in the network, and therefore may not become part of all the paths that exist.

In OLSR, the malicious node becomes a MPR node for its 1-hop neighbors. If the malicious node is centrally located, then like AODV, it has the possibility of receiving all data packets and dropping them. If it is located near the boundary of the network, then data packets may not be forwarded through any of the malicious node's 1-hop neighbors, and therefore will not reach the malicious node.

Black hole attacks may cause both routing protocols to completely cease operation, but they may also only affect part of the network depending on where the malicious node is located. However, in AODV, an attacker could infiltrate the network in a short amount of time, since the malicious node only needs to respond to one RREQ message with false information before it can successfully drop packets. On the other hand, in OLSR, the malicious node would need exchange multiple hello and TC messages before it can get selected as a MPR node and have data packets forwarded to it.

Therefore, the comparative analysis shows that black hole attacks are more detrimental to AODV than to OLSR routing protocols. Although the final effects are similar for both, the attack needs only a short amount of time to affect AODV, whereas it needs to exchange multiple messages with other nodes before infiltrating a network using the OLSR protocol.

6.2 Resource Consumption

On the other hand, resource consumption attacks aim to consume the resources of its victim nodes, such as memory, network bandwidth, or battery power [10]. This type of attack usually injects extra packets into the network to consume those valuable network resources and increase the load on the network.

A flooding attack is a specific type of resource consumption attack in which malicious nodes make their victims constantly process unnecessary packets, which drains off limited resources. The malicious node floods the network with messages, which affects network operation and consumes resources such as energy and bandwidth.

Flooding attacks, like black hole attacks, can also target either a single node or the entire network. If the attack targets only one node, then that node would be affected and won't be able to operate properly. However, by targeting the entire network, multiple nodes will experience those same effects, which makes the flooding attack more effective.

6.2.1 AODV

In AODV, a flooding attack is implemented by a malicious node flooding the network with a large amount of routing control packets, or data packets [1]. The most common type of routing control packet attack is the route request flooding attack.

For the RREQ flooding attack, RREQ messages may be sent to real destinations, or to imaginary ones. The flooded messages take up many network resources. When the destinations don't exist in the network, none of the other nodes will be able to generate RREP messages to respond to the malicious RREQ messages, which means the RREQ messages would be flooded throughout the entire network without response.

While the network is handling all of these RREQ messages, the real RREQ messages coming from nodes that need to send actual data packets are not processed, and have to wait for resources to free up. This could result in lower throughput and network congestion, as the network cannot transmit any legitimate packets while it

is handling the malicious ones. Other effects could include greater end-to-end delay and routing table overflow. Both computational and power resources may be limited by this attack.

Besides RREQ messages, AODV also uses RREP and RERR messages for routing control. Since RREP messages are only sent in reply to RREQ messages, a malicious node cannot initiate an attack by simply generating more RREP messages.

RERR flooding attacks can occur as well. In Figure 5-6, we saw this phenomenon happen naturally, as the simulated network became overwhelmed by the large amount of error messages. RERR messages have to be flooded to any node that might have the newly disconnected link stored, so this type of routing control message will also easily get flooded throughout an entire network, like RREQ ones.

For the data flooding attack, a malicious node sends large amounts of useless data packets to victim nodes. These excessive packets clog the network and reduce available network bandwidth. Victim nodes will be congested by these useless packets, and won't be able to process legitimate messages. As network bandwidth will be limited as well, nodes besides the designated victim nodes may also be affected.

The RREQ and data packet flooding attacks have a number of negative effects on the network, such as depleting network bandwidth, increasing overhead, depleting memory at nodes, exhausting battery power, and decreasing throughput. When combined together by an attacker, the target network may crash completely.

6.2.2 OLSR

In OLSR, a flooding attack is implemented in generally the same way as it was in AODV - through routing control messages or data packets. The routing control messages in OLSR are hello and TC messages. Since hello messages are only sent to 1-hop and 2-hop neighbors, flooding hello messages will only have the effect of congesting the nodes located close to the malicious node. If those nodes happen to be intermediate nodes for other paths, then those other paths may be affected as well. In general, the scope within the entire network of a hello message flooding attack is small.

TC messages are another type of routing message used within OLSR. They are already flooded to the entire network periodically from each node to ensure paths remain up to date. However, a malicious node could send TC messages continuously instead of periodically to increase the load on the network. The network may become mildly more congested, but the difference between the amounts of TC messages being flooded before and after the attack will not drastically differ, since only one node is maliciously sending fake TC messages, and the network is equipped to handle TC messages from all nodes.

For the data flooding attack, the general process for OLSR is the same as for AODV. When a malicious node sends a large amount of fake data packets, many different resources such as network bandwidth or battery power.

6.2.3 Comparison

In AODV, flooding attacks may happen through RREQ messages, RERR messages, or data packets. For OLSR, these attacks may happen through TC messages or data packets. The effects of a data flooding attack are similar for both routing protocols, but since they use different routing control messages, the effects of flooding those are different as well.

Both RREQ and RERR flooding attacks involve the fake routing message being flooded to the nodes in the entire network, which will have big impact on performance. On the other hand, although TC flooding attacks may also involve a fake message being flooded to the entire network, OLSR is better equipped to handle this type of flooding since it is built in to the routing protocol.

Although both routing protocols' flooding attacks target important resources within the network, there is greater variety within AODV for how a flooding attack could happen. The individual attacks within AODV all have the potential to affect the network more than the attacks within OLSR. Therefore, the comparative analysis shows that flooding attacks are more detrimental to AODV than to OLSR routing protocols.

6.3 Summary

In summary, routing disruption and resource consumption attacks are two categories of DoS attacks. Black hole attacks are a specific type of routing disruption attack, and flooding attacks are a specific type of resource consumption attack. Based on a comparison of the implementation details for each attack, both attacks are actually more detrimental to networks using AODV than those using OLSR.

For the black hole attack, a shorter amount of time is needed to affect AODV networks than OLSR ones. For the flooding attack, there is a greater variety of possibilities for how the attack could happen to AODV networks. Therefore, AODV is generally less resistant than OLSR to DoS attacks.

Chapter 7

Conclusion

DoS attacks are prevalent within IoT systems, as many IoT devices have limited security measures in place. IoBT, a specific portion of the IoT world dedicated to military applications, also suffers from this same problem. Besides the inherently insecure nature of IoBT systems, military missions often involve adversarial conflicts, which make the security problem especially important.

The IoBT world has distinct characteristics. Nodes can have high mobility, and can move continuously within the space. This results in constant link re-configurations, as links between nodes are broken and formed when nodes move. A type of network that can handle these characteristics is the MANET, since it is both decentralized and wireless.

MANETs don't specify a particular routing protocol to use, so there have been different protocols developed to be used specifically within MANETs. The two that we have chosen to analyze are AODV and OLSR, since they are both widely used and each represent a different piece of the protocol space.

Through our comparative study of the routing protocol simulation, we learned that OLSR is better suited to the IoBT situation, particularly because of the high mobility. In contrast, AODV is suited for less mobile networks, where links are changed as often. Separately, we also learned through our analytical study of DoS attacks and its effects on these routing protocols that OLSR is less affected by both black hole and flooding attacks than AODV is. Table 7.1 below summarizes these

results.

	high mobility	low mobility	black hole	flooding
AODV		✓		
OLSR	✓		✓	✓

Table 7.1: OLSR is a better routing protocol for high mobility scenarios, while AODV is better for lower mobility ones. OLSR is less affected and therefore can resist both DoS attacks more effectively than AODV can.

7.1 Future Work

The first step to further the work done in this paper is to simulate the DoS attacks on the routing protocols using a simulator such as NS-3. This can provide simulated results and figures to support the analytical comparison we have conducted in this paper.

The scope of this work can be expanded in the future as well. Besides black hole and flooding attacks, there are many other DoS attacks that can greatly affect networks. These attacks should be analyzed and simulated as well to further compare how different routing protocols are affected.

Outside of DoS attacks, further work can be conducted on other routing protocols besides AODV and OLSR. All protocols are different and have differing advantages and disadvantages, so researching more routing protocols will give users a better view of which protocol they should pick for their network.

Finally, the idea of IoBT can be further developed. Currently, the main characteristic of the network that embodies this sort of system is the specific mobility models used for people and vehicles. The military battlefield is made up of many other entities besides those two, such as planes and drones, so creating more mobility models will allow simulations to more accurately depict the reality of IoBT.

Bibliography

[1] Mahmoud Abu Zant and Adwan Yasin. Avoiding and isolating flooding attack by enhancing aodv manet protocol (aif_aodv). *Security and Communication Networks*, 2019, 2019.

[2] Mona N. Alslaim, Haifaa A. Alaqel, and Soha S. Zaghloul. A comparative study of manet routing protocols. In *The Third International Conference on e-Technologies and Networks for Development (ICeND2014)*, pages 178–182, 2014.

[3] Elisa Bertino and Nayeem Islam. Botnets and internet of things security. *Computer*, 50(2):76–79, 2017.

[4] Ruiliang Chen, Michael Snow, Jung-Min Park, M. Tamer Refaei, and Mohamed Eltoweissy. Nis02-3: Defense against routing disruption attacks in mobile ad hoc networks. In *IEEE Globecom 2006*, pages 1–5, 2006.

[5] Thomas H. Clausen and Philippe Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626, October 2003.

[6] Dr. Scott M. Corson and Joseph P. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, January 1999.

[7] Samir R. Das, Charles E. Perkins, and Elizabeth M. Belding-Royer. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[8] Savita Gandhi, Nirbhay Chaubey, Naren Tada, and Srushti Trivedi. Scenario-based performance comparison of reactive, proactive hybrid protocols in manet. In *2012 International Conference on Computer Communication and Informatics*, pages 1–5, 2012.

[9] Albert Greenberg, Gisli Hjalmtysson, David A. Maltz, Andy Myers, Jennifer Rexford, Geoffrey Xie, Hong Yan, Jibin Zhan, and Hui Zhang. A clean slate 4d approach to network control and management. *SIGCOMM Comput. Commun. Rev.*, 35(5):41–54, October 2005.

[10] Ashish Kumar Jain and Vrinda Tokekar. Classification of denial of service attacks in mobile ad hoc networks. In *2011 International Conference on Computational Intelligence and Communication Networks*, pages 256–261, 2011.

[11] Danista Khan and Mahzaib Jamil. Study of detecting and overcoming black hole attacks in manet: A review. In *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, pages 1–4, 2017.

[12] Alexander Kott, Ananthram Swami, and Bruce J. West. The internet of battle things. *Computer*, 49(12):70–75, 2016.

[13] Jelena Mirkovic, Alefiya Hussain, Brett Wilson, Sonia Fahmy, Peter Reiher, Roshan Thomas, Wei-Min Yao, and Stephen Schwab. Towards user-centric metrics for denial-of-service measurement. In *Proceedings of the 2007 Workshop on Experimental Computer Science*, ExpCS '07, page 8–es, New York, NY, USA, 2007. Association for Computing Machinery.

[14] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2):39–53, April 2004.

[15] Abdellah Nabou, My Driss Laanaoui, and Mohammed Ouzzif. Evaluation of manet routing protocols under black hole attack using aodv and olsr in ns3. In *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 1–6, 2018.

[16] Abdellah Nabou, My Driss Laanaoui, and Mohammed Ouzzif. New mpr computation for securing olsr routing protocol against single black hole attack. *Wireless Personal Communications*, 117(2):525–544, 2021.

[17] NSNAM. Ns-3 friis propagation loss model. `https://www.nsnam.org/doxygen/classns3_1_1_friis_propagation_loss_model.html`.

[18] NSNAM. Ns-3 homepage. `https://www.nsnam.org/`.

[19] NSNAM. Ns-3 random rectangle position allocator. `https://www.nsnam.org/doxygen/classns3_1_1_random_rectangle_position_allocator.html`.

[20] NSNAM. Ns-3 random waypoint mobility model. `https://www.nsnam.org/doxygen/classns3_1_1_random_waypoint_mobility_model.html`.

[21] NSNAM. Ns-3 waypoint mobility model. `https://www.nsnam.org/doxygen/classns3_1_1_waypoint_mobility_model.html`.

[22] He Xin. Introduction of centralized and distributed routing protocols. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 2698–2701, 2011.

[23] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, 2014.