ABSTRACT

Secure Neighbor Discovery in Directional Wireless Ad Hoc Networks

by Jessica Vazquez-Estrada

Wireless ad hoc networks (WANETs) are an essential development in providing high-speed data transfer in areas with little to no infrastructure. The conjunction of this technology with free space optical (FSO) transceivers has not only increased the speed of communication but has also greatly decreased the cost of implementation. Because FSO transceivers are highly directional, the problem of neighbor discovery in such systems has posed challenges in accuracy and runtime. In this thesis, we produce a novel neighbor discovery protocol using a supplementary omnidirectional channel and integrate an attack-detection method against several common network-layer attacks. We present an innovative approach that utilizes a low-bitrate, long-range (LoRa) omnidirectional communication channel to assist in coordinating the neighbor discovery process, allowing for the synchronization and establishment of directional FSO links among nodes. Secondly, provide a solution that utilizes the inherent properties of directional transceivers in order to implement attack detection in the neighbor discovery process.

Secure Neighbor Discovery in Directional Wireless Ad Hoc Networks

A Thesis / Thesis Proposal

Submitted to the

Faculty of Miami University

in partial fulfillment of

the requirements for the degree of

Master of Science

by

Jessica Vazquez-Estrada

Miami University

Oxford, Ohio

2023

Advisor: Dr. Suman Bhunia

Reader: Dr. Khodakhast Bibak

Reader: Dr. Honglu Jiang

This Thesis titled

Secure Neighbor Discovery in Directional Wireless Ad Hoc Networks

by

Jessica Vazquez-Estrada

has been approved for publication by

The College of Engineering and Computing

and

The Department of Computer Science & Software Engineering

Dr. Suman Bhunia

Dr. Khodakhast Bibak

Dr. Honglu Jiang

Table of Contents

List of Tables

List of Figures

Acknowledgements

First I would like to thank Dr. Suman Bhunia for recruiting me to his team as an undergraduate and introducing me to the world of computer science research. As well as for his continuous support and advice during my academic career. I would also like to thank Dr. Khodakhast Bibak and Dr. Honglu Jiang for taking the time to be on my graduate committee. Lastly, I would like to thank my parents who have always supported me to pursue my passions.

Chapter 1

Introduction

In the last few decades, the demand for high-speed wireless data transfer rates has grown significantly. Traditional radio frequency (RF)-based omnidirectional communication systems such as WiFi or cellular communication cannot achieve such high speed communication. Directional communication such as free-space-optical (FSO), millimeter-wave and terahertz communication have demonstrated the potential to help solve the problem of high data rate requirement [1, 2, 3, 4, 5]. FSO communication has gained an increase in interest due to its high-speed data transfer rate in conjunction with with its low-cost. In addition to high bit rate, FSO transceivers possess high gain properties which allow them to extend to much longer ranges compared to RF transceivers. FSO networks are a valuable asset in military and security applications due their invulnerability to electromagnetic and radio frequency interference, making them immutable to active attackers. Furthermore, the high directionality of FSO transceivers minimizes the probability of packet collision and enhances signal security. Moreover, higher spatial reuse can help in establishing multiple parallel communication links with different neighbor nodes and thus enable much larger bandwidth compared to RF. The following chapter outlines the motivation for improving systems that utilize such technologies as well as introduces the problem of neighbor discovery and network security in wireless ad hoc networks.

1.1 Motivation

The limited coverage of directional transceivers makes their positioning a crucial aspect of FSO system design. For successful neighbor discovery and communication initiation, two FSO transceivers must establish line-of-sight (LOS) with each other. However, in networks where nodes lack prior knowledge about each other's locations, LOS establishment or neighbor discovery becomes increasingly challenging. Previous research has explored protocols in which nodes are oblivious to one another, meaning they have no prior knowledge of each other's locations. However, these protocols do not guarantee termination within a reasonable timeframe [6]. Moreover, random-based protocols fail to ensure the discovery of any neighboring node [7].

Although the directional transceivers provide additional layers of security when compared to RF, WANETs using FSO are still vulnerable to a variety of different attacks such as relay and wormhole attacks. These attacks are aimed to steal and destroy data as well and interrupt communication. Because WANETs are able to be deployed quickly and have flexible locations, they are the prime candidate to be used in military and maritime communication. In these applications the defense and reliability of the network could be crucial to saving lives. Therefore, the progression in the research of security and efficiency in these networks is vital.

1.2 Contributions

To address the issues outlined in the motivation, we propose combining a supplementary initialization channel with a leader election algorithm to ensure neighbor discovery among multiple nodes. A low-bandwidth omnidirectional channel, facilitated by LoRa technology, assists nodes in coordination. We propose to investigate the design of an innovative protocol that guarantees neighbor discovery with minimal delay.

Each node is equipped with multiple highly directional FSO transceivers which can electronically steer its FSO beam by switching between transceivers to scan the surrounding 360° space. We employ leveraging of the electronic steering capability to control the communication direction of the nodes to addresses the problem of neighbor discovery and LOS detection for link establishment. Additionally, we propose using the properties of directional transceivers in conjunction with the location data provided by the omnidirectional channel to detect attacks from malicious nodes in the network. Lastly, we develop a prototype and validate its effectiveness through experimental results.

The main contributions of this research are listed below.

- We propose a novel method for neighbor discovery for highly directional FSO transceivers.
- The proposed method guarantees neighbor discovery within one 360° beam sweep.
- We present a proof-of-concept prototype using an omnidirectional LoRa[8] transceiver and multiple IrDA3 Click [9] transceivers.
- Secure neighbor discovery protocol with attack detection based on directional transceivers and synchronization using LoRa.
- Implementation of the proposed protocol in Python.
- Simulation results of the protocol and its performance.

Chapter 2

Background & Related Work

The following section provides an overview of the techniques utilized in our proposal as well as notable works in literature that contribute to the ongoing challenges in our research area.

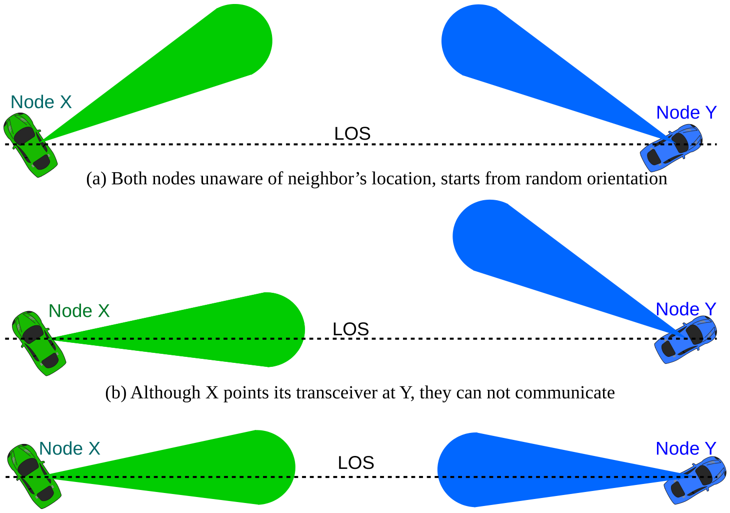
2.1 Wireless Ad Hoc Networks with FSO Transceivers

The wireless ad hoc network is a type of network that is decentralized. Meaning, it does not make use of centralized network devices such as routers or wireless access points to forward data. Thus, the configuration necessary to deploy these networks is minimal. This makes them an ideal choice for communication in applications in that lack infrastructure, such as, maritime, military, search and rescue, and underdeveloped urban areas [10]. WANETs communicate using methods that propagate through the air such as radio frequency (RF) or free-space-optical (FSO) technology, which uses infrared or LEDs to send and transmit data. As the demand for a higher speed data rate increases, FSO is becomes increasingly more attractive due to its lower cost and wider bandwidth compared to RF [11]. In fact, one article cites that the U.S. military were often vulnerable to enemy attacks while spending many hours downloading data [12] The bandwidth of FSO is estimated to be between 10 to 1000 times wider than that of RF [13]. Lastly, FSO transceivers are regarded to be more secure when compared to RF due to their invulnerability to electromagnetic interference.

FSO transceivers come in two forms. Omnidirectional transceivers are able to cast their range equally in all directions while directional transceivers are only able to transmit in one direction at one time. Directional antennas offer several key advantages over omnidirectional antennas, particularly in terms of signal strength, collision reduction, and security. By focusing their radiation pattern in a specific direction, directional antennas are able to transmit and receive signals over greater distances and possess higher gain, leading to improved signal coverage and quality. This property increases the probability of a node receiving unwanted communication, resulting in packet collision. [14]. Directional transceivers are usually implemented with a steering method in order to achieve adequate spatial coverage. In some cases, the transceiver is rotated using a mechanical arm. In other cases, the directional beams can be electronically steered by activating and deactivating strategically placed transceivers.

2.1.1 Neighbor Discovery

Nodes in a WANET are known to be dynamic in the sense that they can change location and connect/disconnect from the network. This behavior presents a challenge to design an effective routing protocol that keeps track of all nodes to create an efficient path from source to destination. This problem is known as neighbor discovery and although the use of directional antennas in WANETs provide several benefits, their focused beams coupled with the lack of a central forwarding device, can make it even harder for the nodes in the network to discover each other. Because directional transceivers can only point in one direction, both the sender node and the receiver node must be in line-of-sight (LOS) with one another in order for the communication to be successful. Figure 2.1 depicts the problem of establish LOS between two nodes.



(a) Both nodes unaware of neighbor's location, starts from random orientation

(b) Although X points its transceiver at Y, they can not communicate

(c) Nodes can only communicate iff both points their transceivers towards each other at the same time

Figure 2.1: Problem of finding LOS for neighbor discovery. Both X and Y are equipped with multiple FSO transceivers but can communicate through only one active transceiver. For effective communication, both X and Y need to coordinate and select appropriate transceivers through which they can communicate with each other.

Neighbor discovery in systems with highly directional transceivers has resulted in many studies. A study showed [15] that, although omnidirectional transceivers were initially believed to have faster discovery times than directional transceivers, directional antennas can actually yield better performance. This is because omnidirectional transceivers are more prone to packet collision and unwanted interference, as they can transmit and receive in all directions. Conversely, directional transmitters are less susceptible to interference, offer enhanced signal security, and have a longer communication range [15].

Oblivious neighbor discovery protocols, which assume that nodes in the system lack prior knowledge of their neighbors' locations are proposed for nodes with mmWave transceivers [16, 17, 6]. While these methods guarantee discovery within a bounded time period, the average discovery delay is significantly long. Another asynchronous design [18] uses directional transmitters and omnidirectional receivers but fails to ensure discovery within a bounded time. Due to their oblivious nature, all these protocols result in lengthy discovery times. In [19], a discovery algorithm was proposed that relies on nodes rapidly switching between transmitting and receiving modes, with GPS-clock synchronization being a key assumption for this highly directional LOS discovery method. Similarly, protocols involving random selection of transceiver positions cannot guarantee neighbor discovery [7].

Efforts have been made to reduce discovery times by developing protocols assisted by low-bandwidth omnidirectional technology. In [20], a neighbor discovery method for a 3D drone network is proposed, where nodes scan the surrounding area using a specialized spiral path to ensure all neighbors are discovered. In [21], an FSO communication module is presented, which employed MicroElectro Mechanical Systems (MEMS) consisting of programmable micromirrors to align the directional beams.

2.2 Security in WANETs

This section summarizes a variety of previous studies involving potential threats and solutions in WANET security. This section will be organized as follows:

1. *Relay Attacks:* This section analyzes papers which find relay attacks as a threat to vehicle wireless ad hoc networks as well as papers that offer defenses against the attacks.

2. *Wormhole attacks:* This section analyzes literature on wormhole attacks and their threat to wireless ad hoc networks networks. In addition, the most relevant papers which offer defenses to these attacks are explored.

2.2.1 Relay Attacks and their Defenses

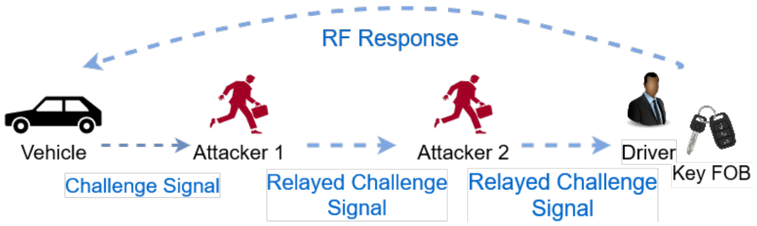


Figure 2.2: Relay attack in a modern vehicle.

The term relay attack, depicted in Figure 2.2, was first coined in a paper [22] demonstrating how to carry out the attack in a wireless network. Relay attacks make use of vulnerabilities related to the inherent properties of optical technology. Meaning, no cryptographic computations are used to carry out the attack. The attacker simply needs two malicious actors to position itself in the network, posing as a node, and use similar hardware to redirect authenticated signals to himself. It can re-transmit the incoming signal in order to pose as a trusted part of the network. In the next few sections, relay attacks and their use in gaining unauthorized access to vehicles is analyzed in various studies. These vehicles are part of a special class of WANETs called mobile ad hoc networks (MANETs). Table 2.1 summarizes each of the analyzed defenses as well as their disadvantages.

Key shielding with Faraday Cage

The analysis in [23] outlines various kinds of solutions that have historically been used to reduce incoming relay attacks. The most obvious and simple method known is the Faraday cage. The Faraday cage, which is made from aluminum, possesses signal shielding properties. In practice, a key fob that is used to unlock a vehicle in a MANET would be encased with a faraday cage while not in use to prevent attackers from gaining access to vehicle communications. On the surface, a faraday cage may seem like a quick and guaranteed safeguard against relay attacks, however, it should be noted that a Faraday cage does not entirely and perfectly block 100% of signals. Rather, aluminum only attenuates signals [23] to a certain degree. Additionally, the user must ensure that their key is completely enclosed in the Faraday cage. If this measure is not taken, signals could still reach the fob and be manipulated by malicious actors. Another disadvantage of the faraday cage is that many modern vehicles make use of passive keyless entry, which provides convenience to drivers by not needing to take out a key fob to unlock the vehicle. Instead, the driver may only need to pull the door handle while the key is stored away to unlock the vehicle. Solutions like the faraday cage and others discussed in the following paragraphs detriment the convenience of keyless entry in exchange for some security.

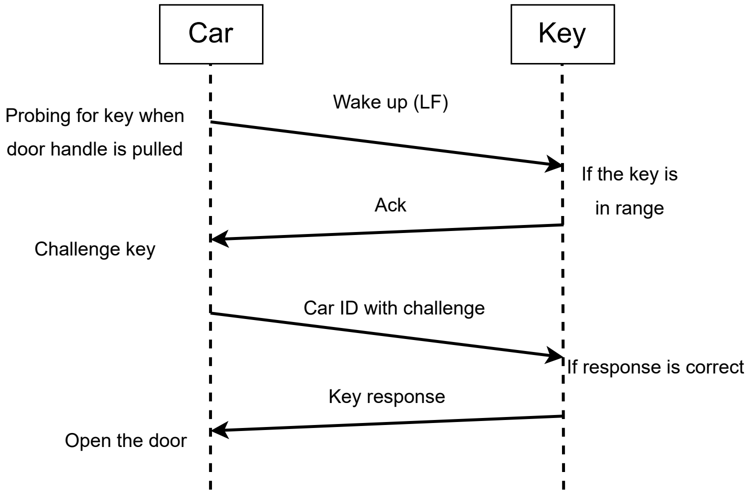


Figure 2.3: Timing diagram of challenge-response protocol in a keyless vehicle

Defense Using Signal Strength

The research in [24] proposes a method to avoid relay attacks by using the signal strength information of the communication (RSSI) to detect malicious signals in scenarios that use keyless entry with keys fobs to unlock vehicles in mobile networks. In these networks, a typical challenge-response protocol, shown in Figure 2.3, is used to authenticate owners of the vehicle to enter and start the vehicle. In this method, the vehicle sends a ”challenge message” containing a random number to the owner’s key fob when the challenge is triggered by some action like pulling the door handle. The key fob device then encrypts the challenge message using an encryption key that is stored

Table 2.1: Summary of defenses against relay attacks.

Defense	**Description**	**Disadvantage**
Key shielding	Uses an RF-shielding metallic container to store the key.	Inconvenient is keyless entry vehicles and does not block 100% of signals.
Electronic Immobilizer	An electronic security system that uses a pin-number to unlock the vehicle.	Requires secrecy of installment, cryptographic attacks exist to crack immobilizers.
Sleeping motion-sensitive key fobs	Allows the key fob to temporarily stop receiving signals during a ”sleep mode” when the driver is not near.	Key fobs that are in motion are still vulnerable.
Defense using RF Signal Strength	Uses the signal strength to determine how far away the key is from the car. The car only unlocks if the key is less than 1m away.	With high quality equipment, the signal strength can be cloned.
Multi-channel Communication	Uses an additional channel to send a verification request to the driver.	Requires a human to verify unrelayable channel message.

within the device. The vehicle encrypts its own challenge message using the same encryption key and awaits a response from the key fob containing the encrypted message. If the response matches the vehicle's calculations, then the request is considered valid and the vehicle will unlock.

Due to the nature of this protocol, the owner of the vehicle is expected to be near the vehicle when he intends to unlock it. A relayed signal, transmitted by an attacker, would then have to travel a longer distance. Thus, it is proposed that if the RSSI value of the signal is below a certain threshold, an attack is detected. This simple solution can unfortunately be easily bypassed. If the attack is in possession of a high-quality waveform generator, antenna, and amplifier, the attack will be able to mimic the minimum signal strength requirement.

Electronic Immobilizers

Emerging devices called electronic immobilizers, presented in [25], are designed to support an additional layer of security for a vehicle. Most commonly, immobilizer security systems provide PIN authentication method when unlocking the vehicle. Using this method, the only way an attacker will be able to steal the vehicle is by physically moving it. In addition, the convenience brought by the design of the keyless entry system is greatly diminished by the installment of immobilizers. Each time the driver wants to unlock the vehicle they must take the time to enter a PIN number. In the worst-case scenario, if the driver manages to lose the PIN, they will not be able to access the vehicle. Although there may be instances in which the cost is worth the extra protection, immobilizers' high cost, coupled with the inconvenience, make them a less desirable option in terms of design. Furthermore, the success of an immobilizer relies on the secrecy of its installation. If the attacker has knowledge that an immobilizer has been installed in a vehicle there have been recorded lock-picking attacks on the electronic security system. [26].

Sleeping motion-sensitive key fobs.

Motion detection has been identified as a reasonable approach to dealing with relay attacks [27]. This method is a kind of hardware modification that involves inserting an accelerometer into a key fob in order to detect motion in an attempt to lower attack probability. The additional features allow the key to be sent into ”sleep mode” in which the key’s ability to send and receive signals is turned off if it is immobile for a certain period of time. The key possesses a motion sensor and can be awakened by the driver when it is taken out to unlock the vehicle. With the help of motion sensing, the provided convenience of the keyless entry system is preserved, however, it would require the key to be stationary when not in use. If the driver is doing an activity, this defense is virtually useless.

Defense using time of flight

Similarly to [24], [28] proposes a defense that uses the round trip time of the challenge-response technique to detect a relay attack. The time estimate of this protocol can is measured and is used as a benchmark to authenticate future signals. The authors indicate that the accuracy of this time estimate is heavily dependent on the bandwidth of the system. Applications that make use of directional transceivers, however, are chosen for their low cost. Choosing other methods of transition that possess higher bandwidth could cost significantly more and therefore misuse the benefits of directional communication.

Defense using multi-channel communication:

There remains a critical issue with the previous two proposed defenses [24] [28]. These detection methods do not detect if the vehicle is communicating with a trusted user. They simply detect whether the signal coming from too far away, a situation in which the true owner may find himself. In order to distinguish a trusted node from an attacker, [29] proposes that an un-relayable channel be used to communicate some physical one-way function. However, this solution implies the need for a human verifier and therefore is not always possible or convenient for mobile vehicle networks.

2.2.2 Wormhole Attacks and their Defenses

First introduced to scientific literature in 2002, a wormhole attack involves [30] inserting two malicious nodes into a multi-hop network that are connected by a direct link called a tunnel. Figure 2.4 provides a simple construction of a wormhole attack. During the routing process, one malicious node receives packets from victim nodes, tunnels them to the second malicious node which in turn replays the packets to the next node in the route. To the other nodes in the network, it may seem that these nodes offer a faster route to their destination and therefore opt to use the malicious nodes to route packets. This replaying of information is called ”tunneling” and can be a serious threat if exploited by an attacker. If the malicious node advertising a more efficient route attracts packets from other nodes in the network, the attacker may choose to eavesdrop the packets or drop these packets in order to perform a continuous denial of service attack known as a black hole attack.

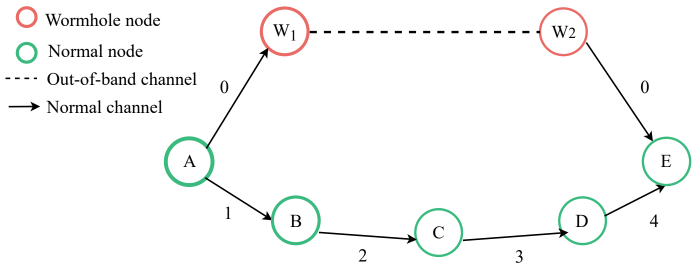


Figure 2.4: Wormhole attack

Packet Leashes

The standard defense against wormhole attacks is the concept of a packet leash[30]. A packet leash is used to restrict the maximum distance a packet can travel during transmission. A timestamp is usually used to keep track of the distance traveled. Firstly, the source node will record the time at which it sends the packet. Next, the destination node will check to see if the packet has traveled too far a distance, given the total time from source to destination and the estimated transmission time of the network. If it determines this to be the case, a tunnel is likely the cause of this increased transmission speed and the attack will be detected. The authors of this proposed method, however, acknowledge that for this calculation to be accurate, nodes must have highly synchronized clocks. The reason for this is that RF signals travel at the speed of light and therefore require a high degree of precision in the recording of the timestamp to reduce the probability of reporting false positives. Additionally, the timestamp information must be protected by an authentication scheme such as a digital signature, and significantly increase the required storage space[31]. Finally, packet leashes do not provide any information on the location of the malicious nodes.

Defense using Relative Direction

The defense proposed in [32] makes use of the properties of directional transceivers. In this system, each node keeps information about its neighboring nodes and the direction they transmit information. With this information, the receiving node knows from which direction it should receive packets from the transmitting node. If the receiver receives it from a different direction, then it detects the attack. This method does not prevent all wormhole attacks, in fact, one-sixth of wormhole attacks would not be detected by this scheme. The authors of the paper recognize this shortcoming and provide an upgraded version of this protocol. In the simple version, neighboring nodes can only detect wormhole attacks if both nodes are in the same direction as the tunnel endpoint nodes. In the upgraded protocol, some nodes are made ”verifiers” to determine the legitimacy of communication between a sender node and a receiver node. These verifiers must receive signals from the sender from a different direction than the receiver. They must also receive signals from the receiver in a different direction from the sender. The verifier will notice that the direction the wormhole endpoint transmits is not the same as the expected transmission direction of the trusted sender node. This method improves the number of detected attacks, but it still does not detect all wormhole attacks, especially those in which the sender and receiver are very close to one another.

Machine Learning Approaches

More recently, machine learning has emerged as a tool of growing interest to detect wormhole attacks. One study explores machine learning as a defense mechanism in vehicle wireless ad hoc networks. In order to compile a training data set, a series of simulations in which two nodes in the network were selected to be malicious nodes were run. Kernel and nearest-neighbor nonparametric regression and support-vector networks, two state-of-the-art machine learning algorithms, were used for testing. The results of this study show that both models had a high accuracy of 99% in detecting wormhole attacks.

Chapter 3

Proposed system Design

In this chapter, the assumptions necessary for our system model are addressed. This chapter also includes a detailed explanation of of the system components and definition of communication protocols for both single and multiple neighbor discovery. Lastly, secure communication and attack detection for the system are presented.

3.1 Assumptions

- *Nodes:* Each node exist in a 2D ad hoc network. Each node can communicate within the range of its transceiver.
- *Directional transceivers:* Each node has a circular structure equipped with multiple directional FSO transceivers The number of transceivers is dependent on the width of the communication beam which is modeled as the divergence angle β in Figure 3.2. The transceivers are laid out to cover all directions for transmission and reception to achieve maximum spacial coverage.
- *Electronic beam steering:* The direction of a node's transmission/reception is accomplished by activating a specific transceiver at a specific time.
- *Omni-assisted channel:*. In the beginning of the neighbor discovery process, an additional side-channel (LoRa) is used to synchronize the LOS discovery using the FSO transceiver. LoRa provides a throughput of less than 20 KBps [8], which can not provide a sufficient data rate to carry out main communication.
- *Compass:* Each node is equipped with a compass in order to determine the direction/transceiver using which it will begin scanning the surrounding space. We are not relying on GPS information because it works poorly inside a building and the precision is not very accurate.

Our proposed neighbor discovery method does not make use of GPS-clock synchronization. Rather, the location detection for the nodes is facilitated by an omni-assisted long range channel. The timing diagram of the proposed neighbor discovery protocol is depicted in Figure 3.1.

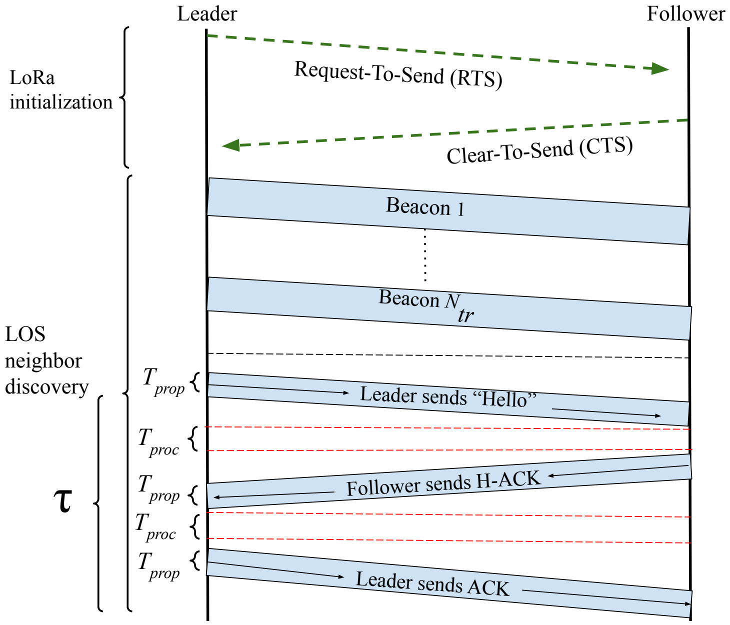


Figure 3.1: A timing diagram of the proposed neighbor discovery protocol

3.2 Number of Transceivers

The FSO transceivers are maneuvered using electronic beam steering. The number of transceivers present on a specific node depends on the transceiver's beam width. A reduced beam width necessitates a greater number of transceivers to guarantee maximum communication coverage encompassing the entire 360-degree space surrounding the node. Consequently, this ensures that other nodes can locate a neighboring node, irrespective of its location. Given a beam divergence angle denoted as β, the number of transceivers can be calculated through the following method:

$$N_{tr} = \lceil(360/(2 \times \beta)\rceil, \tag{3.1}$$

The angle at which the center line of these transceivers should be placed is determined as:

$$\theta_i = i \times \frac{360}{N_{tr}} + \beta, \quad i = 1, 2, ..., N_{tr}. \tag{3.2}$$

Therefore, for $2\beta = 45°$, each node should have eight transceivers at angles 22.5° , 67.5° , 112.5° , 157.5° , 202.6° , 247.5° , 292.5° and 337.5°. The placement of transceivers and steering method is modeled in Figure 3.2

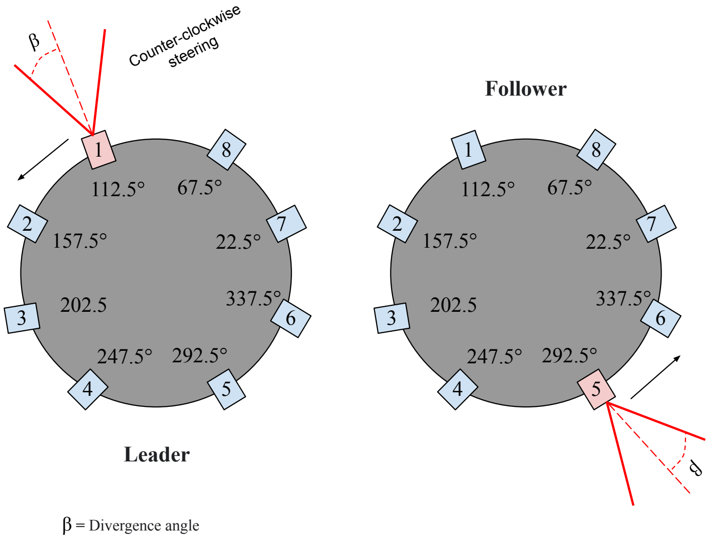


Figure 3.2: Two nodes with a beam width $2\beta = 45°$ are equipped with 8 FSO transceivers.

3.3 Communication Protocol

3.3.1 Initialization

The protocol begins with an initialization phase in order to synchronize the nodes in the network. In the initialization phase, the sender node initiates the communication by through the supplementary omnidirectional channel to send an request-to-send (RTS) beacon message. If another neighbor node exists in the vicinity, upon receiving the RTS, the neighbor sends back a clear-to-send (CTS) acknowledgement. Once the existence of a neighboring node is found, the LOS neighbor discovery process.

3.3.2 Single Neighbor Discovery

In the LOS neighbor discovery phase, the node that initiated the communication, known as the Leader node, begins scanning by activating the transceiver facing north and transmitting a beacon message. It transmits a *Hello* beacon through the FSO transceiver and waits for the *H-Ack* for a wait period. If it does not receive the *H-Ack*, it switches to the adjacent transceiver in a counter-clockwise fashion, hence the term electronic switching/steering. Similarly, the receiving node, known as the Follower node, activates its transceiver facing south for a wait period and repeats the process for the adjacent transceivers. The Leader continuously sends a *Hello* message in the direction it is transmitting and waits for a response. The Follower waits to receive the *Hello* message. Once the beams are aligned (i.e. the transceivers face each other in LOS), the *Hello* message can be received by the Follower and it will stop scanning. The Follower then sends an *H-Ack* message back to the Leader. When the Leader successfully receives an *H-Ack* message in return, it also stops scanning. Finally, the Leader sends a last acknowledgment message, *Ack*, back to the Follower. The

Algorithm 1: Neighbor Discovery using a omni-directional helper channel

```
Leader sends RTS and waits for CTS
if Leader receives CTS then
    Divergence Angle $\beta$
    Number of transceivers $N_{tr}$
    $leaderAngle \leftarrow 1$
    $followerAngle \leftarrow \lfloor \frac{N_{tr}+1}{2} \rfloor$
    while $i \leq N_{tr}$ do
        $Leader$ sends ”Hello” and waits for ”H-ACK”
        if $Leader$ receives ”H-ACK” then
            Reply with ”ACK” and Stop
        end if
        Follower waits for ”Hello”
        if ”Hello” received by $Follower$ then
            Reply with ”H-ACK” and wait for ”ACK”
            if ACK is received by $Follower$ then
                Follower Stops
            end if
        end if
        $leaderAngle++$
        $followerAngle++$
    end while
end if
```

completion of this three-way handshake confirms that neighbor discovery is complete.

In Figure 3.2, the transceivers are numbered 1 to N_{tr}, in order to portray the cyclical activation of transceivers. Here, the Leader node begins by activating transceiver 1 and the Follower nodes begins by activating transceiver 5. In this example, the two nodes are able to communicate with each other when transceiver 7 is activated for both nodes.

The aim of the research is to develop a novel neighbor discovery system that is more efficient that current methods in literature. Additionally, the neighbor discovery scheme should take into consideration common vulnerabilities in wireless systems and include an attack detection mechanism. In order to develop a detection method that is a useful contribution, research must be conducted on the basic structure, motivation and vulnerabilities in wireless ad hoc networks. The steps in carrying out both attacks, as well as their corresponding attack vectors, is essential in designing a model with a high success rate. The proposed detection method should account for a wide variety of network model scenarios, therefore, it should be implemented to carry out simulation testing. This ensures that the detection method is applicable to a wide variety of node positions that mimics real world networks. During simulation, the efficiency, accuracy and cost of the proposed method algorithm should be recorded and compared to other state-of-the art detection methods. In doing so, we are able to analyze the algorithm's performance to make adjustments as needed and make meaningful conclusions regarding our contribution.

3.3.3 Defining the Three-Way-Handshake Time

The three-way handshake time τ is the total time for the Leader to send the *Hello*, the Follower to send an acknowledgement, *H-Ack*, back to the Leader, and the Leader to send the *ACK* back to the Follower. Thus, τ can be modeled as:

$$\tau = T_{tran} + 3 \times T_{prop} + 2 \times T_{proc}. \tag{3.3}$$

Here, T_{tran} is the transmission delay, T_{prop} is the propagation delay, and T_{proc} is the packet processing time.

3.3.4 Simultaneously Discovering Multiple Neighbors

In order to account for scenarios in which more than two nodes are present in the network, we use an iterative approach to discover all the neighbors. After the initialization through LoRa, the node with the highest ID is assigned as the *Leader* and all the other nodes are *Followers*. The Leader begins the LOS discovery as the transmitter and the Followers act as receivers. Leader election algorithms in distributed environments is a very well studied topic and falls outside the scope of this paper [33, 34]. In our discovery mechanism, a Leader can be assigned in two ways. Firstly, by selecting the node which initiates the communication through LoRa, or, by selecting the node with the lowest ID number. Following the similar scanning and three-way handshake process as in the previous subsection, the Follower is able to find all of the neighbors in one scan. After the first scan, the algorithm appoints a new Leader from the Follower nodes. The Follower node with the lowest ID number is made the new Leader. The scanning algorithm will continue in this way

Algorithm 2: Discovering Multiple Neighbors

```
Divergence angle $\beta$
Number of transceivers $N_{tr}$
$leaderAngle \leftarrow 1$
$followerAngle \leftarrow \lfloor \frac{N_{tr}+1}{2} \rfloor$
$followers \leftarrow$ an array of all follower nodes
$neighborsfound = 0$
$visited \leftarrow emptyarray$
if $i > 0$ then
    APPEND $leader$ to $followers$
    $leader \leftarrow followers(0)$
    REMOVE $followers(0)$ from $followers$
end if
while $j < transNum$ do
    for $s$ in $followers$ do
        if $leader$ can communicate with $s$ then
            if !($s$ in $visited$) then
                $Leader$ sends ”Hello”
                if ”Hello” received then
                    reply with H-ACK and wait for ACK
                    if ACK is received then
                        APPEND $s$ to $visited$
                        neighborsfound++
                    end if
                end if
            end if
        end if
        if $neighborsfound \geq n - 1$ then
            TERMINATE
        end if
        leaderAngle++
        followerAngle++
    end for
end while
```

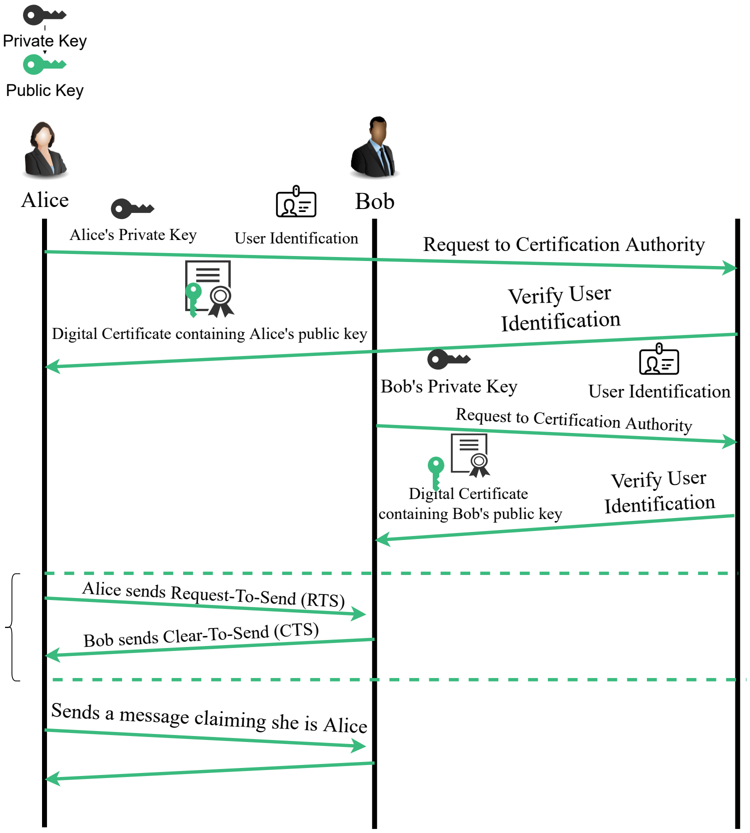

Private Key
Public Key
Alice
Bob
Alice's Private Key
User Identification
Request to Certification Authority
Verify User Identification
Digital Certificate containing Alice's public key
Bob's Private Key
User Identification
Request to Certification Authority
Digital Certificate containing Bob's public key
Verify User Identification
Alice sends Request-To-Send (RTS)
Bob sends Clear-To-Send (CTS)
Sends a message claiming she is Alice

Figure 3.3: Security Protocol

until all neighbors discover each other. The Multiple-Neighbor discovery method is presented in Algorithm 2.

3.4 Securing the System

In order to ensure secure communication between nodes, we have devised a secure communication protocol utilizing unique global identifiers and nonce-based encryption. This secure communication protocol is presented in figure 3.3. A node A will begin by providing its personal information and private key to the certificate authority. The node will ping a request for authentication. If the node is verified by the certificate authority, a digital certificate, containing a the certification authority identification and node A's public key, is granted. to node A. Node B, whom which Node A wishes to communicate with, repeats the same protocol with the certification authority and receives its digital certificate. Directly after both nodes obtain their CAs, the FSO alignment protocol can proceed. After the beams have aligned, Alice will attempt to send a message to Bob, claiming that she is Alice.

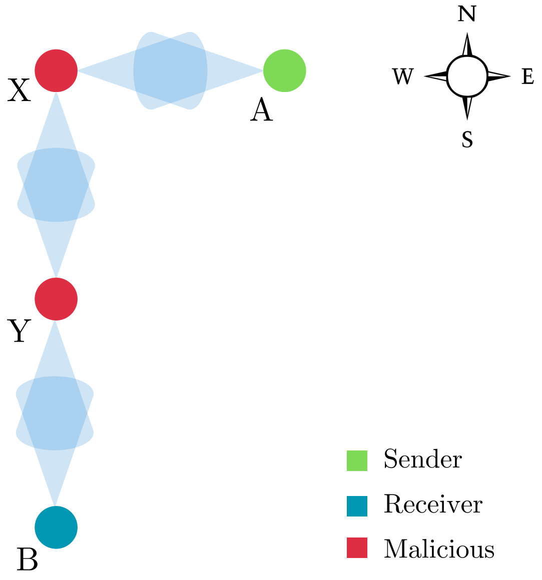


Figure 3.4: Wormhole is detected by the system.

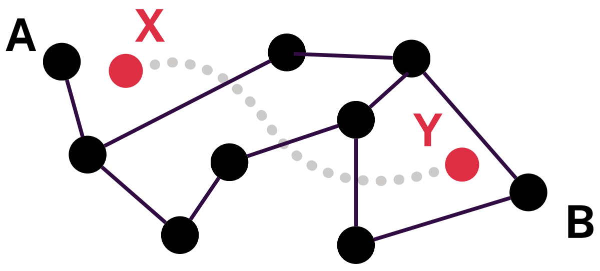


Figure 3.5: Wormhole is undetected by the system.

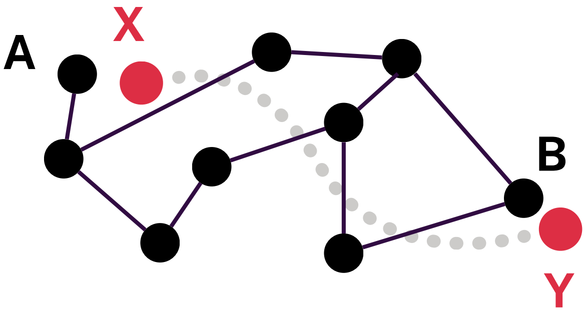


Figure 3.6: Wormhole is detected by the system.

3.4.1 Authenticity of Nodes

3.4.2 Authenticity and Cryptographical Defense

Authentication plays a pivotal role in wireless ad hoc networks. In such environments, the open and dynamic nature of the network exposes it to a range of security vulnerabilities, making authentication not just beneficial but essential. Without an authentication mechanism, ad hoc networks are susceptible to unauthorized access, data interception, and the introduction of malicious nodes. These threats can compromise the confidentiality, integrity, and availability of the network's data and services. Authentication ensures that only authorized and verified devices can participate in the network. This gatekeeping is crucial in maintaining the overall security of the network and protecting sensitive information from potential intruders.

Moreover, in wireless ad hoc networks, where nodes often depend on each other for the forwarding and routing of data, trust becomes a significant factor. Authentication helps build this trust by verifying the identity of each node, thereby preventing spoofing or man-in-the-middle attacks. Furthermore, authentication provides a framework for accountability and non-repudiation, essential aspects in scenarios where the origin and integrity of the data must be unquestionable. This is particularly important in applications involving critical data exchanges, such as military communications or emergency response systems.

The implementation of certificates, utilizing public key infrastructure (PKI), offers a robust solution to this problem. Each node in the network obtains a digital certificate from a trusted Certificate Authority (CA). This certificate contains the node's public key and identifying information, all signed by the CA. When a node wishes to communicate with another node, it presents its certificate as proof of identity. The receiving node verifies this certificate by checking the CA's signature, ensuring its validity and confirming the sender's identity. This process effectively thwarts impersonation attacks, as only those with a valid, CA-signed certificate are recognized as legitimate participants in the network. Moreover, the public keys in these certificates facilitate the establishment of secure, encrypted communication channels between nodes. This ensures that even if a malicious entity were to intercept the transmitted data, without the corresponding private keys, the information remains indecipherable.

3.4.3 Defense against relay and wormhole attacks

While certificates effectively address authentication in wireless ad hoc mobile networks, it is important to note that they do not prevent network layer attacks such as wormhole or relay attacks on their own. These types of attacks involve an adversary capturing packets from one part of the network and tunneling them to another location, either to disrupt the network or to create a false notion of direct connectivity. Wormhole attacks can be executed without compromising any cryptographic keys or breaking the authentication mechanisms produced by certificates. The certificates ensure that nodes are who they claim to be, but they do not validate the integrity of the route or the actual distance between nodes. Therefore, even in a network where certificates are used, attackers could still exploit the routing protocols. This underscores the necessity for additional security measures, complementing the authentication provided by certificates.

Figure 3.4 shows how a node's beam and relative position can be used to detect an attack. For example, in figure 3.5, node X and node Y are malicious and have established a tunnel between them. If node A wishes to communicate with node B, A sends its packets to node X. Node X will forward these packets through its tunnel to node Y who will replay them on the other side to node B. This wormhole attack goes undetected. However there are cases in which the position of the wormhole can allow us to detect an attack from occurring. In Figure 3.6, if we follow the same protocol, node B would be able to tell that a wormhole attack is occurring due to the fact that it expects the message from the West, but receives the message from the East instead. We expect the detection rate to be approximately

$$1 - \frac{2\beta}{360^\circ}$$

Evidently, this defense mechanism cannot detect all wormhole attacks and depends heavily on the topology of the network and wormhole placement.

Chapter 4

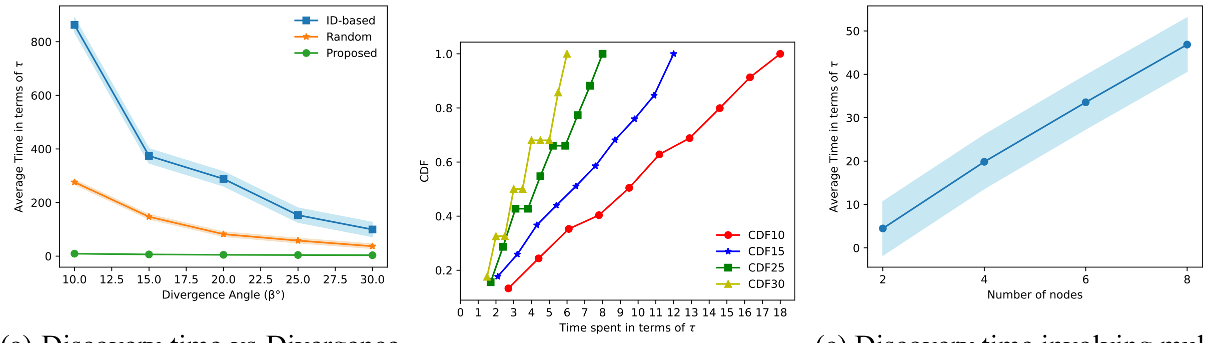
Evaluation

To test our model with certainty, a simulation of the protocol is run using python over thousands of different trials. The simulation is designed to consider a variety of different node locations, distances and beam widths in order to ensure the functionality of the protocol. The results of our proposed simulation are compared to the results of two oblivious state-of-the-art protocols as described below.

4.0.1 Benchmark protocols

We have simulated a random-based neighbor discovery algorithm which have used to compare our proposed algorithm [7]. The random based discovery tests a random pair of transceivers until a neighbor is found. This algorithm takes longer than our proposed algorithm and it also does not guarantee that a neighbor will be found. Because of its arbitrariness, it is necessary to run the simulation 1000 times for each divergence angle width in order to get at least one successfully discovered neighbor. Consequently, as the beam width becomes smaller, the algorithm tries more pairs of transceivers until a neighbor is discovered, resulting in a longer discovery time. This is modeled in Figure 4.1a. Unlike our proposed model, which guarantees a discovery slot time of at most the number of transceivers, a successful discovery is not guaranteed on every run.

Similarly, we compared our proposed algorithm to an ID-based neighbor discovery algorithm which is guaranteed to successfully discover a neighbor in at most the ID length in slots [6]. Each node has an ID of binary digits where 0 corresponds to receiving and 1 corresponds to transmitting.



(a) Discovery time vs Divergence angle

(b) CDF of neighbor discovery

(c) Discovery time involving multiple nodes

Figure 4.1: Simulation results

The nodes will follow the ID sequence until the length of the ID. Figure 4.1a reveals that, because this particular protocol assumes that the nodes are oblivious to one another, it takes considerably more time than the proposed algorithm and the random-based protocol.

4.0.2 Results for discovering a single neighbor

To test our proposed algorithm, 1000 runs of the algorithm were completed for a series of different beam widths[1]. These runs considered the scenario in which a node has only a single neighbor. As presented in Figure 4.1a, the average discovery time increases, as the beam width narrower. This is an expected result as our beam covers less area, we will need to add more transceivers and therefore check more positions. In addition to the average discovery times, Figure 4.1b displays the cumulative probability distribution for the series of beam widths has also been plotted. In both graphs it is evident that as the beam width increases the discovery time decreases. When compared to both of the oblivious benchmark protocols, our model with omni-assisted discovery is faster. For a divergence angle of 10^o, the proposed algorithm achieves 99.42% and 98.19% reduction in discovery time compared to the ID based [6] and random based protocol [7], respectively. For a divergence angle of 30^o, the reduction is 98.38% and 95.68% for ID based and random based, respectively.

4.0.3 Simulation for discovering multiple neighbors

The proposed simulataneous multiple neighbor discovery algorithm (descrived in Section 3.3.4) is simulated to account for scenarios which involve more than one neighbor. Multi-neighbor discovery is conducted using an iterative ID-based approach. Completion of multi-neighbor discovery is defined as the time it takes for all nodes in the system to discover its neighboring nodes. In this variation, each node has a unique ID number. Multiple-neighbor discovery dictates that each node in the system is able to communicate with each one of its neighbors. Only the Leader is in transmission mode in each scan in order to avoid the problem of packet collision. If there is more than two nodes, the leader is able to find all of the nodes, which are followers, in one scan. Once a Follower has established communication with the leader, the follower ceases to scan in receiving mode. After the first scan, the algorithm appoints a new Leader among the Follower nodes. The follower node with the lowest ID number is made the new Leader. The scanning algorithm continues to search for the remaining nodes in this way until all neighbors are discovered by the current leader. Figure 4.1c portrays the average time taken for this to occur in for a varying number of total nodes. Using this approach, we can conclude that the time it takes to discover increases with a higher number of neighbors.

4.0.4 Simulation for Detecting Attacks

Figure 4.2 represents the relationship between beam width in degrees and attack detection rate. As the beam width decreases from 30 degrees to 10 degrees, the attack detection rate increases.

[1] The code is available at `https://github.com/wsl-miami/nd-simulation`

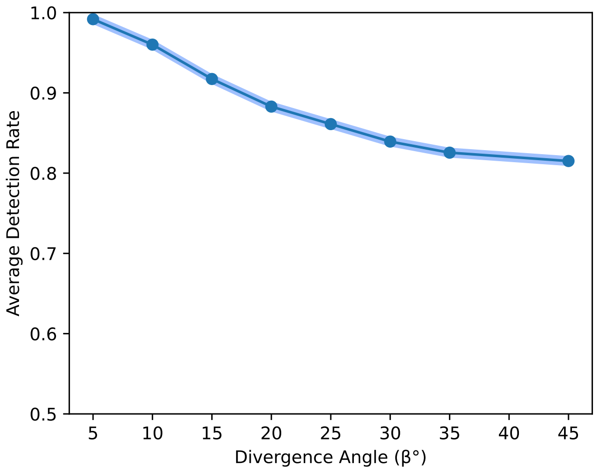


Figure 4.2: Proportion of attacks detected over 1000 runs

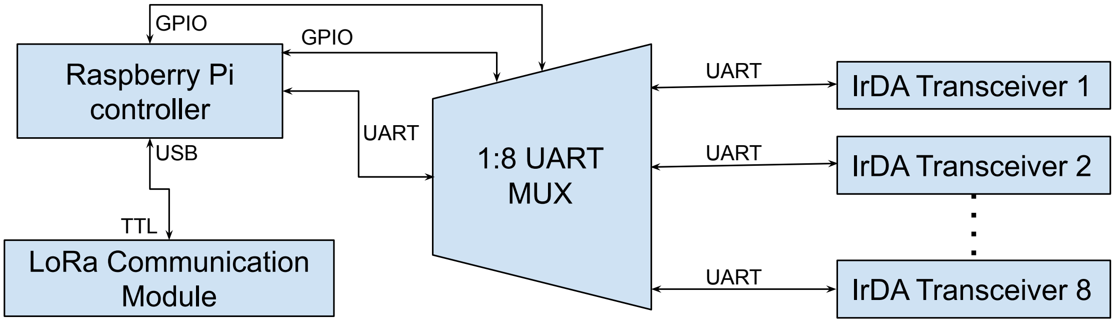
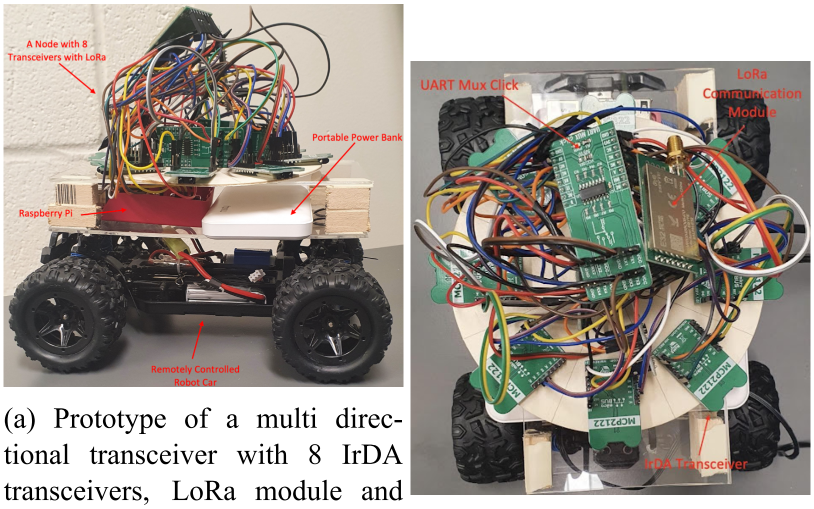


Figure 4.3: Schematic of the prototype

Specifically, at a 10-degree beam width, the attack detection rate is the highest at 0.966, indicating a high level of accuracy in detecting attacks. When the beam width is expanded to 15 degrees, the detection rate remains relatively high at 0.93. However, further widening the beam to 30 degrees results in a decrease in the attack detection rate to 0.823, suggesting a lower level of accuracy in detecting attacks with a broader beam width. This trend highlights the importance of selecting an appropriate beam width to achieve an optimal balance between detection precision and coverage.

4.1 Experiments with prototype

After all the rigorous simulation, in this section, we describe a prototype using off-the-shelf devices. First, we describe the prototype implementation and then present the experiment results.


A Node with 8 Transceivers with LoRa
Portable Power Bank
Raspberry Pi
Remotely Controlled Robot Car
UART Mux Click
LoRa Communication Module
MCP2122
IrDA Transceiver

(a) Prototype of a multi directional transceiver with 8 IrDA transceivers, LoRa module and Raspberry Pi as the controller

(b) Top view of the prototype

4.1.1 Prototype

Figure 4.4b and Figure 4.4a depicts the top and the side view of the state-of-the-art prototype built using off-the-shelf components. The schematic of the prototype's components are modeled in figure 4.3. We programmed the discovery protocol in python[2].

The system prototype consists of eight infrared transceivers, three UART [35] (universal asynchronous receiver-transmitter) multiplexers, a LoRa [8] communication module, and one Raspberry Pi as the controller. The IrDA [9] transceiver is an infrared transceiver which has one piece of integrated circuit for UART-IrDA conversion. Eight IrDA transceivers are connected to the MUX through UART. Two dual 4-Channel UART MUXs/DEMUXs are used as follower MUXs for switching data for a total of eight IrDA transceivers, and a leader Mux is wired to Raspberry Pi through UART for switching data for the two follower MUXs according to communication needs. By this method, the data path is completely controlled through four GPIO ports(two ports are used for the leader MUX, the other two ports are shared by two follower MUXs) of Raspberry Pi. Above is the wiring method used to control the IrDA transceiver to complete the communication. The LoRa communication module can communicate directly with the USB port of raspberry Pi. The LoRa communication module connects to the serial USB port of Raspberry Pi by using a USB to TTL converter.

4.1.2 Experiment results

This section discusses the result of over 110 experiments conducted using the system prototype. The results are plotted in Figure 4.5. Note that we are using UART-based serial communication for sending packets through IrDAs. To tackle several delays associated with the MUX, IrDA, etc., we force the nodes to wait for 160 ms before switching to the next IRDA. This makes the τ higher. The average time for discovery over these experiments is approximately 2.985 seconds. In

[2] The code is available at `https://github.com/wsl-miami/nd-system`

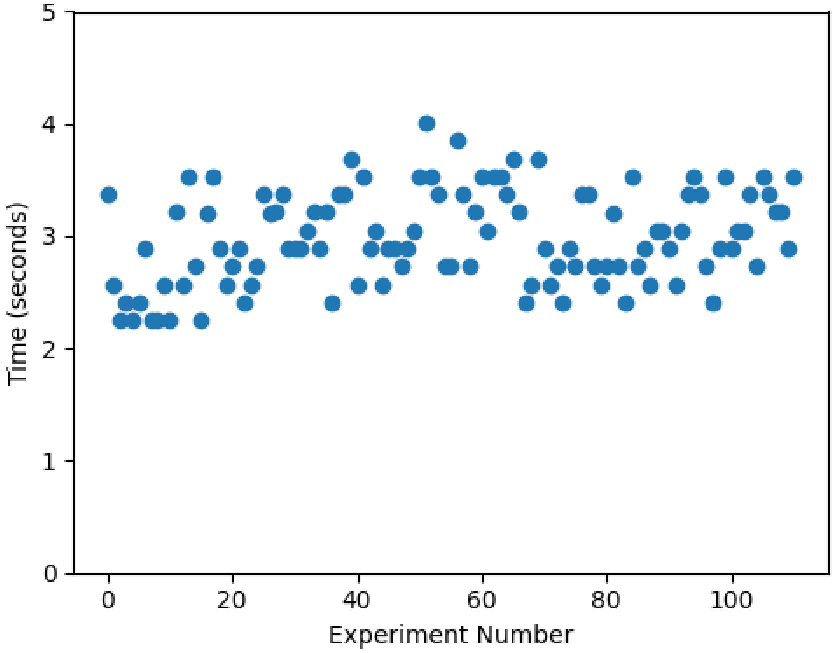


Figure 4.5: Neighbor discovery time for each experiment

the future, we aim to reduce this latency by optimizing the UART communication and finding a suitable waiting time.

Chapter 5

Conclusion

Neighbor discovery is a widely studied topic in wireless mesh networks. Neighbor discovery becomes more challenging in directional communications as the nodes need to discover the line-of-sight with their neighbor. Both nodes need to steer their communication beam towards the neighbor for effective communication. Oblivious neighbor discovery, i.e., where nodes do not possess apriori knowledge of neighbor's location, is a well-studied topic for directional communication. In this thesis, we present a novel design for neighbor discovery with the help of a long-range low-bit rate omnidirectional helper communication channel. We are able to incorporate an attack detection method using relative placement of nodes. Additionally, through rigorous simulation and a proof of concept prototype using off-the-shelf equipment we are able to present efficient and secure neighbor discovery process.

References

[1] Ju-Hyung Lee, Ki-Hong Park, Young-Chai Ko, and Mohamed-Slim Alouini. A UAV-mounted free space optical communication: Trajectory optimization for flight time. *IEEE Transactions on Wireless Communications*, 19(3):1610–1621, 2019.

[2] Saim Ghafoor, Noureddine Boujnah, Mubashir Husain Rehmani, and Alan Davy. MAC protocols for terahertz communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 22(4):2236–2282, 2020.

[3] Yu-Ngok Ruyue Li, Bo Gao, Xiaodan Zhang, and Kaibin Huang. Beam management in millimeter-wave communications for 5G and beyond. *IEEE Access*, 8:13282–13293, 2020.

[4] reconfigurable beam system for non-line-of-sight free-space optical communication.

[5] Xin-Wei Yao and Josep Miquel Jornet. TAB-MAC: Assisted beamforming MAC protocol for Terahertz communication networks. *Nano Communication Networks*, 9:36–42, 2016.

[6] Mahmudur Khan and Jacob Chakareski. Neighbor Discovery in a Free-Space-Optical UAV Network. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2019.

[7] Sudarshan Vasudevan, Jim Kurose, and Don Towsley. On neighbor discovery in wireless networks with directional antennas. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, volume 4, pages 2502–2512. IEEE, 2005.

[8] LoRa E32-TTL-100 433T20DC SX1278 433 MHz 433MHz UART Long Range 1000w Wireless RF Module. `https://img.filipeflop.com/files/download/E32_User+Manual_EN_v1.00.pdf`.

[9] IRDA 3 CLICK. `https://www.mikroe.com/irda-3-click`.

[10] Marcelo Rubinstein, Igor Moraes, Miguel Campista, Luís Costa, and Otto Carlos M. B. Duarte. *A Survey on Wireless Ad Hoc Networks*, volume 211, pages 1–33. 11 2006.

[11] Peng Yan, J.J. Sluss, H.H. Refai, and P.G. LoPresti. An initial study of mobile ad hoc networks with free space optical capabilities. In *24th Digital Avionics Systems Conference*, volume 1, pages 1.D.3–11, 2005.

[12] David Talbot. How Technology Failed in Iraq. *Technology Review*, 2004.

[13] Abdulsalam Ghalib Alkholidi and Khaleel Saeed Altowij. Free space optical communications — theory and practices. In Mutamed Khatib, editor, *Contemporary Issues in Wireless Communications*, chapter 5. IntechOpen, Rijeka, 2014.

[14] In Matthew Neely, Alex Hamerstone, and Chris Sanyk, editors, *Wireless Reconnaissance in Penetration Testing*, pages 153–159. Syngress, Boston, 2013.

[15] Zhenshang Zhang. Performance of neighbor discovery algorithms in mobile ad hoc self-configuring networks with directional antennas. In *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pages 3162–3168 Vol. 5, 2005.

[16] Lin Chen, Yong Li, and Athanasios V Vasilakos. On oblivious neighbor discovery in distributed wireless networks with directional antennas: Theoretical foundation and algorithm design. *IEEE/ACM Transactions on Networking*, 25(4):1982–1993, 2017.

[17] Yu Wang, Shiwen Mao, and Theodore S Rappaport. On directional neighbor discovery in mmwave networks. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*, pages 1704–1713. IEEE, 2017.

[18] Zhiqing Wei, Xinyi Liu, Chenyang Han, and Zhiyong Feng. Neighbor discovery for unmanned aerial vehicle networks. *IEEE Access*, 6:68288–68301, 2018.

[19] Zhensheng Zhang and Bo Li. Neighbor discovery in mobile ad hoc self-configuring networks with directional antennas: algorithms and comparisons. *IEEE Transactions on Wireless Communications*, 7(5):1540–1549, 2008.

[20] Mahmudur Khan, Suman Bhunia, Murat Yuksel, and Lawrence C Kane. Line-of-sight discovery in 3D using highly directional transceivers. *IEEE Transactions on Mobile Computing*, 18(12):2885–2898, 2018.

[21] Michael Atakora and Harsha Chenji. Fast Neighbor Discovery in MEMS FSO Networks. In *2020 International Conference on Computing, Networking and Communications (ICNC)*, pages 1031–1037, 2020.

[22] Mohammad Sheikh Zefreh and Pejman Khadivi. Secure directional routing to prevent relay attack. In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, pages 1–6, 2008.

[23] Cynthia Kuo, Mark Luk, Rohit Negi, and Adrian Perrig. Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes. In *SenSys '07*, 2007.

[24] Gyul Kim, Kwanhyung Lee, Shim-Soo Kim, and Ju Min Kim. Vehicle relay attack avoidance methods using rf signal strength. *Communications and Network*, 5:573–577, 2013.

[25] Geeth Jayendra, Sisil Kumarawadu, and Lasantha Meegahapola. Rfid-based anti-theft auto security system with an immobilizer. In *2007 International Conference on Industrial and Information Systems*, pages 441–446, 2007.

[26] Roel Verdult, Flavio D Garcia, and Baris Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *USENIX Security Symposium*, pages 703–718, 2013.

[27] Abel Valko. *Relay Attack Resistant Passive Keyless Entry: Securing PKE Systems with Immobility Detection*. PhD thesis, 08 2020.

[28] Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. On the security of carrier phase-based ranging. *CoRR*, abs/1610.06077, 2016.

[29] Frank Stajano, Ford-Long Wong, and Bruce Christianson. Multichannel protocols to prevent relay attacks. In Radu Sion, editor, *Financial Cryptography and Data Security*, pages 4–19, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[30] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Wormhole detection in wireless ad hoc networks. *Department of Computer Science, Rice University, Tech. Rep. TR01-384*, 2002.

[31] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks. In *2006 Securecomm and Workshops*, pages 1–12, 2006.

[32] Lingxuan Hu and David Evans. Using directional antennas to prevent wormhole attacks. In *NDSS*, volume 4, pages 241–245, 2004.

[33] Koji Nakano and Stephan Olariu. A survey on leader election protocols for radio networks. In *IEEE I-SPAN*, 2002.

[34] J Villadangos, Alberto Cordoba, Federico Fariña, and Manuel Prieto. Efficient leader election in complete networks. In *IEEE PDP*, 2005.

[35] UART MUX CLICK. `https://www.mikroe.com/uart-mux-click`.