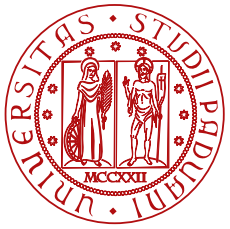

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Master Thesis in ICT for Internet and Multimedia

Network Node Authentication by Wireless Signal Overhearing

Master Candidate

Yusuf Taylan Yuksel

Student ID 2005536

Supervisor

Prof. Stefano Tomasin

University of Padova

Academic Year
2021/2022

To my parents
and wife

Abstract

Ad hoc networks are infrastructure-less networks that are not based on a center. The absence of centralized control raises some doubts about having a secure data transfer. We assume a wireless network where the nodes are connected with a given probability α and data packet transmission over the next hop nodes starting from a Source Node (SN) to a Destination Node (DN). Some packets can be modified, corrupted, or forwarded by a node outside of the route in a data packet transfer. To detect this, we propose an authentication solution for the transmitting nodes each time they transmit a data packet to the next hop node. Since the data transmission signal can be heard by some nodes in a transmission range, any nearby node can also receive the same packet. Thus, it can verify whether the transmitted packet came from a real transmitting node. The solution aims to detect misbehaving nodes and cut them off from future packet transfers on the expected packet route. Additionally, it sends an alarm packet to the DN to warn that the incoming data packet was transmitted by an *illegal* node.

Contents

List of Figures

List of Tables

List of Acronyms

WN ..... Wireless Network

SN ..... Source Node

DN ..... Destination Node

TP ..... Timestamp

WDN ..... Watch Dog Node

AN ..... Attacker Node

VN ..... Victim Node

AR ..... Alternative Route

OSI ..... Open Systems Interconnection

IEEE ..... Institute of Electrical and Electronics Engineers

TCP ..... Transmission Control Protocol

Wi-Fi ..... Wireless Fidelity

WLAN ..... Wireless Local Area Network

MU-MIMO ... Multi-User, Multiple-Input, Multiple-Output

OFDMA ..... Orthogonal Frequency Division Multiple Access

MAC ..... Medium Access Control

MANET ..... Mobile Ad hoc Network

VANET ..... Vehicle Ad hoc Network

WSN ..... Wireless Sensor Network

WMN ..... Wireless Mesh Network

P2P ..... Peer-To-Peer

CSMA ..... Carrier Sense Multiple Access

CSMA/CA .... Carrier Sense Multiple Access Collision-Avoidance

CSMA/CD .... Carrier Sense Multiple Access Collision-Detection

R-MAC ..... Reservation based Medium Access Control

FDMA ..... Frequency-Division Multiple Access

TDMA ..... Time-Division Multiple Access

CDMA ..... Code-Division Multiple Access

RREQ ..... Route Request

RREP ..... Route Response

2ACK ..... Two-hop Acknowledgment

PKI ..... Public Key Infrastructure

CA ..... Certification Authority

List of Notations

$\mathbf{m}$	Node
m_i	A node in the set
$\mathbf{N}$	Total number of nodes in the wireless network
C_m	Neighboring nodes for m
$\mathcal{R}$	Route
ρ	Set of nodes in the route $\mathcal{R}$
$\mathcal{R}^c$	set of ρin the route $\mathcal{R}$
$\mathcal{W}_{\Updownarrow}$	Set of WDNs for node m
$\mathbb{P}$	Probability
$\lvert W_m \rvert$	Count of WDN for node m
ω	Count of m authenticated by a WDN in the route $\mathcal{R}$
β	Probability of a node has at least one WDN
υ	Probability that each node in route $\mathcal{R}$ has at least one WDN
$\delta(\mathcal{E})$	AR existence from WDN to DN
ϕ	Probability of AR in
ψ	Probability that each node in route $\mathcal{R}$ has at least one WDN
α	Probability of a communication link exist between two nodes
$\lvert R \rvert$	Route length

1

Introduction

Communication between nodes in wireless networks can be achieved in many ways. Sometimes malicious nodes get access to wireless networks and this is a threat to their security. Ad hoc networks are infrastructure-less networks that are not based on a central node get their working. Nodes in ad hoc networks route data packets to provide network-wide connectivity as some nodes may not be in the signal range required to transmit a data packet directly to the desired node. This however raises some doubts on the security of data transmission, due to the lack of central control and the nodes sometimes may misbehave. The nature of the transmission medium and mobility adds more complexity to developing solutions to prevent these attacks in wireless networks. For ad hoc networks, attacks can come from anywhere in the network and from any node. Taking control of a node can result in many manipulative actions on the network.

Considering these facts, here we consider a wireless network where nodes are connected with a given probability and a next-hop data packet transmission starting from a Source Node (SN) to a Destination Node (DN) in Chapter 3. Some packets can be modified, corrupted, or forwarded by a node outside the intended route. To detect this, we propose an authentication solution for transmitting nodes in Section 3.3. Since the data transmission signal can be heard by some nodes in a transmission range, any nearby node can also receive the same packet. Thus, it can verify whether the transmitted packet came from a real transmitting node. The solution aims to detect misbehaving nodes and cut them off from future packet transfers on the used route. Additionally, it

sends an alarm packet to the DN through an alternative route (AR) to warn that the incoming data packet was transmitted by an *illegal* node. We created a simulation setup that demonstrates the presence of misbehaving nodes in the route and using the Python3 *networkx* library in Chapter 4. In Chapter 5, we created plots from the data and analyzed these charts. Finally, Chapter 6 concludes the thesis and discusses the directions for future works.

2

Wireless Network And Authentication Methods

In this Chapter, we first describe the Wireless Network and its types, the data transfer methods, and the authentication methods used. Then we revise the literature about spoofing attacks and main defense techniques.

2.1 Wireless Network

Wireless communication refers to the transfer of data, voice, or video from one point to another, without using a physical connection such as a copper cable. Multiple devices (adapters, computers, phones...) connected to each other form a wireless devices network. These devices may be two computers standing next to each other, or they may be thousands of computers spread all over the world. A key characteristic of these networks is *mobility*, which leads to dynamic topology as node positions change over time [11].

Wireless network systems work with radio frequencies. Data transmission takes place by converting data from binary zero and one form to radio waves. The newly converted data is then broadcast and captured by wireless antennas and suitable receiving devices, which then convert the radio signals to zeros and ones for the computer to understand. Wireless networks use 2.4 GHz or 5 GHz radio frequencies. Higher frequency allows more data be transmitted while reducing the range.

Communication of devices using radio waves can be three types. These are called receiver, transmitter, and trans-receiver. To briefly mention them;

- **Receivers**: As the name suggests, they are devices that can only receive radio signals but do not have the ability to send them. E.g., FM radios and televisions.
- **Transmitters**: Devices that can only send radio signals but cannot receive them. E.g., radio transmitting stations, television transmitting stations, etc.
- **Transceivers**: These are devices that have both transmit and receive capabilities. E.g., radio relays, mobile phone base stations, mobile phones, etc.

Another point that needs to be known in terms of communication is the direction of transmission. The transmission directions are divided into three categories:

1. **One-Way Transmission (Simplex)**:
   It is the name of the established transmission system when the transmission can only be made in one direction. FM radios are an example.
2. **Bidirectional Asynchronous Communication (Half-Duplex)**:
   These are the systems in which two-way transmissions can be made, but only one party can send a signal of any given time. Radio applications can be shown as an example. Wireless communication systems working with radio frequencies used in information systems are generally of this type. For example, the IEEE 802.11g standard offers Half-Duplex transmission at 54 Mbps.
3. **Duplex Simultaneous Communication (Full-Duplex)**:
   It is the name given when two devices can transmit (and receive) simultaneously. Examples include mobile phones and cordless phones. A seamless network of ports is created over the city. In this way, in the train, in the car, in the park, cafes, restaurants, etc. It is possible to freely connect to the Internet in many places. An uninterrupted and continuous connection is ensured with the connection points placed at certain intervals in the cities.

2.2 Communication in Wireless Networks

In order to understand the communications in wireless networks, we first need to look into the network layers and the communication between them. In this manner, we need to review Open Systems Interconnection (OSI), which defines how communication between two devices will be.

In a nutshell, the purpose of OSI is to enable network architectures and protocols to be used as a component of a network product. The OSI model is divided into 7 layers. Each layer is responsible to provide services to the upper layers. Considering a communication between two computers, the layers of their network communicate in order; peer layers do not actually communicate directly, but a virtual communication occurs between them. Note that the OSI is a guide to comprehending the actual networking protocols used by embedded devices. Therefore, it doesn't mean that OSI should be applied within the same 7 levels. These layers can be implemented by one as well as many together in multiple protocols. Fig. 2.1 shows the data flow of OSI model[17].

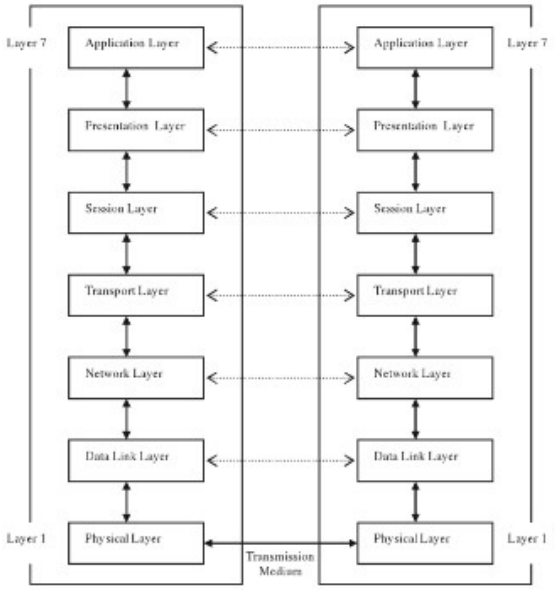

Figure 2.1: OSI Layers.

The mode of data transmission through the lower layers in OSI works as follows: The transport layer divides the data received as information into segments. When the data is reassembled on the receiving system in this manner, the right sequence is guaranteed. Data arriving to the network layer in the form of segments is supplemented with address information, turning the slices into packages. The unique address of the network devices which are 12 digits and identifies the network devices are added to packets at the data link layer where the structure known as frames is created. The receiving frames of the physical layer are finally converted to a bit stream and prepared for transmission.

There are many ways to communicate with other communication endpoints across the network at different layers of the OSI e.g., IEEE 802.11, Bluetooth on psychical layer, Transmission Control Protocol (TCP) in transport level. A protocol should be established in order to determine the communication way, as it is important to choose the same way to talk to each other.

IEEE 802.11 is an international standard protocol for wireless networks for devices to interact with each other, and Wi-Fi (Wireless Fidelity) is one of the most popular wireless communication protocol families for wireless local area networks (WLAN) based on this standard. There are several versions of 802.11 standard developed to improve the capabilities and the speed. 802.11b was the first well-adopted protocol for houses and businesses which work with 2.4GHz frequency range within up to 11Mbs of speed. The most recent one of this protocol 802.11ax as known as Wi-fi 6 gives a better efficiency in order all the devices to communicate such as mobile phones and IoTs. It has multiple user Multi-user, multiple-input, multiple-output (MU-MIMO) capabilities and orthogonal frequency division multiple access (OFDMA), which enables many devices to connect at once [9]. Zigbee, bluetooth etc. can be given as examples of other communication protocols.

Infrastructure-based wireless networks have base stations deployed in a specific area where each device communicates via an access point (wireless router). Conversely, there are infrastructure-less networks where a node can access the communication channel to forward the message to its neighbors to find the route to the destination without a base station to route the message, such methods called as Multi-hub routing and such networks are called ad hoc networks. The methods to coordinate among nodes to access the channel care called Medium Access Control Protocols (MAC). In the following section we will describe ad hoc networks and its protocol layers.

2.3 Ad Hoc Networks

Ad hoc is a Latin expression meaning "for this", i.e. specific. Ad hoc networks are the wireless networks that devices can create in a short time with minimum configuration without a fixed cable infrastructure. An ad hoc network becomes a LAN when it is permanently installed. An ad hoc network may host multiple users at once but this can reduce the performance. However, ad hoc networks

do not have installation or maintenance costs as they are infrastructure-less networks, so they are cost-friendly. They are easy to deploy and reconfigure. These features make the ad hoc networks more interesting to be preferred. Due to their decentralized nature, node redundancy, and lack of single points of failure, they also show excellent robustness which is especially important for military applications. Ad hoc networks are classified according to their use as mobile ad hoc networks (MANET), vehicle ad hoc networks (VANET), wireless sensor networks (WSN), and wireless mesh networks (WMN) [8].

Fig. 2.2 shows an example of ad hoc network where the nodes are connected within a signal range.

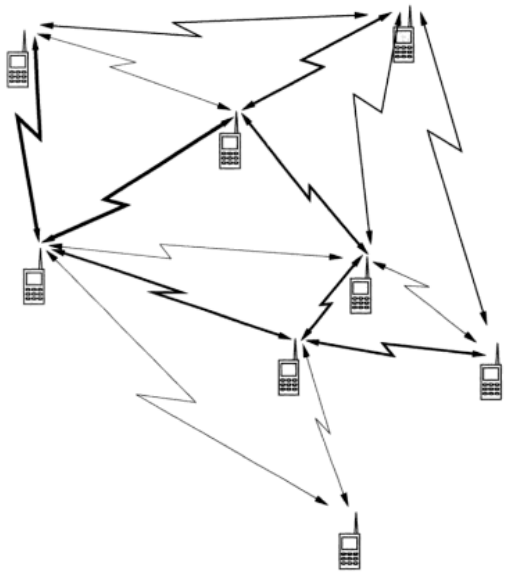

Figure 2.2: Ad hoc network.

2.3.1 Protocol Stack and Challenges

One of the biggest challenge and at the same time the benefit of the ad hoc networks are its infrastructureless characteristic. Ad hoc networks work as peer-to-peer (P2P) communication. The control functions of the network are distributed among all nodes, and routing can use intermediate nodes as relays [2].

Every node within the transmitter's transmission range can receive the signal, therefore, the communication channel in wireless networks is a broadcast medium. Occasionally, a node will transmit a message to a certain recipient while another node tries to send a packet to the same device. These two transmitters may attempt to pass packets to the same receiver, resulting in a collision, if they are out of each other's broadcast range and are unaware of the other node's existence. The receiver is unable to decode the signals it receives due to what is known as the buried terminal problem. This is called as *hidden terminal problem*.

There has been discussions about different access techniques for wireless systems in order to avoid from such terminal problems. Following Fig. 2.3 shows the types of multiple access protocols subdivided according different process.

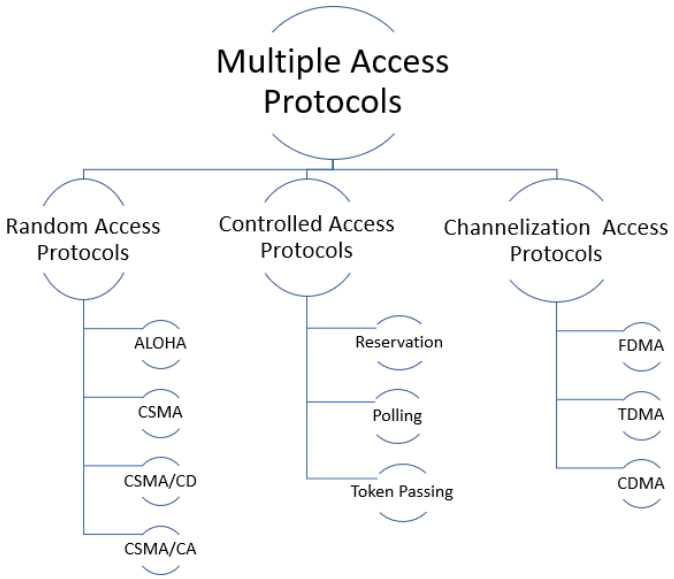

Figure 2.3: Multiple access protocols subdivided.

In the random access protocol, stations provide idle random access as the name suggests. Any station can send data at any time while the state of the medium is idle. It has two main features for sending data:

- No fixed time
- No fixed sequence

Due to their random access strategies, simplicity, and relative effectiveness in giving channel access in a distributed manner, some MAC protocols have received more attention than others. These are the Carrier Sense Multiple Access (CSMA) and variants of the Aloha protocols.

Aloha

Aloha is a protocol proposed by Abramson [1] for multihop wireless networks in 1968 in order to investigate the usage of radio communications for computer-computer and console-computer links.

Aloha gives freedom to any station to transmit data across a network simultaneously whenever it has a frame to be transmitted. This method works well with bidirectional asynchronous communication links. However, when the network becomes more complex, for example, when multiple sources and destinations use the same path due to the conflict of data sets, the protocol does not work efficiently. It gets worse the more the network traffic increases. In order to prevent that, different variants of Aloha have been developed such as Slotted Aloha.

CSMA

Carrier-sensing multiple access (CSMA) is a MAC protocol developed against collisions. The protocol verifies before a transmission that there is no other traffic occurring through the shared transmission medium. It requires each stations to first check the medium before a transmission is started [16].

CSMA has two basic variants; collision-avoidance (CSMA/CA) protocol, which basically decreases the chances of collisions for carrier transmissions in 802.11 networks and collision-detection (CSMA/CD), which detects the collisions [3].

Fig. 2.4 shows the differences between these two variants.

S.NO	CSMA/CD	CSMA/CA
1.	It's used in Wired Networks.	It's used in wireless LANs and other types of wireless networks.
2.	It is more effective after a collision has occurred.	It is more effective before a collision has occurred.
3.	It will not take measures to prevent transmission collision until it has occurred.	It will try to endeavour to avoid any collision as there is no way of knowing if any collisions have occurred.
4.	It is standardized in IEEE 802.3	It is standardized in IEEE 802.11.

Figure 2.4: CSMA/CD vs CSMA/CA

There are several modes of the CSMA access modes.

1. **1-Persistent**: Used in CSMA/CD methods, like Ethernet. The working logic of this method is to wait for the medium to be idle first and then transmit the data. The transmitter must keep track the status of the medium [21].

2. **Non-Persistent**: It is the method in which the transmitter first checks whether the medium is idle or busy when it wants to transmit data. If the medium is busy, it waits for a random time and checks the medium again. It does not persist in checking the medium's state. This flow continues until it finds the media in an idle state. The advantage of this method of comparing 1-persistent is that the transmitter waits a period of time before trying to transmit the data again. Thus, waiting time in multi-station networks is significantly reduced [12].

3. **P-Persistent**: Used in CSMA/CA methods, like Wi-Fi. Unlike the 1-Persistent method, this method transmits data with probability p after it finds the medium state is idle. If data could not be sent (1-p), the transmitter waits for the medium to be idle again and transmits p with another possibility[21].

4. **O-Persistent**: In this method, each node is assigned a transmission queue and the data enters a queue to move through it. When the medium is idle, the next node in the queue can transmit data. It is mainly used in controller area networks [12].

In the controlled access protocol, each station has to talk to each other in order to learn the order of access to the medium. Stations must be authorized before transmitting data, which means they must have given permission. We will see three different methods developed based on this protocol.

Reservation

In the reservation-based MAC method (R-MAC) [22], stations need to make a reservation before sending any data. Time is divided in slots. These slots are two types of periods:

- Fixed time reservation intervals
- Data transmission time of variable duration

Let us have K stations connected in a network. The reservation interval assigns each station a slot, i.e. we get K slots. If a station, for example Station 1, wishes to transmit a frame, it transmits 1 bit during this slot and all other stations wait during this slot. That is, if K_i announces its reservation by putting 1 bit in

its i^{th} slot, then all the stations know the order of the transmission accordingly. Thus, everyone agrees on sequence and no collusion occurs.

Polling

Compared to the reservation method, polling works by selecting one device as the primary station and the others as the secondary. Therefore, it ensures that all exchanges go through the primary station. This primary station plays the role of controller. This controller asks the secondary stations if there is data to send. This process is simply called polling [18]. The controller is the initiator of the sessions, allowing other stations to access it one at a time. Because the controller acts as a bridge between stations, it also shares the original sender's address when sending data.

Token Passing

The symbol pass protocol is based on a token, which is a control signal. A token is a 24-bit packet that regularly circulates throughout the network as shown in Fig. 2.5. The logic of the protocol is based on the rule that only one station can talk at the same time. Therefore, every station that wants to transmit a message must first capture the token [7].

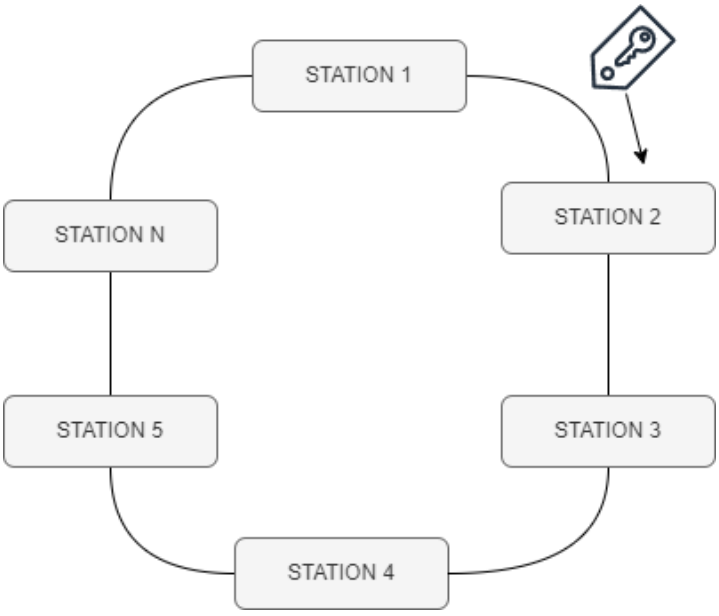

Figure 2.5: Token passes through the network by stations.

Some disadvantages of this protocol are the handling of tokens such as cases where the token is not available or duplicated or a station is lost and monitoring of the network. The protocol works to generate a new token in the cases related to token but the solution becomes very costly.

Channelization is another type of MAC protocol developed in order to access channel simultaneously. The available bandwidth of the link is shared in time across multiple stations. There are various methods developed based on this technique in order to access the channel and they can be broadly classified based on time, frequency, and codes.

Frequency-division multiple access (FDMA): This technology uses high-performance filters to divide the bandwidth into frequency bands. Thus, more than one user can send data to these divided subchannels at different frequencies. Each transmitting station allocates and keeps a band to prevent cross-talk. For example, this technology is used in cable TV systems where coaxial cable is the medium that broadcasts thousands of channels. It is also used in fiber optic communication systems.

Time-division multiple access (TDMA): This technology allows the usage of the same frequency bandwidth across multiple stations by dividing the band into time slots. This technology works efficiently especially slow voice data signals.

Code-division multiple access (CDMA): CDMA gives users unique codes instead of sharing time and frequency resources. Since these resources were not divided, it was possible to reach higher data rates. In this respect, CDMA forms the basis of 3G technology W-CDMA. So, It allows the transmission over the entire frequency range without limiting the user's frequency range while optimizing the use of available bandwidth. Thus, several transmitters can communicate simultaneously over a single channel.

The comparison of these three techniques can be explained with a simple example as follows. Suppose that many people in a room communicate by speaking. In the FDMA method, people speak with different tones and therefore the receiver receives the message by paying attention to the relevant tone, so the people talking to each other share a frequency. In the TDMA method, people speak in turn and one at a time, and the corresponding receiver receives the message of the person speaking, so that people talking to each other share a time. In the CDMA method, people speak in different languages, so it is perceived by people who know that language, and data transmitted by other

people is perceived as noise and is not considered, so people talking to each other share a code.

Fig. 2.6 illustrates the time-frequency assignment in FDMA, TDMA and CDMA.

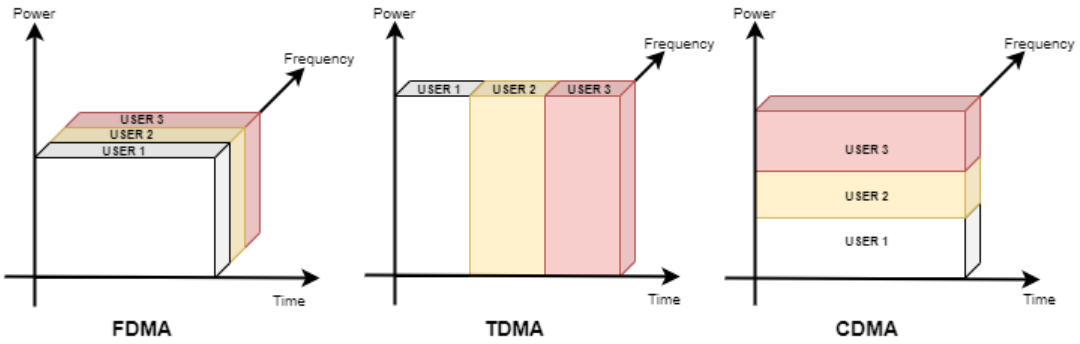

Figure 2.6: Comparison of FDMA, TDMA and CDMA.

2.3.2 Routing Protocols

Considering the dynamic characteristics of wireless networks, some routing methods are proposed to send a data packet to a node over a multi-hop connection using the MAC protocols described in the previous section. Routing protocols for ad hoc networks are broadly classified into nine different categories according to their underlying architectural framework as follows [4]:

1. Reactive (On-demand)
2. Proactive (Table-driven)
3. Hybrid
4. Multipath
5. Multicast
6. Location-aware (Geographical)
7. Geographical Multicast
8. Hierarchical
9. Power-aware

In this section, we will describe some of the important algorithms regarding our solution and based on the given routing protocols.

Dynamic source routing (DSR)

It is one of the most known On-demand routing algorithm designed simply with two phases, *route discovery* and *route maintenance*.

In the source discovery phase, the goal is to find the shortest route when a node wants to send a message. The node first broadcasts an *route request* to its neighbors within a signal range. Receiver nodes add the transmitter node ID to the request and rebroadcast. This signal can either reach the destination node where the sending node wants to send the packet, or it can reach neighbors that have a *route catch* with the shortest paths to the destination node. When the cached shortest path is found, neighboring nodes stop forwarding the packet to other nodes and send a reply message to the source node. This response message contains all the route information from the source node to the destination node, and the source node catches this route information for further message transmissions.

The other phase in this routing algorithm is route maintenance, which includes the *route error* and *acknowledgements* packets. When a message is sent, DSR waits for an acknowledgement from neighboring nodes to validate the existence of the route. The packet also contains a *passive acknowledgement* because overhearing nodes forward the packet across the nodes to the target node. If a node cannot receive this packet due to a transmission error, an error message is generated. This packet is sent to the source node and it returns to the previous phase where a new route is discovered. Nodes also exclude entry of broken link from their route catches [10].

Ad hoc on-demand distance vector (AODV)

It is a routing protocol that enables self-starting, multi-hop routing between the nodes in the MANETs or in other wireless networks. An important feature of this algorithm is that finds the routes to the new nodes quickly and does not require to communicate between the source node and the destination node before it initiates a transmission. Instead, it initiates a *route discovery* to locate the nodes. The source node broadcasts a control packet named route request (RREQ) to its neighbor nodes and this broadcast lasts until it finds the destination.

Since the nodes are in mobility, it aims to adapt the network links rapidly. The protocol uses target sequence numbers to remember the latest path information

of all routes that occur. Here, each node maintains its sequence number so that during the RREQ forwarding process, the intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet was received in their routing tables and create a reverse route. When the RREQ reaches the desired destination or an intermediate node with a sufficiently new route to the destination, the destination or intermediate node responds by unicast back to the neighbor from which it first received a route response (RREP) control packet. Thus, a route path is established from the source node to the destination node and vice versa. The route recently used to transmit data packets is called Active Route. If a link breaks while the transmission on the route is active, the node upstream of the break emits a path error (RERR) message to notify the source node about the currently unreachable destination. If the source node still requests a route after receiving this RERR message, it can restart route discovery. Different variants of AODV have been developed, LQ-AODV, AODV-PA, AODV-ST, AODV-HM in order to improve the performance of the protocol [15].

Destination Sequenced Distance-Vector (DSDV)

It is one of the first routing protocol for ad hoc networks developed based on the Bellman-Ford proposed for the wired networks which consider the shortest path as a route for the destination. In DSDV protocol, all the nodes maintain the hop count for each destination and they update the routing table periodically. This causes a slow performance when a link breaks on a path since all the nodes need to calculate the shortest path and update the routing table from starch. Therefore, there are two different update methodologies, incremental and full dumps. When a node does not notice any substantial changes in the local topology, the incremental update is employed, and the update just contains data that has changed since the last full dump. The full dump is a complete dump utilized when there have been noticeable topology changes and the message contains all routing table data [15].

Overall the protocol works very well in networks where fewer nodes exist and with low moderate mobility. However, it shows poor efficiency in larger networks such as ad hoc networks where the nodes need to maintain all the route information for the destination node.

2.3.3 Security in Ad Hoc Networks

Security is an important issue for ad hoc networks, especially for security-sensitive applications. If cyber attackers get into the signal range, they will usually be able to connect to a wireless ad hoc network, and thereby connecting to the devices. This topic has been studied by many different researchers, e.g., Zhou and Haas [23] studied on secure routing and how to set up a secure key management service on private networks. Stajano and Anderson [19] proposed a solution called *resurrecting duckling* which is a security policy model that defines a device's secure temporary relationship with multiple serialized owners.

The studies on security in ad hoc networks can be broadly classified into two different schemes: the *credit-based* scheme in which a payment system is set up for each node to be paid to transmit packets, and the *reputation-based scheme* in which misbehaving nodes will be detected by network nodes and disconnected from the rest of the network.

Another important issue to manage in MANETs is its high power consumption. Some individual nodes may be selfish enough to take advantage of other nodes and may not want to share their own resources. These nodes may refuse to transmit data due to their selfish behavior. Such nodes are called *misbehaving* or *selfish* nodes.

Several different techniques [13], [5], [6] have been proposed to detect the effects of such nodes, and some have also been proposed [14] to avoid using these nodes in ad hoc networks to transmit a data packet.

In a study by Marti et al. [14] some techniques are suggested for MANETs similar to these of our work. They were developed for detecting the misbehaving nodes and avoid those nodes in a data packet transfer across the network. They use a *watchdog* logic that overhears the transmission on the wireless medium and identifies the misbehaving node, and *pathrater* logic which helps prevent those misbehaving nodes in future route selections. However, this proposed solution can only make successful detection if the next hop node is transmitting the data packet. Neither it did not propose a logic to notify the destination node about this misbehaviour.

In another study by Liu et al. [13], a solution proposed called *Acknowledgment-Based Approach*. In a nutshell, this solution proposes a special two-hop acknowledgment (2ACK) that will be sent back to the transmitting node that the data packet has been successfully received by the receiving node.

In a study by Suguna and Subathra [20], one of the most popular authentication schemes for ad hoc networks involves a distributed certificate authority based on Public Key Infrastructure (PKI) studied and proposed a solution. PKI concept has a certification to identify devices while communicating over a network. The cryptography used in PKI offers a virtual Certification Authority (CA) where many nodes perform certification services collectively. The concept of Certificate chaining fits very well with ad hoc networks due to its distributed and infrastructure-less manner. Also, it raises some questions about the access of the unknown nodes to the network a high level of security needs to be guaranteed. In order to improve the performance of the ad hoc networks, Suguna and Subathra proposed a scheme called *a stable chain-based authentication*. They aimed to handle the link breakage and unstable topology problems which causes unstable performance of MANETs with delays and losses of data packets. They proposed to do the chain of certificates through stable links that are already determined by each node in the chain with a calculation and showed that their proposed scheme shows better performance in terms of end-to-end delay, packet delivery late, and authentication time. But detection of a possible misbehaving node or an attacker node is not defined in this scheme.

3

System Model

We consider a wireless network formed with N communication nodes. For each node m, we have a C_m that have a good channel with m. Therefore, packets transmitted by node m_i can be correctly decoded by all nodes in C_m. This wireless network will be considered as a graph where nodes are the devices and two nodes are connected by an edge if there exists a direct communication link between them. We assume these direct communication links in this wireless network are authenticated, i.e., each node can verify that a received packet comes from the declared sender. This occurs only for each single hop. The wireless network will allow a data transfer from a source node (SN) to a destination node (DN) that cannot hear each other directly. Fig. 3.1 shows an example of the considered wireless network.

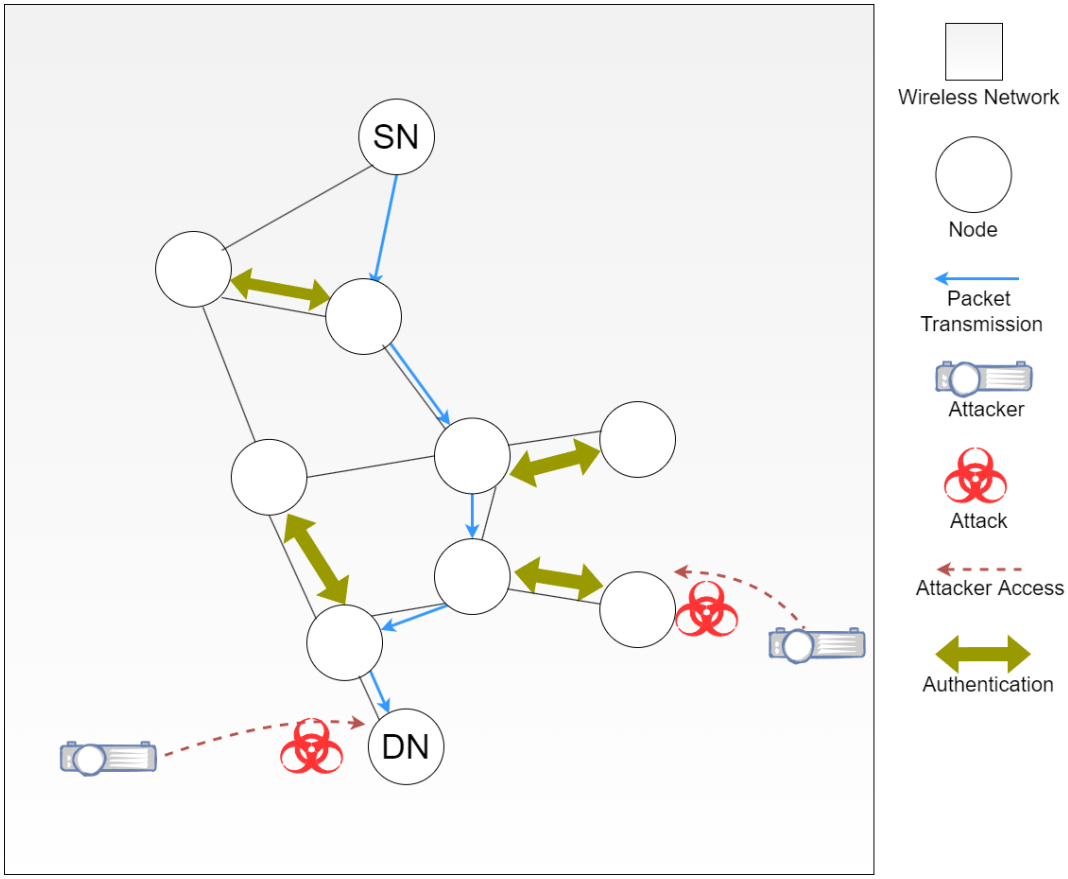

Figure 3.1: Wireless network packet transfer.

Transmitted data is organized in packets and each packet contains the route $\mathcal{R}$ of ρ nodes intended to be followed by the packet from SN to DN, i.e.,

$$\mathcal{R} = \{m_1, m_2, ..., m_\rho\}, \quad \text{where } m_i \text{ is } i^{\text{th}} \text{ node on the route.} \tag{3.1}$$

3.1 Attack Model

A spoofing node aims on transmitting packets to the DN impersonating the SN, i.e., making the DN believe that the packet comes from the SN. In this attack, the attacker can send the packet to any nearby node, which will forward it to the DN according to the route $\mathcal{R}$ indicated in the packet. Here we assume that either the authentication mechanism used by attacked node does not work so

that it will accept the packet (i.e. the receiving node is a victim) or the attacker is a node of the network itself.

3.2 Problem

In this work, we aim at designing an authentication mechanism such that the DN (together with the other nodes in the network) can distinguish between packets coming from SN and those coming from the attacker. To this end, the network nodes will cooperate in the authentication procedure.

3.3 Solution

We define the packet structure as in Fig. 3.2.

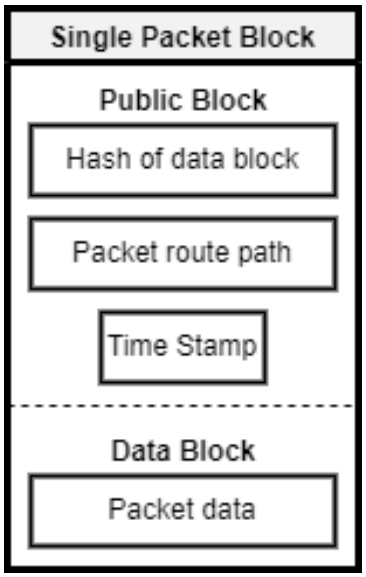

Figure 3.2: Packet structure

The packet includes two separate parts: the public and the data part. The public part has the hash of the data block, the route of the packet, and a timestamp (TP).

In order to prevent the attack, the protocol works as follows. The nodes that overhear the transmission, denoted as watch dog nodes (WDNs) will first check

that the packet is transmitted by a node on the route, and if so they will approve that it was transmitted by a routed node. The set of WDNs for node m is the subset of C_m not containing nodes of the route $\mathcal{R}$ i.e. Equation 3.2.

$$C_m \cap \mathcal{R}^c, \quad \text{where } \mathcal{R}^c \text{ is the set of } \rho \text{ in the route} \tag{3.2}$$

We define the set of WDNs of node m,

$$\mathcal{W}_m = C_m \cap \mathcal{R}^c \tag{3.3}$$

The same way we define the count of m authenticated by a WDN in the route $\mathcal{R}$ as ω.

Based on this check if the transmitted packet did not come from the actual node, the transmitter is either an attacker (AN) or a victim (VN). No matter if it is accessed from outside of the wireless network or by an impersonated node that was already in the wireless network, an alarm will be sent to the DN to warn that the incoming packet is not legitimate. Following this situation, this node will be excluded from the new route. The new route for sending the alarm to DN is called an alternative route (AR). Since there might be more than one attacker in this *WN*, alarm messages will also be sent by this protocol to be authenticated in each transmission.

The probability that a node has at least one WDN is

$$\beta = \mathbb{P}(|\mathcal{W}_m| \geq 1) \tag{3.4}$$

The probability that each node in route $\mathcal{R}$ has at least one WDN is

$$\upsilon = \mathbb{P}(m \in \mathcal{R} \cap |\mathcal{W}_m| \geq 1) \tag{3.5}$$

Let $\delta(\mathcal{E}) = 1$ if there is an AR from WDN m to DN given that nodes in the set $\mathcal{E}$ are corrupted, and $\delta_m(\mathcal{E}) = 0$ otherwise.

The probability of having an AR is

$$\phi = \mathbb{P}(\delta_m(\mathcal{E}) = 1) \tag{3.6}$$

where the randomness is given by the set of corrupted nodes.

The probability that each node in route $\mathcal{R}$ has at least one WDN and an AR is

$$\psi = \mathbb{P}(\forall m \in \mathcal{R}\ \exists m \in W_m : \delta_m(\mathcal{E}) = 1) \tag{3.7}$$

Fig. 3.3 demonstrates an occasion where an attacker node is detected by WDN. The WDN sends an alert packet to inform the DN that the incoming packet is not legitimate.

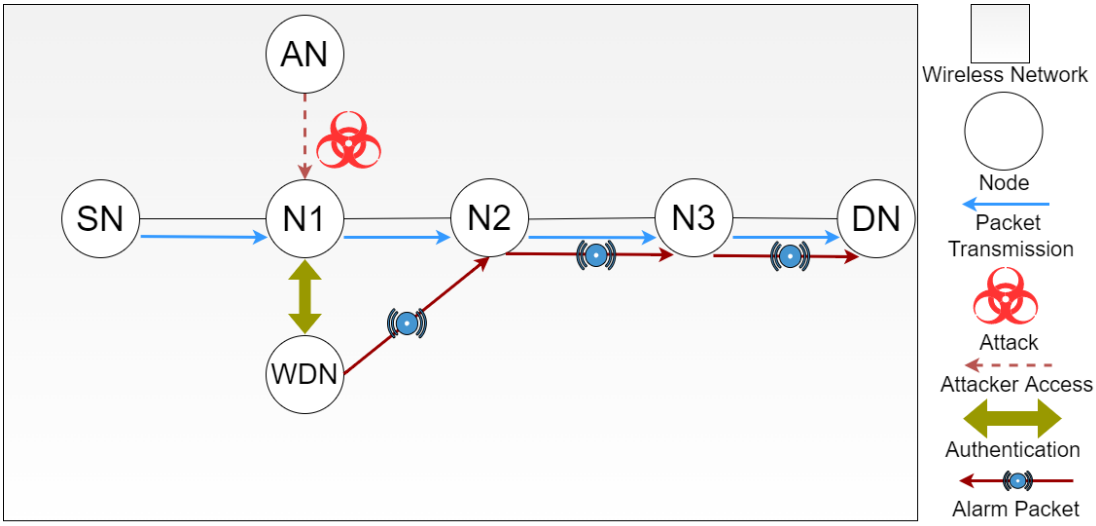

Figure 3.3: Attack detection and alarming by WDN through an AR.

4

Simulation Setup

We design a simulation system to generate random wireless networks using various variables such as the number of nodes in the network and the probability (α) of connections between the nodes. Then we assess the performance of the reported security method in the simulation.

4.1 Creating Wireless Network Graphs

Python3 was used for this solution to simulate, collect data about the network and perform the calculations to review the solution success rate with its own libraries. These libraries are **networkx** to create and manage complex networks, **pandas** to manipulate and handle the data sets, and **matplotlib** to create figures.

As a first step, we chose **Erdös-Renyi** network model to create random graphs according to the Chapter 3. In a nutshell, the idea of this model is to start with creating a network with the given number of nodes and no edges amongst them. Then choose randomly two pairs of nodes to be connected according to probability to connect any two nodes. The α is chosen as a unit interval between 0 and 1.

Total number of the possible edges is

$$\frac{N(N-1)}{2}\alpha \quad , \tag{4.1}$$

where N is the total node count in the network.

Based on this model an undirected graph network was created and the

following steps are implemented to generate a network.

1. Initialize an empty graph from the networkx library

```
    G = networkx.Graph()
```

2. Create nodes into this graph for the given number of nodes

```
    G.add_nodes_from(range(nodescount))
```

3. If the given α is 1, set it as a complete graph where every nodes are connected. If it is 0, set it to an edgeless graph where no edges exist. Else follow the next steps

4. Create a Python tuple which contains all the possible edge combinations

```
    edges = combinations(range(nodescount), 2)
```

5. For each node, select a random edge available from the edges tuple calculated above in order to guarantee that the created graph is connected. Then, loop through edges tuple for each node to add more edges selected randomly by comparing α with a float number in the interval $[0, 1)$ like below

```
    if random.random() < probability:
        G.add_edge(*an_edge_from_tuple)
```

Following these steps provides us not only a graph where each node has an edge but also ensures that the resulting graph has at least one route from one node to any other node.

After the graph has been created, the *Bellman-Ford* algorithm was used to calculate all the shortest paths between nodes. Roughly, this algorithm works in a bottom-up manner. It calculates the distance from SN to all the other nodes and then selects the shortest paths for each node pairs. This algorithm was chosen because it does not loop through the same nodes over and over while finding a path. So, it is applied to calculate the paths between each nodes with networkx library function and stored into a Python 3 dictionary like below.

```
path_dict = dict(networkx.all_pairs_bellman_ford_path(G))
```

Thus, a Python3 dictionary with the shortest path for each pair of nodes P obtained. A random path has been selected from this dictionary by using python uniform random variable generator.

Fig. 4.1 below shows an example graph of the wireless network built with 10 nodes and α of 0.1. The node that initiates the first packet transfer is called SN, and the last node to receive this packet is called DN in the graph. The edges

marked with green color display the randomly selected route for the packet transfer between SN and DN.

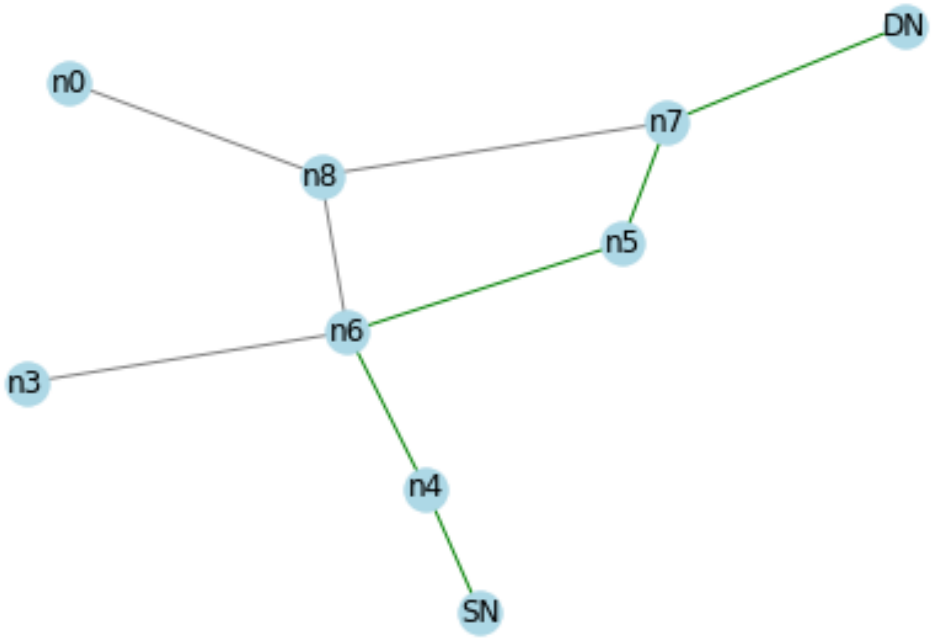

Figure 4.1: Random generated wireless network graph.

4.2 Collecting Data Sets

Nodes that have a connecting edge are called neighboring nodes (NN). A NN is defined by the edge existing between its pair. In order to label a NN as a WDN it has to be able to pass the (3.5). The WDNs were used to calculate the percentage of the nodes authenticated in route $\mathcal{R}$. An AR is calculated starting from this WDN by excluding that node to which the WDN neighbors like described in the (3.6) to calculate the percentage of the system monitored. All the shortest ARs are listed from this WDN to DN using **all_shortest_paths** function of the python **networkx**.

A Python3 **dataframe** was created to store those information of the nodes in the R. This dataframe named as *Route Analysis*.

The process of obtaining these data sets is repeated a thousand times with different values for the total nodes and α to gather more consistent data.

Table 4.1 shows an example of a dataframe obtained from the analysis of the

network Fig. 4.1.

Table 4.1: Route Analysis

node	neigbors	WDN	ARs
SN	1	0	0
N4	2	0	0
N6	4	2	1
N5	2	0	0
N7	2	1	0
DN	1	0	0

According to result set Table 4.1, there are only two nodes has at least one WDN can authorize the transmissions and only one node has an AR to communicate with the DN to send an alarm packet.

To define the authentication level of the network with this solution three different proportions were considered for υ, ϕ and ψ.

Overall data collection steps were repeated for a hundred times with a variety of the values of:

- Total number of nodes N
- Probability α
- Route length $|R|$

Following Table 4.2 shows an example of the data sets obtained during the data collection step. This data sets were created in order to calculate υ, ϕ and ψ according to equations described in Section 3.3.

According to Equation (3.3), a data set is collected to analyze WDNs in the $\mathcal{R}$ route. These results are averaged because these samples are collected in simulations where networks are constructed a thousand times for each selected α and N values. The Table 4.3 shows a sample data set captured during network simulations for $N = 10$. The collection of the data set is repeated for every N selected; 10, 20, 30, 50 and 100.

Table 4.2: Network Analysis

N	α	v(%)
10	0,01	44
	0,05	59
	0,1	71
	0,25	91
	0,5	99
20	0,01	55
	0,05	73
	0,1	87
	0,25	99
	0,5	100
50	0,01	65
	0,05	91
	0,1	99
	0,25	100
	0,5	100
100	0,01	72
	0,05	99
	0,1	100
	0,25	100
	0,5	100

Table 4.3: WDN ω Analysis for N=10

N	α	$\omega = 0$	$\omega = 1$	$\omega = 2$	$\omega = 3$
10	0.01	1.376	3.217	0.146	0.001
	0.05	1.508	3.01	0.616	0.029
	0.1	1.513	2.926	1.027	0.093
	0.15	1.343	2.924	1.449	0.154
	0.2	1.338	2.887	1.658	0.269
	0.25	1.275	2.763	1.915	0.397
	0.3	1.07	2.695	2.225	0.545
	0.35	1.01	2.603	2.331	0.758
	0.4	0.846	2.492	2.551	0.916
	0.45	0.662	2.29	2.778	1.146
	0.5	0.537	2.049	2.935	1.409

5

Numerical Results

In this chapter, we evaluate our authentication approach using the simulation networks described in Chapter 4. We used them to visualize and analyze the randomly created networks successful authentication level from Section 3.1.

5.1 Analysis of Node Authentication

Equation (3.5) is used to prove that a node in route $\mathcal{R}$ is authenticated by the WDNs. Following this, the network is analyzed according to the pairs of N & α and, $|R|$ & α.

Following Fig. 5.1 is an analysis result of the networks evaluated with N & α pair based on the data frames we obtained.

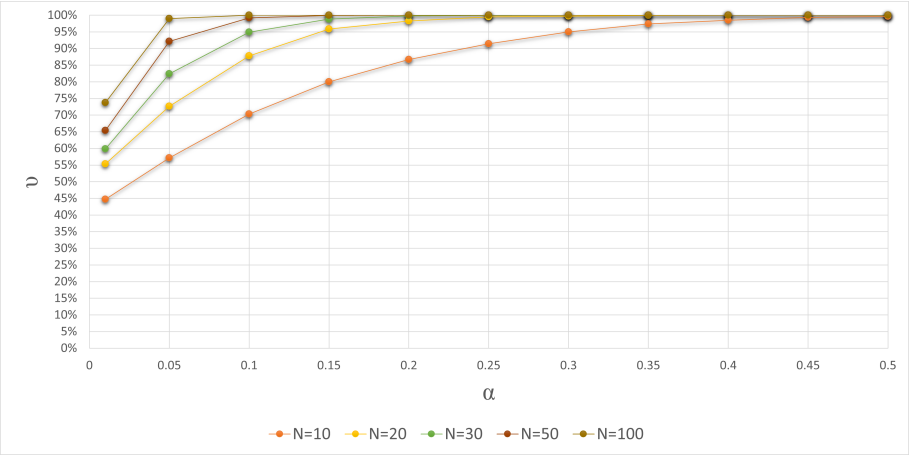

Figure 5.1: Probability υ vs probability α for various number of nodes M.

As α increases, the υ increases, since α directly affects the edge existing between the nodes. This increases the chance of getting a WDN for each node in the $\mathcal{R}$. We see that the first data frame with $\alpha = 0.01$ and $N = 10$ gives an authentication level 45% and this rate increases gradually. It reaches 100% when $\alpha = 0.4$ and $N = 20$ and continues same with α increasing. The same correlation can be observed with all other α. Considering this fact, we can evaluate that the closer the value of α to 1, the more likely nodes can be authorized by WDN.

Meanwhile, we see the same equivalently between N and υ. While the N is steadily increasing, the chances that a WDN exist for N_i will also increase the same way. Thus, for example, at $\alpha = 0,01$, $N = 20$ is more robust than $N = 10$, although α is at lower values. While N increases, it is significantly quicker to reaching the peak of N_i υ. For example, when $N = 100$ and α is $0,05$ all the nodes in $\mathcal{R}$ already have a WDN, even this can be a complete graph.

In order to approach the node validation level analysis from another angle, we made a new data set and examined it. This data set was obtained this time with grouping by the $|R|$ and α by not considering the N.

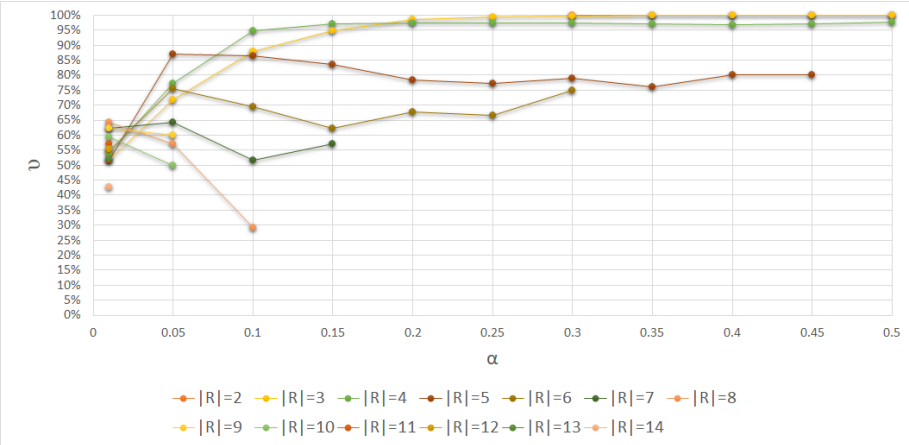

Figure 5.2: Probability υ vs probability α for various $|R|$.

In this analysis, we cannot observe a linear increase in the υ level where $|R|$ value is low such as 2, 3. The reason for this is that while the α is low, the rate of nodes connected being on $\mathcal{R}$ decreases the same way. However, we can observe the equivalent of α and υ as in the previous analysis. But where α is low, it's not possible to say exactly that.

We can say that the relation between $|R|$ and v is inverse proportion with minor inconsistencies. The reason for these minor inconsistencies in the graph is that the $|R|$ are chosen randomly, regardless of the N. The fact that having low value of N and an $|R|$ value close to this number in some randomly generated networks may explain this situation. Likewise vice versa of this. Another reason to have these inconsistencies are having a $|R|$ high value only while the N is high.

5.2 Analysis of Route Authentication

In order to analyze an R in the network, we need to consider R_n have at least one W and from this W there exists an AR to D as explained in Equation 3.6.

In the Fig. 5.3 below, we will see the correlation between the N and α on overall R_i.

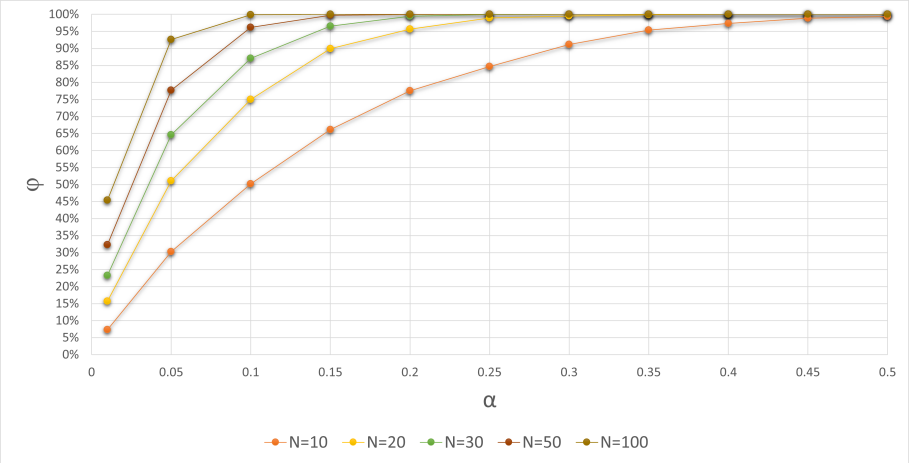

Figure 5.3: Probability ϕ vs probability α for various number of nodes M.

At first glance, we see that the route verification level rate is lower than in Fig. 5.2. This is because the calculation is done taking into account R_n individually in the previous analysis but here each R_i affects the overall rate for the level of route validation since we are looking for an existing of AR.

We observe that the route authentication level is low where the α is low, as we have seen in the past analysis. The α and route authentication levels have a straight ratio, so the graph also increases linearly. If we consider the part where the $N = 10$, the α of nodes connecting to each other should be quite high so that more probably an AR exist there overall for R_n. Meanwhile, when we check

how the N affects the route authentication level, we see a similar result with the correlation to α. It is very clear to say that the reason for this is although N increases and you have a low α such as 0.05, this α is proportional to the N and thus more edges are obtained. Therefore, we see that with the increase of N, the peak point is reached quickly in numbers such as 50, 100 and continues the same way with higher α as linear.

In the following analysis we will see the correlation between $|R|$ and α on route authentication level. So, the Fig. 5.4 shows this relationship with the selected α values.

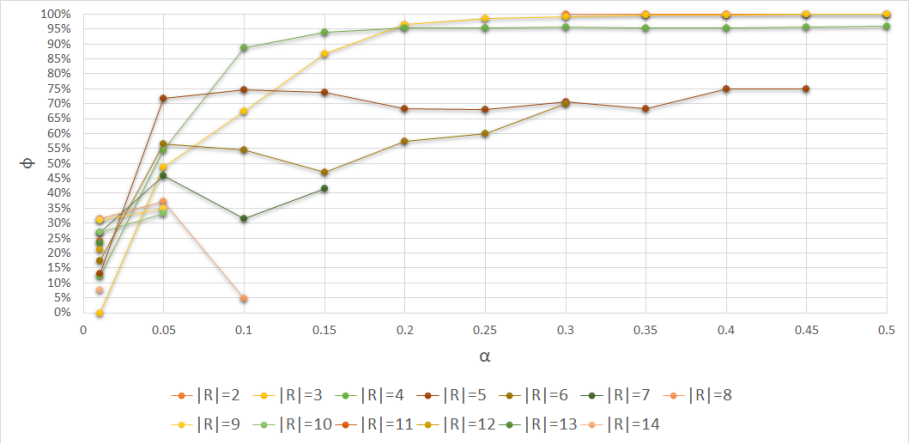

Figure 5.4: Probability ϕ vs probability α for various $|R|$.

In this graph, we observe irregular increases while the α value is low as in the previous $|R|$ and α analysis. It is possible to observe that it even goes to 0 in some values such as at $|R| = 3$ and $\alpha = 0.01$ or at $|R| = 5$ and $\alpha = 0.3$ where it is hard to obtain an AR for R_i. This may also be due to the random sampling of networks with various R values from these particular points compared to other generated networks. We can see better sampling with $|R| = 3$ or $|R| = 4$. We can observe the direct ratio with α by considering these samples. It is possible to say that R is better authenticated and AR exists to D when attempting short-range packet transfer (lower value of $|R|$).

5.3 Analysis of Full Network Authentication

In this section we will analyze the network on a different angle. In addition to the analysis of the authentication of each R_i, we examined the authentication of R_n. Moreover, we need at least an W for R_n and an AR. This analysis was made according to Equation 3.7. The Fig. 5.5 shows the resulted graph of this analysis.

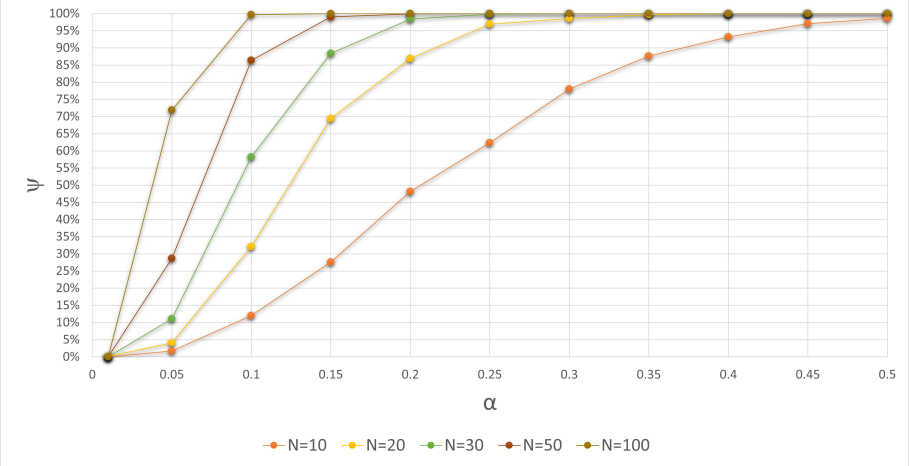

Figure 5.5: Probability ψ vs probability α for various number of nodes M.

When we look at the previous analyzes, we see that the authentication level is lower here. This is because as specified in Equation 3.7, in this analysis each node must have a WDN and an AR from those nodes to the DN. Therefore, when we consider that this should be provided at every m node in the $\mathcal{R}$ route, this rate will definitely decrease.

We observe that at low α values, namely $0.01 or 0.05$, it is not possible at all to have control over the entire network. Despite the increase in N, it is not possible to observe significant changes in these authentication levels. However, with the joint increase in N and α, we can say that it is not difficult to have control over the entire network. Therefore, we can state that analysis shows us that high authentication level rates can be achieved in the network with very high α values or very high numbers of N.

5.4 Analysis of WDN Workload

In this part of the analysis, we take another perspective to understand the roles of WDN in the route $\mathcal{R}$. We consider Equation(3.3) and hence Table 4.3 along with the other N selected as the backbone of this analysis. We created this analysis for values of ω <=3. The following figures (Fig. 5.6, 5.7, 5.8, 5.9, 5.10) display the resulted analysis in graphs.

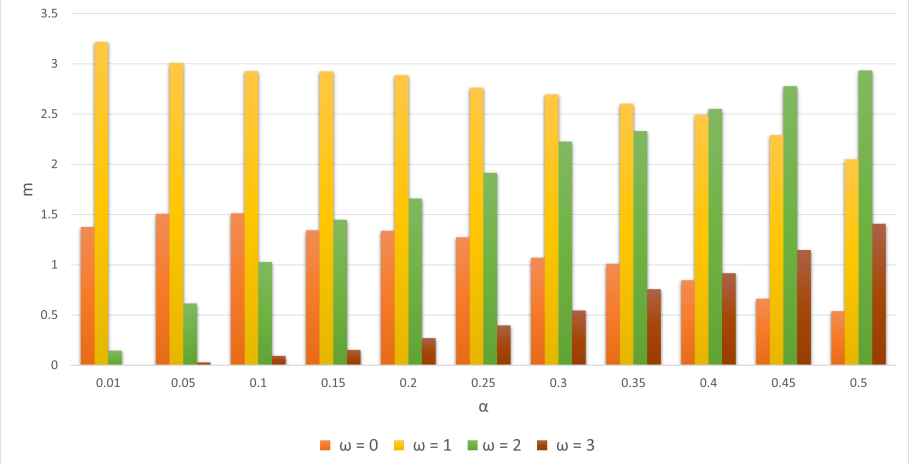

Figure 5.6: Count of node m with ω for various α and $N = 10$.

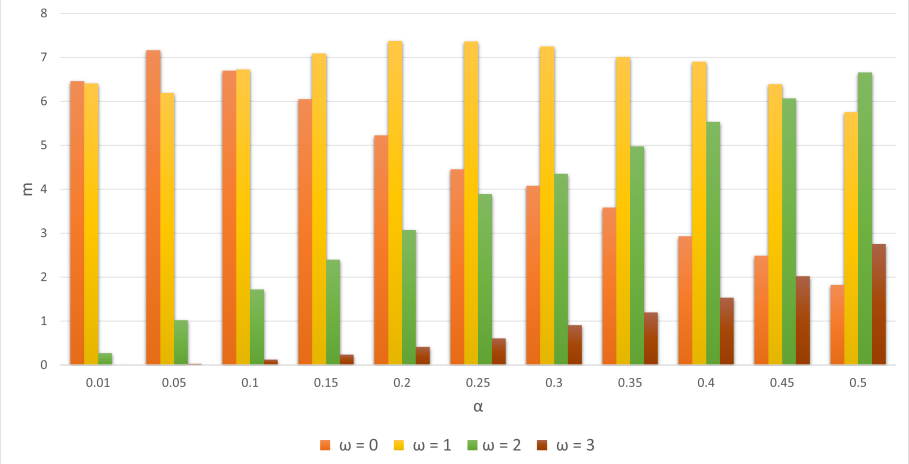

Figure 5.7: Count of node m with ω for various α and $N = 20$.

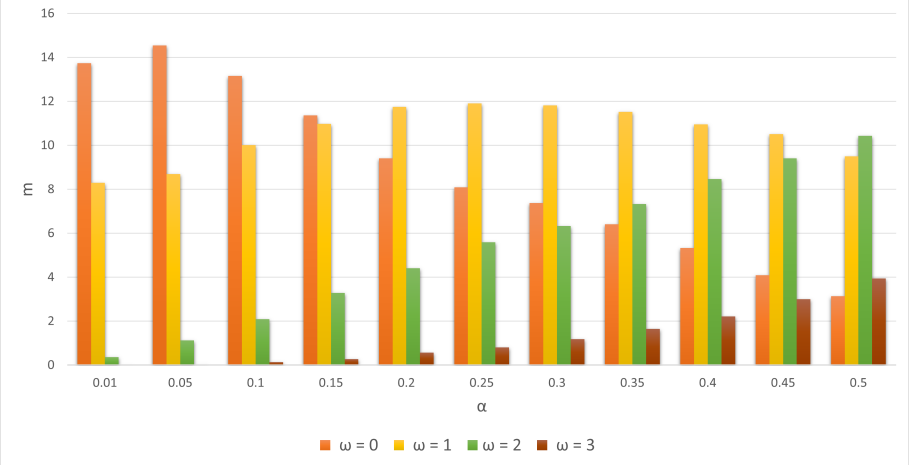

Figure 5.8: Count of node m with ω for various α and $N = 30$.

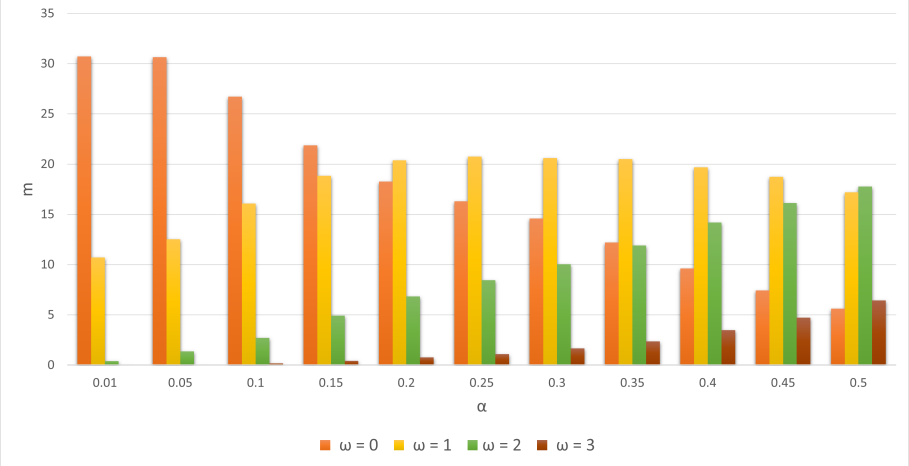

Figure 5.9: Count of node m with ω for various α and $N = 50$.

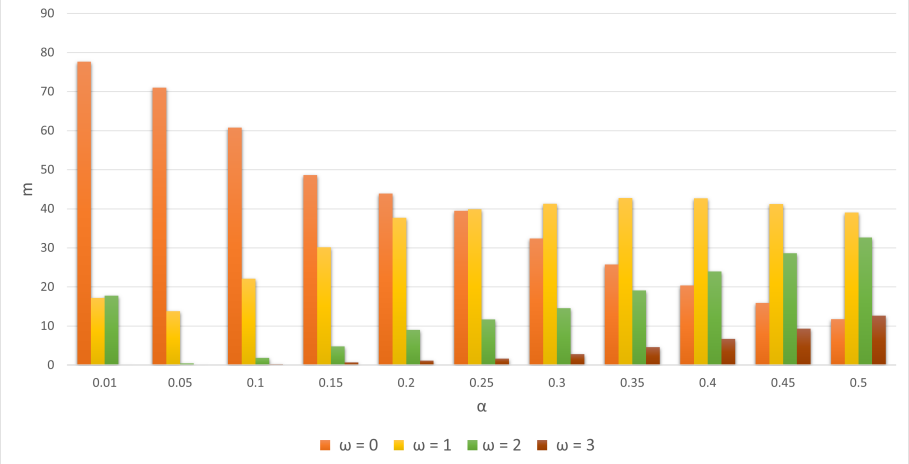

Figure 5.10: Count of node m with ω for various α and $N = 100$.

Looking at these numbers, we see that within a lower α value such as 0.01, 0.05, the nodes have quite a few neighbors, so WDNs have few connections to a node m on the route $\mathcal{R}$. We can observe that having numerous WDNs with $\omega = 3$ is only possible with a higher α value, and this ratio increases linearly. Likewise, we observe that while $\omega = 0$ ratio decreases, α ratio increases.

In the other hand, we can say that a WDN controlling multiple nodes can actually weaken the system's authentication rate in cases where the WDN is misbehaving.

6

Conclusions

It is known that wireless networks without a centralized entity such as ad hoc networks have a problem authenticating the transmitter nodes in a data packet transfer.

We presented an authentication mechanism by checking whether the transmitter node is on the route $\mathcal{R}$ specified by the first node where the data transfer starts, SN, for each transmission to the last node, DN. In cases this authentication fails for any node, the authenticator node, WDN, sends an alarm packet through a new route, AR, to DN by eliminating that node in order to notify that the incoming packet is not legitimate.

We created a setup in to analyze and perform the tests for the proposed solution. The results in showed us that a high ratio of success on the detection of misbehaving nodes is easier in the networks where high number of the communication links exist for the nodes in the route $\mathcal{R}$. Also, obtaining a secure AR is slightly difficult where fewer communication links exist.

We analyzed wireless networks with various node counts and thus, proved that the presence of more nodes in the wireless network drives more control mechanisms and increases the percentage of authentication with the probability of multiple neighbors occurring at each node in the route $\mathcal{R}$.

Also, we analyzed the same networks with different route $\mathcal{R}$ lengths, and saw how this length affects authentication. Here, we have considered that consistent results may not occur in some networks and interpreted accordingly. Considering that these randomly selected route lengths are directly related to the total number of nodes in the network, we can say that the presence of excess

nodes and communication links also increases the percentage of authentication.

Finally, we analyzed how many nodes a WDN controls on the route and realized the robustness of the authentication mechanism when a WDN misbehaves, such as being AN or VN.

We can conclude that wide networks with many nodes can increase the security of the system. Considering that this may not be the case for every wireless network, the WDN definition can be extended to include nodes in the route as well. For example, any neighboring node can be considered a WDN. Thus, one step further, a receiving node can also act as a WDN to the transmitter node.

References

[1] Norman Abramson. "The ALOHA system: Another alternative for computer communications". In: *Proceedings of the November 17-19, 1970, fall joint computer conference*. 1970, pp. 281–285.

[2] S. Basagni, D. Turgut, and S.K. Das. "Mobility-adaptive protocols for managing large ad hoc networks". In: *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240)*. Vol. 5. 2001, 1539–1543 vol.5. DOI: 10.1109/ICC.2001.937178.

[3] Giuseppe Bianchi, Luigi Fratta, and Matteo Oliveri. "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs". In: *Proceedings of PIMRC'96-7th International Symposium on Personal, Indoor, and Mobile Communications*. Vol. 2. IEEE. 1996, pp. 392–396.

[4] Azzedine Boukerche et al. "Routing protocols in ad hoc networks: A survey". In: *Computer networks* 55.13 (2011), pp. 3032–3080.

[5] Sonja Buchegger and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol". In: *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. 2002, pp. 226–236.

[6] Levente Buttyan and J-P Hubaux. "Enforcing service availability in mobile ad-hoc WANs". In: *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No. 00EX444)*. IEEE. 2000, pp. 87–96.

[7] Ray-Guang Cheng et al. "Ripple: A wireless token-passing protocol for multi-hop wireless mesh networks". In: *IEEE Communications Letters* 10.2 (2006), pp. 123–125.

[8] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005, pp. 535–558.

[9] *IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*. 2021, pp. 47–497. DOI: 10.1109/IEEESTD.2021.9442429.

[10] David B Johnson, David A Maltz, Josh Broch, et al. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks". In: *Ad hoc networking* 5.1 (2001), pp. 139–172.

[11] John Kindervag. "The five myths of wireless security". In: *Information Security Journal* 15.4 (2006), p. 7.

[12] Lixin Li and Huisheng Zhang. "A novel effective protocol design for wireless ad hoc networks". In: *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)*. Vol. 1. IEEE. 2009, pp. 361–364.

[13] Kejun Liu et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs". In: *IEEE transactions on mobile computing* 6.5 (2007), pp. 536–550.

[14] Sergio Marti et al. "Mitigating routing misbehavior in mobile ad hoc networks". In: *Proceedings of the 6th annual international conference on Mobile computing and networking*. 2000, pp. 255–265.

[15] Renato Mariz de Moraes and Hamid R Sadjadpour. "Wireless network protocols". In: *Mobile Communications Handbook*. CRC Press, 2017, pp. 603–614.

[16] Asis Nasipuri, Jun Zhuang, and Samir R Das. "A multichannel CSMA MAC protocol for multihop wireless networks". In: *WCNC. 1999 IEEE Wireless Communications and Networking Conference (Cat. No. 99TH8466)*. Vol. 3. IEEE. 1999, pp. 1402–1406.

[17] Tammy Noergaard. *Embedded systems architecture: a comprehensive guide for engineers and programmers*. Newnes, 2012, pp. 54–67.

[18] Oran Sharon and Eitan Altman. "An efficient polling MAC for wireless LANs". In: *IEEE/ACM Transactions on networking* 9.4 (2001), pp. 439–451.

[19] Frank Stajano and Ross Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks". In: *International workshop on security protocols*. Springer. 1999, pp. 172–182.

[20] M Suguna and P Subathra. “Establishment of stable certificate chains for authentication in mobile ad hoc networks”. In: *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*. IEEE. 2011, pp. 234–239.

[21] Hideaki Takagi and Leonard Kleinrock. “Throughput analysis for persistent CSMA systems”. In: *IEEE transactions on communications* 33.7 (1985), pp. 627–638.

[22] Peng Xie and Jun-Hong Cui. “R-MAC: An energy-efficient MAC protocol for underwater sensor networks”. In: *International Conference on Wireless Algorithms, Systems and Applications (WASA 2007)*. IEEE. 2007, pp. 187–198.

[23] Lidong Zhou and Zygmunt J Haas. “Securing ad hoc networks”. In: *IEEE network* 13.6 (1999), pp. 24–30.

Acknowledgments

My sincere thanks go to my supervisor Professor Stefano Tomasin for guiding me with big patience all the time. I am indebted to him for his invaluable assistance and insights leading to the writing of this thesis. I would also like to thank my professors who generously helped us learn for all the courses during this Masters degree.