JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 06 Issue 02
2024

Research Article
https://doi.org/10.56979/602/2024

A Technique for Safeguarding Legitimate Users from Media Access Control (MAC) Spoofing Attacks

Makhdoom Muhammad Naeem[1], Intesab Hussain[2*], and Malik Muhammad Saad Missen[3]

[1]NFC Institute of Engineering & Technology, Multan, Punjab, Pakistan.
[2]Quaid-e-Awam University of Engineering, Sciences & Technology, Pakistan.
[3]The Islamia University of Bahawalpur, Pakistan.
[*]Corresponding Author: Makhdoom Muhammad Naeem. Email: makhdoomnaeem@nfciet.edu.pk

Received: December 30, 2023 **Accepted:** January 29, 2024 **Published:** March 01, 2024

Abstract: Both wired and wireless networks are susceptible to MAC spoofing attacks, in which an attacker pretends to be a legitimate user on the network by changing the MAC addresses of both Ethernet and wireless devices. Authorized MAC addresses can, however, be easily impersonated to launch a variety of attacks, including phishing, denial-of-service attacks, SIP Registration hijacking attacks, and denial-of-access attacks. Cybercrime detectives face a formidable barrier when attempting to impersonate a legitimate user's MAC address. We suggest using Kea DHCPv4 and MySQL as the back-end database to implement an SMS-based system. Our objective is to completely safeguard real users from MAC spoofing assaults. The combination of MAC address and mobile number as host-name is what distinguishes the suggested technique from others. If the legitimate user is utilizing the network service, he can ignore the alarm message from the SMS application. If not, the legitimate user can tell the network administrator to block the IP address of the errant user. In this article, we successfully apply the suggested technique, identify the intruder via SMS alert message, and safeguard the machine of the authorized user via the network administrator. A prototype is used to confirm the veracity of the suggested methodology. The discussion section goes into further detail about how the proposed methodology was implemented using this prototype.

Keywords: MAC Spoofing; Network Security; Kea DHCP.

1. Introduction

Everything in today's society is interconnected, making a trustworthy network crucial for businesses to generate value. Society is a prime target for threat actors because of how heavily it relies on network connectivity. The network's access layer is a particular weak point. This does not require strong access controls like the data center and is open to anyone who is in the organization's public cafe or waiting area.

In the modern network, there are many different kinds of devices, some of which are outdated and others that do not support contemporary authentication and security techniques. Threat actors arise as a result of this evolution, and they discover new techniques to hack into networks and gadgets that can't keep up. Due to the possibility of them being used as a point of entry by a threat actor, they might therefore be regarded as a security flaw in the network. Using certificates, authentication can be carried out to confirm a device's legitimacy. However, the device must have the resources and processing power to handle these kinds of authentication and requests, in addition to supporting the protocols being used, in order to be able to authenticate using certificates. The security of an organization and society at large is thereby compromised by gadgets that do not enable secure authentication techniques.

A cyberattack constitutes a purposeful and malicious endeavor, undertaken by either an individual or a collective, with the intent of compromising the security of an information system belonging to another individual or group. Typically, the attacker wants to gain whatever good will they can by disrupting the victim's network. Man-in-the-middle (MiTM), malware, phishing, denial-of-service [1], registration hijacking [2], SQL injection [3], DNS tunneling [4], and zero-day exploits [5] are the most frequent types of

assaults. A man-in-the-middle (MiTM) attack is a type of cyberattack in which an attacker uses a way to interfere with the communication process to intercept important data. It's possible for the attacker to passively observe your communication while secretly stealing your information, or they might actively take part and alter the substance of your messages or pretend to be the person or system you think you're speaking to. MAC spoofing, WEB site spoofing [6], ARP spoofing [7], DNS spoofing [8]}, GPS spoofing [9], Email spoofing [10]}, Caller-ID spoofing [11], IP spoofing [12], Text Message spoofing, and other popular assault methods.

Attackers may be able to enter networks through spoofing techniques. A spoofing attack may go unnoticed for a considerable amount of time, in contrast to ransomware assaults, where the threat actor may want the targeted organization to be aware that an attack is taking place. The attacker is thought to have remained undetected on the network for an average of 146 days until the breach was discovered.

An attempt to impersonate a legitimate MAC address is known as a MAC address spoofing attack. The attacker located valid MAC addresses on the network. The attacker then presents himself as the device's default-gateway and imitates all the data transferred to it without being noticed. Attacks such as MAC spoofing are started by computer clients on a network's layer 2. MAC spoofing is the kind of attack where the cybercriminal can also get around authentication checks because it offers this as the default gateway and copies all data sent to the default gateway covertly, giving you all the important details about the applications and logical addresses of the end host. There are numerous distinct attack types, and each one takes advantage of a unique network vulnerability. A higher danger of spoofing attacks exists with MAC spoofing. By taking advantage of these flaws, the attacker can access a person's private information without authorization.

The majority of earlier MAC spoofing research was based on wireless networks. Previous studies have employed a variety of techniques, including Machine Learning via Artificial Neural Networks (ANN), Channel State Information (CSI) based on Kalman filtering, Received Signal Strength Indicators (RSSI), Random Forest Ensemble Method and RSSI, PHY Alert, Algorithm and Shared Key Exchange, and Centralized Co-operative Detection Algorithms (CCDA). [13-19]. The detection of MAC spoofing can be done using a variety of methods, including sequence number analysis, received signal strength-based detection, random forest ensemble method, dynamic MAC change, CSI, etc. A malicious user may be misclassified by any of these methods as authenticated and only interested in wireless networks. The permitted user of the IEEE 803.3 and 802.11 networks is not always protected by any kind of technique. All of the available solutions, nevertheless, have only concentrated on analysis, simulation, and wireless network prototypes. To secure MAC addresses, each of these solutions consists of a clearly stated methodology. None of them, however, can be utilized to confirm the attacker who is impersonating the assailant using the same IP-MAC address.

DHCP, short for Dynamic Host Configuration Protocol, is the dominant protocol for the data link layer. DHCP is neither immune to network intrusions nor flexible enough to prevent third parties from intercepting communications. Numerous networks already make use of the modern DHCP Protocol. These networks include workplaces, manufacturing facilities, educational institutions, and pretty much anything connected to the Internet. Numerous Organizations Were Targeted by Hackers Using the DHCP Vulnerability [20]. Kea, sometimes referred to as DHCP, developed an open-source DHCP server known as the Internet Systems Consortium (ISC). The ISC Kea software is available for download as a source code via GitHub [21], several ISC websites, and a number of operating systems, including the Fedora project, FreshPorts, Ubuntu packages, Debian packages, and Arch Linux packages. Under the terms of the Mozilla Public License 2.0, Kea is permitted [21]. The Kea distribution contains a dynamic DNS server (DDNS), a DHCPv6 server, and a DHCPv4 server. Kea can save leases locally in a memfile, or in a MySQL, Cassandra, or PostgreSQL database.

In this study, a Kea DHCPv4 implementation with MySQL as the backend is used to construct an SMS-based solution. The SMS-based DHCP strategy has not yet been suggested. The main objective is to completely defend legitimate users from MAC spoofing attacks. The crucial aspect of this method is that the hostname is replaced with a mobile number, the IP address is bound to the MAC address, and the MySQL database has been given access to leasing data regarding the active DHCP clients. The Twilio Website is used to send alert messages to the DHCP host users. The SMS sender's programme will send alert message to the genuine user and the SMS receiver will ignore the message as a legitimate user;

otherwise, it will contact the network administrator to block this fraudulent user. Thus, in this paper, we established an SMS-based detection technique to generate a warning message against MAC spoofing assault.

The rest of this paper is organized as follows: In Section \ref{Related}, we discuss the associated work; Section \ref{Spoofing} presents MAC Spoofing Attacks; Section \ref{Kea} presents ISC Kea DHCP. In Section \ref{Protection}, we present Protection Technique for MAC Spoofing Attack; Section \ref{Discussion} presents discussion and results. Finally, Section \ref{Conclusion} presents conclusions and future work.

2. Related Work

The Artificial Neural Network (ANN) is a machine learning-based detection approach introduced by Benzaïd et al. in their research [13]. This method successfully overcomes limitations associated with threshold-based strategies. ANNs empower the capability to categorize and identify network behavior even in the presence of noisy, imperfect, constrained, and non-linear data sources.

Li and Sezgin [14] proposed an adaptive detection scheme based on Kalman. Using the knowledge of the predicted channel, they eliminated the channel estimation error, especially the random phase error that occurred due to the lack of synchronization between the transmitter and the receiver. In addition, they defined Kalman residual-based test statistics for attack detection.

Alotaibi and Elleithy [15] reported an inactive outcome that requires no modifications to protocols or standards. They conducted experiments using two air monitors as sensors on a real test bench (a WLAN), achieving accuracy rates of 99.77%, 93.16%, and 88.38% when the attacker was positioned at 8~13 m, 4~8 m, and less than 4 m away from the victim device, respectively. Their approach exhibited improved performance when applying the three earlier strategies to the same benchmark. The author's solution is primarily based on the utilization of random forests.

Jiang et al. introduced a spoofing attack detection system named PHYAlert [16], designed to safeguard WiFi-based edge networks. PHYAlert enabled real-time validation of Wi-Fi frames, utilizing rich dimensional data within the PHY Wi-Fi layer to characterize wireless connections. The researchers conducted comprehensive experiments across various scenarios, employing commonly accessible devices to develop PHYAlert. Their findings demonstrated an impressive eight-fold reduction in the false positive rate compared to conventional methods relying on signal intensity. This underscores the viability of spoofing detection based on physical layer information.

Liu [17] focused on identifying the MAC spoofing assault at the PHY layer by applying a centralized cooperative detection algorithmic program in multi-user networks. Generally, they proposed an intrusion detection approach that achieves the channel fingerprint power (CFPP) in a time-varying slow-fading channel as well as derives the CFPP computation approach with the thought of estimation error. As it is a challenge for the suspect factor function design, they designed it and discussed its characteristics.

In their research, Yu and colleagues [18] introduced a model designed for the efficient detection of device spoofing incursions. This model offers the capability to continuously monitor the physical network attributes of devices, ensuring the detection of significant alterations in the measured values. To illustrate the effectiveness of their proposed algorithm, they conducted an empirical study within a real ZigBee (IEEE 802.15.4) network. During this study, they analyzed the variations in RSSI values of packets at different physical distances.

Hegde [19] proposed an algorithm that utilizes shared key exchange methods and advanced smart antenna technologies to effectively identify and prevent MAC spoofing.

The authors have furnished a compendium of directives and strategies for the detection of MAC address spoofing. It is notable that previous investigations into MAC spoofing primarily concentrated on wireless networks. The identification of MAC spoofing can be accomplished through an assortment of techniques, encompassing CSI analysis, sequence number scrutiny, detection grounded on received signal strength, utilization of the random forest ensemble method, dynamic MAC address changes, and more [13–19]. It is worth mentioning that some of these methods may erroneously flag legitimate users who are merely inquisitive about the wireless network and not yet authenticated. Consequently, it is crucial to recognize that not all these methods afford protection to authorized users of both wired and wireless networks.

3. MAC Spoofing Attack

Attacks on identity theft occur when a hacker is successful in presenting himself as a genuine user of a system. The act of disguising a message or identification to make it appear to come from a trustworthy and authorized source is known as identity theft. Despite the fact that they are all forgery attacks, sniffing and spoofing attacks are distinct from one another. In a spoofing attack, a malicious program or party pretends to be another computer device or user on a computer network in order to launch an attack against data theft, network hosts, access controls, or virus distribution. The malicious actor will frequently use identity theft to access broader cyberattacks, such as a "man-in-the-middle" attack.

Changing the device's MAC address is referred to as MAC spoofing. By changing their MAC address to match one of the authorized devices on the network, hackers can get access to a network, and it is a simple process. Linux allows for the simple installation of Macchanger, which can be used to change the MAC address to one's preference with the following command:

sudo macchanger - custom-address interface

When a malicious programme or party poses as another user or device on a computer network to launch an attack against data theft, network devices, access controls, or virus distribution, this is known as a MAC spoofing assault [22]. An attack on a network known as the "Address Resolution Protocol (ARP) spoofing" occurs when an attacker sends false Address Resolution Protocol (ARP) messages to the internal network with the intention of intercepting and diverting network traffic [22]. In order to conceal oneself, an attacker uses IP spoofing to broadcast Internet Protocol (IP) packets from a false source address (also known as "identity theft"). Every computer or other device that can access the Internet has a logical (IP) address, which is comparable to your residential address. Attacks that cause a denial of service (DoS) frequently use IP spoofing to flood networks and devices with packets that are from legitimate source logical addresses [12].

DNS cache poisoning, also known as domain name server (DNS) identity theft, refers to an attempt to use updated DNS records to divert online traffic to a fraudulent website that mimics the target website [8]. DNS spoofing is a technique that directs a client-user to a false website rather than the one they intended to visit. If you are a victim of DNS spoofing, you may believe you are connecting to a secure, reliable website while in reality you are dealing with a scammer. Creating an email with a fictitious sender address with the intent to trick the recipient into sending them cash or sensitive information is known as phishing [10]. Banks and other financial institutions' email accounts are occasionally targeted by hackers. They can observe transactions between an organization's clients and themselves at any given time as they grow entry. In order to communicate their own instructions to customers, the attackers can then impersonate the institution's email address.

It is the practice of constructing a website in an attempt to deceive readers into thinking it was created by someone other than the actual creator or creators of the website. The scam website frequently uses the target website's look and occasionally has a URL that is identical to the target website [23]. When "HTTPS" rather than "HTTP" is used to identify a website, it indicates that the website is secure and reliable. As a matter of fact, the "S" stands for "safe." Your HTTP browser can be duped by an attacker into believing that you are visiting a reliable website when you are not. The attacker can monitor your interactions with that website by redirecting your web browser to an insecure HTTP one and possibly stealing the personal information you are sharing.

Caller Identity (ID) spoofing is the practice of manipulating the telephone network to inform the telephone receiver of a call that the call's initiator is a different base than the call's true initiating base [11]. Sending a text message to the sender ID or another person's phone number is known as text message spoofing or Short Message Service (SMS) identity theft. If you're still texting from your computer, the message isn't coming from your phone; instead, you're spoofing your own phone number to send it. When hackers need to hide dangerous executable files, extension spoofing is used. The name of the file being anything like "filename.txt.exe" is a common extension faking the trick that offenders like to use. Normal Windows users will see this executable file as "filename.txt" since violators are aware that file extensions are hidden in Windows by default.

A GPS recipient is being tricked during a Global Positioning System (GPS) spoofing assault by a fake GPS signal being transmitted from Earth. The erroneous location begins to appear in all neighboring browsers. In addition to being used to steal drones and cars, GPS spoofing can also be used to fool sailors

and cab drivers [24]. Through the practice of "facial spoofing," a criminal can undermine or make an attempt at a facial recognition system while pretending to be a licensed user, getting access to and advantages from the system that are not legal [25]. Hackers can make Wi-Fi links with names that sound quite legitimate and are similar to those of an adjacent organization in order to eavesdrop on Wi-Fi communication. Once a consumer connects to the hacker's WiFi, the assailant will have access to all of the client's online activity as well as the buyer's credit card information, username and password, and other details.

4. ISC Kea DHCP

A dynamic DNS update daemon that offers a REST API for DNS update servers and DHCP control, a Control Agent (CA), and fully working DHCPv6 and DHCPv4 servers are all included in the Kea DHCP software created by Internet Systems Consortium (ISC), Inc. In addition to hosting reservations, releases, renewals, rebinds, rejections, address assignments, DNS updates, client classification, information requests, and server discovery, both DHCP servers also assist with server discovery. Lease data is by default stored in the CSV file. We can choose to store leasing data in databases like MySQL, PostgreSQL, and Cassandra rather than a CSV file. It is possible to keep host reservations in a configuration file, a MySQL, PostgreSQL, or Cassandra database. Help for YANG models is provided by Kea's DHCPv4 and DHCPv6 daemons. These models can be created using the NETCONF protocol and are stored in a Sysrepo database [26].

5. Protection Technique for MAC Spoofing Attack

We devised a technique to safeguard trustworthy clients against MAC spoofing attacks. We have configured and installed ISC Kea DHCP4 with the backend database as MySQL. The DHCP server keeps lease information in the MySQL database. Every user, even legitimate or illegitimate, on the network receives a logical address, MAC address, and hostname from the DHCP server. To send alert messages to the registered users via the application, we used the hostname as the cellphone number. The hostname, MAC address, and IP address of each user who connects to the network are recorded in the MySQL database. We developed a program that pulls the most recent lease data from the database. The lease table is where the application collects hostname information. After obtaining the host name as the mobile phone number, the application sends a warning message to that number regarding the user, saying "If you are using network services, then OK; otherwise, notify the network administrator about an illegal user."

5.1. Network Architecture

We have implemented the network architecture as per the client-server architecture shown in Figure 1. We have installed Ubuntu LTS 20.04 as the operating system, ISC Kea DHCP4, MySQL as the DATABASE backend server and an application that sends messages to legitimate users, in the server machine. We have used the Ethernet network for different services such as DHCP, MySQL, SMS Application and we have also used the twilio website through the wireless network. The network address, that is, 192.168.100.0/24, has been used for the DHCP network configuration, as shown in Table 1, and the network address, that is, 192.168.10.0/24, has been used for Internet over the wireless network as shown in Table 2.

5.2. Kea DHCPv4 Configuration

The DHCPv4 protocol uses the User Datagram Protocol (UDP) transmission and, in some instances, uses unicast. DHCPv4 server machines listen on port 67, same as DHCPv4 clients listen for messages on port 68 from a server. The initial request from the client requires Layer 2 (Ethernet) connection. DHCPv4 configuration is shown in Figure 2 and Figure 3}. The primary configuration parameters of our investigation are given below.

"**Dhcp4**": The Dhcp4 configuration begins with "Dhcp4": { on the first line with the opening brace (or bracket). All configurations must hold an object that designates the ISC Kea configuration module that uses it.

"**interfaces-config**": To ensure proper configuration of the Kea DHCP server, it is imperative to specify the network interfaces on which the DHCP service should be active. This is achieved through the utilization of the "interface-config" option, which defines a list of network interfaces (e.g., enp10s0) that the DHCP

server is intended to listen on. The list of interfaces is enclosed within square brackets, and multiple items are separated by commas.

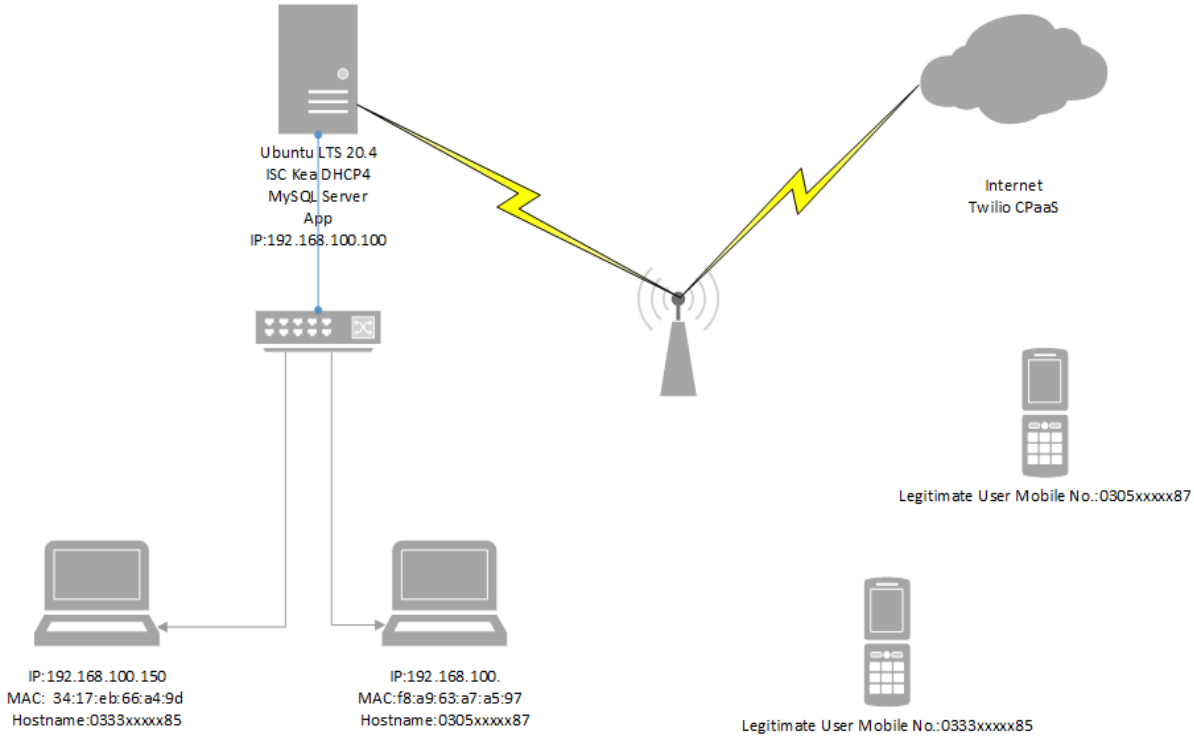

Figure 1. Network Architecture of Protection Techniques

Table 1. Network Configuration for DHCP

IP Address	MAC Address	Hostname	Gateway	Connection
192.168.100.150	34:17:EB:66:A4:9D	0333xxxxx85	-	Ethernet
192.168.100.151	F8:A9:63:A7:A5:97	0305xxxxx87	-	Ethernet

Table 2. Configuration for WAN

IP Address	MAC Address	Hostname	Gateway	Connection
192.168.10.9	58:91:CF:2F:14:3F	makhdoom-research-platform	-	Ethernet

"**Control-sockets**": The control socket delineates the communication conduit connecting the management tools to the DHCP server process. The configuration specifies the files to which the UNIX domain sockets are linked within the "dhcp4" map. Specifically, the socket name is set as "/tmp/kea4-ctrl-socket," and the socket type is designated as "Unix."

"**Lease-database**": Configuring the storage location for lease data is a crucial aspect of Kea DHCP setup. The ISC Kea-DHCP4 server offers the flexibility to employ multiple database backends for managing hosts, leases, and settings. In our specific configuration, we've employed MySQL as the backend. The "lease4" table, housed within the "research_platform_db" database, contains all the leases assigned by the DHCP server. The parameters set for the DHCPv4 lease database intricately define the configuration of the lease database.

"**Valid-lifetime**": Some DHCP parameters, such as the renewal timer, rebind timer, and valid lifespan, possess a global scope and impact all subnets and pools under the DHCP server's management. In this context, the addresses have been allocated a lifespan of 4000 seconds.

"**subnet4**": Address assignment is a central function of Kea DHCPv4. In this configuration, it involves the establishment of at least one IP subnet and a set of dynamic IP addresses organized into pools. The network segment linked to the server carries the 192.168.100.0/24 prefix. While the subnet is conveyed as plain text, it's worth noting that the pool argument is, in reality, a list of pools, and thus, it is encapsulated within square brackets. The range of addresses designated for this particular pool spans from 192.168.100.0 to 192.168.100.255.

"**Reservations**": There are numerous scenarios in which having a pre-host setup proves beneficial. One straightforward application is to allocate a dedicated static IP address for an individual host or client's exclusive use. Host reservations are established as variables within each subnetwork. Each host must possess a unique identifier, often based on their MAC address or physical address. Within the subnet4 structure, an optional reservation layout is available. It is essential to incorporate a distinct host identity into the design, with MAC or physical addresses frequently serving as the identification method in DHCPv4 systems. In most circumstances, a logical address will be defined. You can also define a host name, options supplied by the host, or fields included in the DHCPv4 message, for example, siaddr, sname, or file. This is a reservation for a MAC / hardware address. It's a pretty simple host reservation: just an address, a hostname, and nothing else.

```
// This is an example configuration file for the DHCPv4 server in Kea.

{ "Dhcp4":

{

// Kea is told to listen on ethX interface only.
  "interfaces-config": {
    "interfaces": [ "enp10s0" ]
  },

  "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea4-ctrl-socket"
    },

   "lease-database": {
      "type": "mysql",
      "name": "research_platform_db",
      "host": "localhost",
      "port": 3306,
      "user": "makhdoomnaeem",
      "password": "Naeem0000",
      "connect-timeout": 3
   },
```

Figure 2. Kea DHCP4 Configuration Part (a)

5.3. MySQL as a backend Database

In order to use the database for host reservation and lease settings (IP addresses, MAC addresses, mobile number as host name, etc.), we configured Kea-DHCPv4 to do so. The various backend databases are referred to as backend. Here, we have created a relational MySQL database and used it to store lease data. The database area is established in MySQL when the database has been set. On the MySQL server, we have created a database with the name research_platform_db. There are various fields in the lease4 table, as depicted in Figure 4. Only the hwaddr, expiration, and hostname from the lease4 database have been used by our software.

5.4. Application for Short Message Service

As seen in Figure 5, we have created a Python programme to send out automatic SMS messages to defend the legitimate user from MAC spoofing assaults. For the client object, we have imported two modules: the MySQL connector and one from twilio.rest. We utilized the account_sid and account_token functions from the Twilio website. In order to obtain DHCP leases, we then wrote a Python program that connects to a MySQL database. By using the Structured Query Language (SQL) select command, we have extracted the hostname that serves as a mobile number from the lease4 table of the database (research_platform_db). As seen in Figure 6} and Figure 7}, the program has delivered messages to authorized users for the legal or illicit use of network services based on this code.

```
// Addresses will be assigned with a lifetime of 4000 seconds.
  "valid-lifetime": 4000,
//  "renew-timer": 1000,
//  "rebind-timer": 2000,

  "subnet4": [
   {
      "pools": [ { "pool":  "192.168.100.101 - 192.168.100.200" } ],
      "subnet": "192.168.100.0/24",
       "interface": "enp10s0",

       "reservation-mode": "all",
       "reservations": [
// This is a reservation for a specific hardware/MAC address. It's a very
// simple reservation: just an address and nothing else.
        {
            "hw-address": "34:17:eb:66:a4:9d",
            "ip-address": "192.168.100.150",
            "hostname": "+9233        85"
        },
        {
            "hw-address": "f8:a9:63:a7:a5:97",
            "ip-address": "192.168.100.151",
            "hostname": "+9230        87"
        }

      ]
    }
  ]
}
}
```

Figure 3. Kea DHCP4 Configuration Part (b)

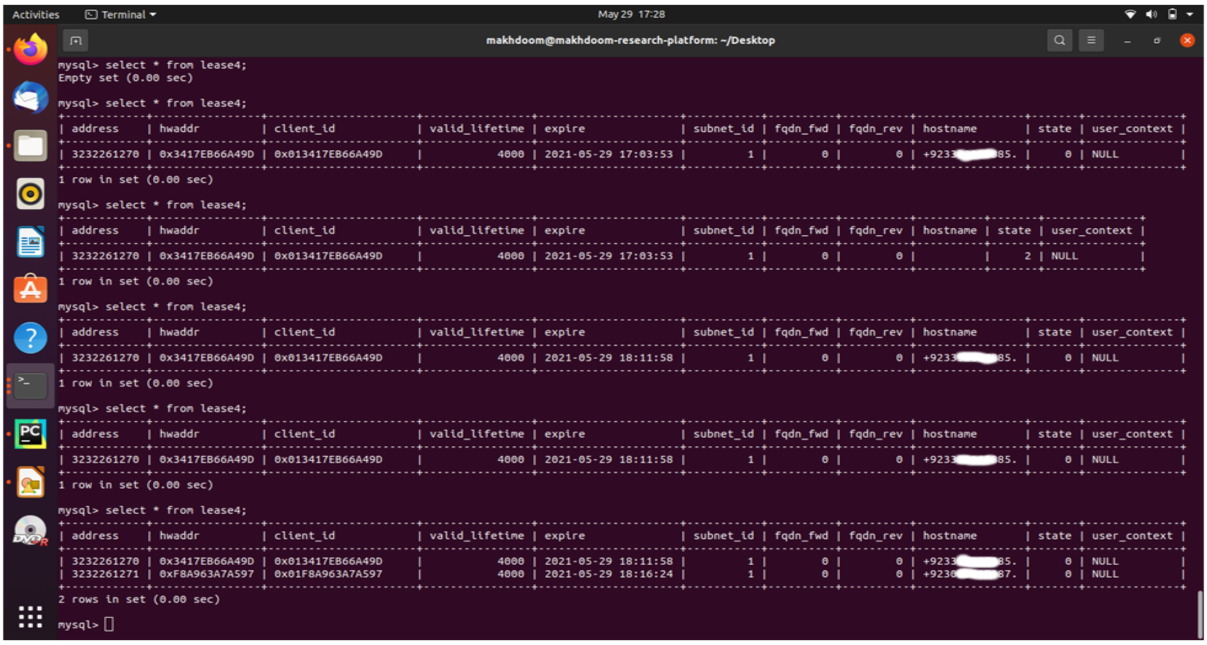

Figure 4. MySQL Lease 4 Table

```
from twilio.rest import Client
import mysql.connector



account_sid = "AC5d8be0ade74458ce3094c7450d6146fc"
auth_token = "191a99a950ca866c4ea41207b9a66b00"

client = Client(account_sid, auth_token)

mydb = mysql.connector.connect(host="localhost", user="root",
passwd="[illegible]",
                    database="research_platform_db",
auth_plugin="mysql_native_password")

mycursor = mydb.cursor()
mycursor.execute("select hostname from lease4 WHERE expire IN (SELECT
max(expire) FROM lease4)")

myresult = mycursor.fetchone()
for row in myresult:
   mobile_number = row
client.messages.create(
      to=mobile_number,
      from_="+19545046167",
      body="Welcome to QUEST network, if you are using QUEST network,
ignore this message otherwise notify manager IT that an illegitimate user is using
your IP and MAC address. Thank you."
)
```

Figure 5. Send SMS Code in Python

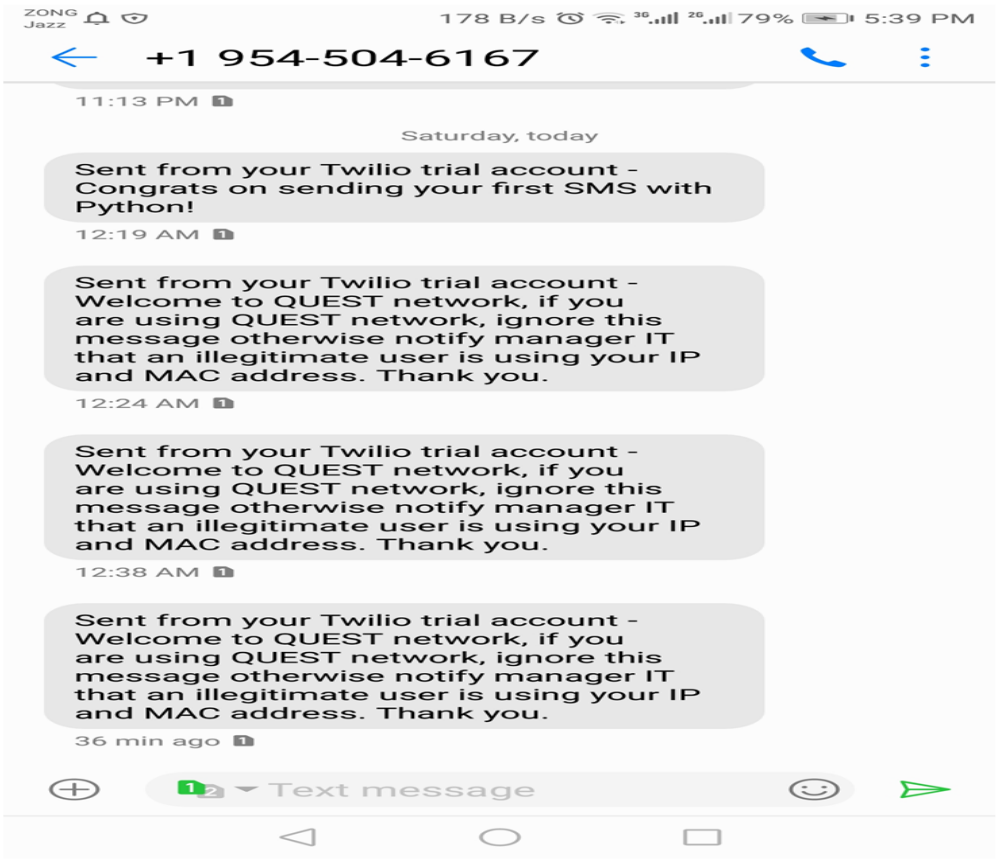

Figure 6. Alert message through SMS 0333xxxxx85

Figure 7. Alert message through SMS 0305xxxxx87

6. Discussion

MAC spoofing is the sort of attack where the cyberpuk can also bypass authentication checks as it offers this as the default-gateway as well as copies all data passed to the default-gateway without being identified, giving you all the important details about the applications as well as the logical (IP) addresses of the end host. There are many distinct kinds of attacks, and each one takes advantage of a different network vulnerability. The risk of spoofing assaults is larger with MAC spoofing. These flaws can be exploited by the attacker, who will then be able to access the victim's private information without authorization.

In this paper, utilizing Kea-DHCPv4-MySQL-SMS to detect and defend against MAC spoofing attacks, we implemented a reliable approach on a prototype network. Table 3 demonstrates that the only solutions [13-19] that were already in place and could handle the analysis mode were wireless threshold, CSI, signal strength, channel fingerprint, and algorithm based on smart antennas.

The discussion demonstrates that, in order to implement the best protection measures, both detection and prevention approaches should be used in the network. It is also important to take into account reducing the amount of time that cryptography operations take to complete in order to minimise network security inconveniences. All prior solutions, however, have been wholly centred on wireless network analysis, modelling, and prototyping. To secure MAC addresses, each of these solutions consists of a clearly stated methodology. But none of these can be used to confirm that an attacker is using the same IP-MAC address as the attacker. As a result, the method we've suggested is quite powerful and efficient against MAC spoofing attacks using Kea-DHCPv4-MySQL-SMS to identify and safeguard the legitimate user.

Table 3. Comparison between different approaches against MAC spoofing attack

Paper	Approach	Technique	Operation Mode	Results
[13]	Detection	Machine Learning through ANN	Analysis	Identified and classified different network behavior of data sources.
[14]	Detection	CSI based through Kalman filtering	Analysis	Used the Kalman filtering based test for Attack Detection
[15]	Detection	Random Forest	Analysis	MAC address spoofing detection based

		Ensemble Method and RSSI		in random forests
[16]	Detection and Protection	PHY Alert	Prototype	Protected edge networks through PHY layer information based on identity detection
[17]	Detection	CCDA	Simulation	Proposed a centralized cooperative detection algorithm against MAC spoofing attack
[18]	Detection	RSSI	Analysis	Proposed framework for monitoring physical network devices
[19]	Detection and Protection	Algorithms and shared key exchanges	Algorithm	Used shared key exchange techniques and algorithms based on smart antenna technology

ANN, Artificial Neural Network; CSI, Channel State Information, RSSI, Uniform Resource Indicator, CCDA, Centralized Cooperative Detection Algorithm.

7. Conclusions and Future Perspectives

In this article, we implemented a solution based on the Kea DHCPv4-MySQL-SMS technique, which provides detection and protection to legitimate users against MAC address spoofing. All of the above methods based on wireless networks assume that they focus only on wireless channels. Our thorough prototype assessments have shown that the robust security performance of our suggested solution is very strong. As it beats all previously proposed client-based approaches in terms of various security approaches, we developed a method for detecting MAC address spoofing based on Kea-DHCPv4-MySQL-SMS. Furthermore, through the network administrator, it has given authorized users defense against MAC spoofing assaults. Expanding and putting the idea into practice in a real organization will be part of our future efforts. It is possible to assess and, if necessary, improve the design through the use of the technique.

Acknowledgments: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest: The authors confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

References

1. I. Hussain, S. Djahel, Z. Zhang, F. Nait-Abdesselam, A comprehensive study of flooding attack consequences and countermeasures in session initiation protocol (sip), Security and Communication Networks 8 (18) (2015) 4436–4451, doi.org/10.1002/sec.1328.
2. M. M. Naeem, I. Hussain, M. M. S. Missen, A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP), Computer Networks 175 (2020) 107250, doi.org/10.1016/j.comnet.2020.107250.
3. V. Abdullayev, A. S. Chauhan, SQL Injection Attack: Quick View, Mesopotamian Journal of CyberSecurity 2023 (2023) 30–34, SQL Injection Attack: Quick View.
4. M. Sammour, B. Hussin, M. F. I. Othman, M. Doheir, B. AlShaikhdeeb, M. S. Talib, DNS tunneling: A review on features, International Journal of Engineering and Technology 7 (3.20) (2018) 1–5, DNS tunneling: A review on features.
5. N. Peppes, T. Alexakis, E. Adamopoulou, K. Demestichas, The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers, Sensors 23 (2) (2023) 900, The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers.
6. S. Mathankar, S. R. Sharma, T. Wankhede, M. Sahu, S. Thakur, Phishing Website Detection using Machine Learning Techniques, in: 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP), IEEE, 2023, pp. 1–6, Phishing Website Detection using Machine Learning Techniques.
7. T. U. Chai, H. G. Goh, S.-Y. Liew, V. Ponnusamy, Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory, Systems 11 (4) (2023) 211, Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory.
8. N. U. Aijaz, M. Misbahuddin, S. Raziuddin, Survey on DNS-Specific Security Issues and Solution Approaches, in: Data Science and Security, Springer, 2021, pp. 79–89, doi.org/10.1007/978-981-15-5309-7 9.
9. M. Nayfeh, Y. Li, K. Al Shamaileh, V. Devabhaktuni, N. Kaabouch, Machine Learning Modeling of GPS Features with Applications to UAV Location Spoofing Detection and Classification, Computers & Security 126(2023) 103085, Machine Learning Modeling of GPS Features with Applications to UAV Location Spoofing Detection and Classification.
10. S. Maroofi, M. Korczynski, A. Duda, From Defensive Registration to Subdomain Protection: Evaluation of Email Anti-Spoofing Schemes for High-Profile Domains, in: Proc. Network Traffic Measurement and Analysis Conference (TMA), 2020, .
11. V. Buriachok, V. Sokolov, M. TajDini, Research of Caller ID Spoofing Launch, Detection, and Defense, arXiv preprint arXiv:2004.0031810.28925/2663-4023.2020.7.616 (2020).
12. V. Singh, S. Pandey, Revisiting Cloud Security Threats: IP Spoofing, Soft Computing: Theories and Applications: Proceedings of SoCTA 2018 1053 (2020) 225, 10.1007/978-981-15-0751-9 21.
13. C. Benzaïd, A. Boulgheraif, F. Z. Dahmane, A. Al-Nemrat, K. Zeraoulia, Intelligent detection of mac spoofing attack in 802.11 network, in: Proceedings of the 17th International Conference on Distributed Computing and Networking, 2016, pp. 1–5, doi.org/10.1145/2833312.2850446.
14. C. Li, A. Sezgin, Spoofing attack detection in dynamic channels with imperfect CSI, arXiv preprint arXiv:2101.06185(2021).
15. B. Alotaibi, K. Elleithy, A new mac address spoofing detection technique based on random forests, Sensors 16 (3) (2016) 281, doi.org/10.3390/s16030281.
16. Z. Jiang, K. Zhao, R. Li, J. Zhao, J. Du, PHYAlert: identity spoofing attack detection and prevention for a wireless edge network, Journal of Cloud Computing 9 (1) (2020) 1–13, doi.org/10.1186/s13677-020-0154-7.
17. S. Liu, MAC Spoofing Attack Detection Based on Physical Layer Char-acteristics in Wireless Networks, in: 2019 IEEE International Confer-ence on Computational Electromagnetics (ICCEM), IEEE, 2019, pp. 1–3, DOI: 10.1109/COMPEM.2019.8779180.
18. J. Yu, E. Kim, H. Kim, J. Huh, A framework for detecting MAC and IP spoofing attacks with network characteristics, in: 2016 International Conference on Software Security and Assurance (ICSSA), IEEE, 2016, pp. 49–53, DOI: 10.1109/ICSSA.2016.16.
19. A. Hegde, Mac spoofing detection and prevention, Int. J. Adv. Res. Comput. Commun. Eng 5 (1) (2016) 229–232.
20. A. Shete, A. Lahade, T. Patil, R. Pawar, DHCP Protocol Using OTP Based Two-Factor Authentication, in: 2018 2nd International Conference on rends in Electronics and Informatics (ICOEI), IEEE, 2018, pp. 136–141, 10.1109/ICOEI.2018.8553753.
21. Isc-Projects, isc-projects/kea (2016). URL https://github.com/isc-projects/kea
22. M. Anathi, K. Vijayakumar, An intelligent approach for dynamic network traffic restriction using MAC address verification, Computer Communications 154 (2020) 559–564, doi.org/10.1016/j.comcom.2020.02.021.
23. R. Prasad, V. Rohokale, Cyber threats and attack overview, in: Cyber Security: The Lifeline of Information and Communication Technology, Springer, 2020, pp. 15–31, doi.org/10.1007/978-3-030-31703-4 2.
24. J. Xie, A. S. Meliopoulos, Sensitive detection of GPS spoofing attack in phasor measurement units via quasi-dynamic state estimation, Computer 53 (5) (2020) 63–72, 10.1109/MC.2020.2976943.
25. Z. Akhtar, G. L. Foresti, Face spoof attack recognition using discrimina- tive image patches, Journal of Electrical and Computer Engineering 2016, doi.org/10.1155/2016/4721849 (2016).
26. [link]. URL https://kea.readthedocs.io/en/kea-1.8.1/_sources/ arm/intro.rst.txt