

A Secure and Optimized Authentication Scheme for Network Devices



**By
Naveed Husain**

Fall 2019-MS (IS) - 00000317540

Supervisor

Dr. Hasan Tahir Butt

Department of Computing

**A thesis submitted in partial fulfillment of the requirements for the degree of
Masters of Science in Information Security (MS IS)**

In

**School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.**

(August 2021)

Approval

It is certified that the contents and form of the thesis entitled "A Secure and Optimized Authentication Scheme for Network Devices" submitted by NAVEED HUSAIN have been found satisfactory for the requirement of the degree

Advisor : Dr. Dr Hasan Tahir

Signature:  _____

Date: 09-Aug-2021

Committee Member 1: Dr. Muhammad Moazam
Fraz

Signature:  _____

09-Aug-2021

Committee Member 2: Dr. Mehdi Hussain

Signature:  _____

Date: 09-Aug-2021

Signature: _____

Date: _____

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "A Secure and Optimized Authentication Scheme for Network Devices" written by NAVEED HUSAIN, (Registration No 00000317540), of SEecs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____  _____

Name of Advisor: Dr. Dr Hasan Tahir _____

Date: _____ **09-Aug-2021** _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

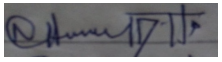
Dedication

This work is dedicated to my loving father and mother who remained by my side and supported me throughout this journey. Without their support and help, it would not have been possible hence their guidance on the value of education and constant encouragement contributed to this piece of work. I am eternally grateful especially to my loving grandfather **Muhammad Shareef** and my loving father **Mr. Jan Muhammad** for their full support both financially, socially, and shelter. I also dedicate this work to my loving mother who stood by me, prayed for me, and loved me unconditionally for as long as I can remember. They hold a dear place in my heart.

Certificate of Originality

I hereby declare that this submission titled "A Secure and Optimized Authentication Scheme for Network Devices" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: NAVEED HUSAIN

Student Signature: 

Acknowledgment

I am highly indebted and prayerful to the magnificent and Merciful Almighty Allah, who bestowed his immense blessings enabling me to undertake and complete the studies reported in this manuscript. Countless salutations are upon Prophet Muhammad (Peace be upon him) who declared it to be an obligatory duty of every Muslim to seek and acquire knowledge.

My deepest gratitude to my supervisor **Dr. Hasan Tahir Butt** for his continuous support and guidance during my thesis. I could not have imagined having a better supervisor and mentor for my master's degree. He will remain a great source of inspiration and kindness for me. I am also thankful to my teachers for providing me with an academic base, which enabled me to complete this thesis. The heartiest thanks and gratitude are also extended to my other two respected committee members **Dr. Muhammad Moazam Fraz** and **Dr. Mehdi Hussain** for their scholarly contribution, valuable suggestions, and constructive criticism toward the successful completion of the thesis. I am obliged to all my respectable teachers for sparing their valuable time and sharing the knowledge. I believe that this work would not have been possible without their cooperation and support.

I am very thankful to my elder brothers **Amjad Ali** and **Sajjad Ali** and all my fellows and friends for their support and motivation.

Last but not the least, I would like to thank my parents for their endless prayers and support throughout.

Table of Contents

Chapter 1	1
Introduction	1
1.1 Overview	1
1.2 Problem Statement	3
1.3 Solution Definition/Description	3
1.4 Thesis Motivation	4
1.5 Thesis Contribution	4
1.6 Thesis Organization	5
1.7 Summary	5
Chapter 2	6
Literature Review	6
2.1 Authentication	6
2.2 Authentication Techniques	6
2.2.1 Hash-chain Based Authentication	7
2.2.2 Multi-factor Authentication	8
2.2.3 Public and Symmetric key-based Authentication	9
2.2.4 Password-based Authentication	10
2.2.5 Digital Signature-based Authentication	11
2.2.6 Biometric Authentication	12
2.3 Summary	14
Chapter 3	15
Research Methodology	15
3.1 Introduction	15
3.2 Research Types	16
3.2.1 Qualitative vs Quantitative	16
3.2.2 Descriptive vs Analytical	16
3.2.3 Fundamental vs Applied	17
3.2.4 Conceptual vs Empirical	17
3.3 Research Methods and Research Methodology Overview	17
3.4 Thesis Research Methodology	18

3.5 Proposed Scheme Development Strategies	19
3.5.1 Overview of the Scheme Development Tool Scyther	19
3.5.2 Scheme Development Language	20
3.5.3 Why Scyther Tool is selected?	20
3.6 Summary	21
Chapter 4	22
Proposed Solution	22
4.1 Scheme Primitives	22
4.1.1 Timestamps	22
4.1.2 Hash Functions	23
4.1.3 Symmetric Cryptography	23
4.1.4 Random Numbers	24
4.2 Scheme Features	24
4.3 The Proposed Approach	25
4.3.1 Preface	26
4.3.2 Scheme Description	27
4.3.2.1 Proposed Scheme Sequence Diagram	27
4.3.2.2 Proposed Scheme Important Terms	28
4.3.2.3 Proposed Scheme Details	29
4.4 Table of Notations	31
4.5 Summary	32
Chapter 5	33
Implementation and Results	33
5.1 Scheme Analysis	33
5.2 Scheme Attributes	33
5.2.1 A minimal input file	33
5.2.3 Symmetric keys	35
5.2.4 Hash function	36
5.2.5 Events	36
5.2.5.1 Received and Send Events	36
5.3 Security Properties	37
5.3.1 Security Claims	37
5.3.1.1 Secrecy	37
5.3.1.2 Aliveness	39

5.3.1.3 Weak Agreement	39
5.3.1.4 Non-injective Agreement	40
5.3.1.5 Non-injective Synchronization	40
5.3.1.6 Running and Commit.....	41
5.4 Scyther Scripts.....	42
5.5 Scyther Results	44
5.6 Security Analysis	48
5.6.1 Man-in-the-Middle Attack.....	48
5.6.2 Replay Attack	48
5.6.3 False Data Injection Attack.....	49
5.6.4 Fake Node Injection	49
5.7 Proposed Scheme Performance Evaluation	50
5.7.1 Resource Accessibility and Availability.....	50
5.7.2 Numerical Results	50
5.8 Summary.....	53
Chapter 6.....	55
Conclusion & Future Work.....	55
6.1 Conclusion.....	55
6.1.1 Future Work.....	56
6.2 Summary.....	57
Bibliography	58
Appendices.....	62

List of Abbreviations

WNS	Wireless Networks
CR	Cognitive Radio
MDs	Message Digests
DoS	Denial-of-Service
SV	Secret Value
BS	Base Station
TS	Token Server
NN	Network Node
IS	Information Security
M2M	Machine-to-Machine
AS	Authentication Sever
IBS	Identity-Based Signature
CRNs	Cognitive Radio Networks
MITM	Man-in-the-middle attack
FDIA	False Data Injection Attack
TTA	Trusted Timestamp Authority
ECC	Elliptical Curve Cryptography
RFID	Radio-Frequency Identification
CIA	Confidentiality, Integrity, Availability
Spdl	Security Protocol Description Language
TD-SCDMA	Time Division - Synchronous Code Division Multiple Access

List of Tables

Table 1 Table of Notations.....	32
Table 2 Cryptographic Primitive and Algorithm	51
Table 3 Cryptographic Primitives Count.....	52

List of Figures

Figure 1 Research Types	16
Figure 2 System Model	25
Figure 3 Scheme Key Set	27
Figure 4 The Sequence Diagram of the Proposed Scheme.	28
Figure 5 Scyther Script-1	42
Figure 6 Scyther Script-2	42
Figure 7 Scyther Script-3	43
Figure 8 Scyther Script-4	43
Figure 9 Scyther Script-5	44
Figure 10 Scyther Script-6	44
Figure 11 Scyther Results-1	45
Figure 12 Scyther Results-2	46
Figure 13 Scyther Results-3	47

Abstract

In the technology world, the wireless network is more flexible and adaptable compared to the wired network. Because it is easy to install and does not require cables. Also, there have been many recent advances in the area of WNs (Wireless Networks), which have undergone rapid development. WNs is being emerged as a prevailing technology due to their wide range of applications in every field of life. The WNs are easily prone to security attacks since once deployed these networks are unattended and unprotected. In networks, authentication is a well-explored research area. Recent advancements in networks and ubiquitous devices have meant that there is a need to explore the area of authentication with a new perspective. This study explores authentication schemes and their adoption to network-connected devices. The research will study how a wide variety of devices like those in IoT, WSN, industrial IoT, wearable healthcare devices establish authentication. The focus of the study will be on high levels of security with an algorithm that has a small footprint.

The scheme will be studying the design of a lightweight and secure authentication framework for network-connected devices. The proposed scheme provides extended security features while minimizing wireless communication security challenges. The final results will validate the authenticity of this scheme.

Chapter 1

Introduction

The first chapter provides an overview of essential concepts, their importance, and the history of the research work. This chapter presents the study route map and briefly outlines the thesis subsequent arrangement and structure. The reasons for doing the research are explained in this chapter. This chapter also offers an overview of the study with major contributions, area of study, problem statement, and main goals.

1.1 Overview

A computer network is a collection of computers connected by digital interconnections and using a set of standard communication protocols to share resources located on or delivered by network devices. And a wireless network is a computer network that uses wireless data connections between network nodes. Network nodes use radio communications to send or receive data between each other. Wireless information systems have received much interest, and they are now widely utilized across the world to meet the communication demands of a huge number of end-users. A large scale wireless network is formed by the connectivity of multiple wireless communication systems, where "large scale" refers to the high density of network stations (or nodes) and the vast coverage area [1]. Moreover, a Wireless network is more flexible and adaptable compared to a wired network. Since it doesn't require cables so, it's very cost-effective and easy to install. Also, there have been many recent advances in the area of WNs networks, which have undergone rapid development. Wireless Networks (WNs) is being emerged as a prevailing technology due to their wide range of applications in military, industries, and civilian domains. The WNs play a vital role in the IoT, WSN, Smart cities, Cognitive Radio Networks (CRNs), and Industry 4.0 networks.

Over time computing devices and related technologies increase day by day. So, as the number of services available and the complexity of those services grows, the potential of elements infecting information systems also increasing at the same speed. Security plays an

CHAPTER 1. INTRODUCTION

important role in WNs architecture, as nodes may be deployed in enemy territory, contain private monitoring information, relay trade secrets, or possess other forms of sensitive data. The WNs are easily prone to security attacks since once deployed these networks are unattended and unprotected. Wireless natures of communication, resource limitation, secure communication, high risk of node addition/removal, etc. are major challenges. Because network resources and their communication data are very confidential, and moving upon the insecure network can create problems. If any network node or secrete communication is compromised then all the network goes to the attacker's hands. So, in any kind of computing system implementation of the security layers are very important due to which we protect our network from different types of attacks.

Many principles should be used to ensure secure communication between WNs nodes, which are known as security requirements: CIA (confidentiality, integrity, availability) and authentication [2]. Confidentiality [3] protects information by preventing unauthorized access to the system and/or personal information. Integrity is the protection mechanism need to ensure that information is not altered or destroyed unintentionally or deliberately [4]. This indicates that data is delivered without modification from source to destination. Only the sender can change the message without being detected by other nodes. Integrity safeguards data against illegal creation, modification, or destruction. If a corrupted message is acknowledged, a violation of the integrity property is identified [5].

Availability ensures that users have access to systems, apps, and data when they need them [6]. And the last important security requirement is authentication that can be defined as "Authentication is the process of verifying a user's stated identity." For achieving all other security properties authentication plays a crucial role in any kind of computing technology including wireless networks. Because it is a primary security constraint all other security requirements need proper authentication first [7]. In this study our main focus upon authentication. For secure communication in wireless networks authentication of nodes is very important. Because as previously said, the authentication procedure is regarded as the most important security aspect in wireless networks.

The authentication stage is critical to the proper operation of the information system. If anyone wants to mitigate the attack surface upon their network then the authentication phase

CHAPTER 1. INTRODUCTION

should be strong. Provisioning of resources to an adversary or a lack of providing to a legal user may be the result of poorly authentication. Problems during the authentication steps frequently result in system compromise, as has been widely reported in the literature [8]. This is the main point why authentication is so important. So, for achieving strong authentication in WNs a lot of secure authentication schemes are proposed. But most studied schemes in the literature are based upon public-key cryptography due to that during communication packet size increases rapidly that's are not feasible mostly in small wireless networks. Most wireless network nodes have limited resources (processing power, memory) that's why handling over payloads is very challenging for these nodes.

Although some authentication schemes are lightweight and suitable for WNs these are most vulnerable against many attacks. Our main focus is to propose the optimized and secure authentication scheme for WNs that provides strong and continuous authentication and also provides strong protection against common attacks vectors.

1.2 Problem Statement

Based on the issues found throughout the literature study, the following statement throws light on the problem at hand and a possible solution.

“Design and Implementation of secure and optimized authentication scheme for Network devices that use limited computing resources for secure communication over an insecure network.”

1.3 Solution Definition/Description

The proposed solution includes:

- Strong authentication and continuous authentication.
- The scheme will provide strong protection against common attacks (Man-in-the-middle, replay attack, false data injection attack, fake node injection).
- This study provides an authentication framework that is efficient, optimized, and less complex, takes less time for authentication time, and is secure for wireless network devices communication.

CHAPTER 1. INTRODUCTION

- Provide extending security features that minimize the wireless communication security challenges using less authentication time, power utilization, and less memory occupation.
- The proposed authentication scheme proved mutual and continues authentication to network devices until communication is performed securely over the insecure network.

1.4 Thesis Motivation

Security plays an important role in WNs architecture, as nodes may be deployed in enemy territory, contain private monitoring information, relay trade secrets, or possess other forms of sensitive data. So, secure communication over the insecure network needs strong authentication and conventionally developed authentication provides strong authentication using public-key cryptography only i.e. RSA, but it does not apply to the wireless environments because using such kind of security algorithm communication payload increase frequently that's not feasible for lightweight power devices. Also, there are many attacks upon wireless communication that's are not considered in the conventional authentication schemes. So, there is a need to develop such an efficient scheme that overcomes these issues using less authentication time with a small footprint.

1.5 Thesis Contribution

- The proposed scheme eliminates the need for public-key cryptography for secure communication.
- This study provides an authentication framework that is efficient, optimized, and less complex, takes less time for authentication time, and is secure for wireless network devices communication.
- Provide extending security features that minimize the wireless communication security challenges using less authentication time, power utilization, and less memory occupation.
- The scheme is implementable in all the environments where need wireless communication i.e. (Military radar system, IoT, Industry 4.0, Environmental

CHAPTER 1. INTRODUCTION

WSN, Smart cities, Cognitive Radio Networks (CRNs), Tracking and monitoring where WNs transmission link fragile makes its performance unstable).

- Results that validated the authenticity of this scheme. For that automatic verification of this protocol, the scheme should be done with the help of the protocol analyzer tool.
- Provide solid directions for those researchers who want to work in this domain.

1.6 Thesis Organization

The thesis is organized in the following manner. The literature study of the key topics relevant to this thesis is presented in Chapter 2. The research methodology used throughout the study was explained in Chapter 3. The suggested scheme and its features are explained in Chapter 4. In Chapter 5, a description of the proposed scheme testing, implementation, and final results are presented. The proposed scheme conclusion is presented in Chapter 6, along with a proposal for future work.

1.7 Summary

In this chapter introduction of the study has been presented. It provides an overview of the thesis, motivation, scope, research work primary objectives, and the thesis structure. This chapter also explains why this research is carried out with research contribution. Motivation for carrying out this research work also discusses in this chapter briefly.

This chapter also highlights the well-defined problem statement based on the issues found throughout the literature study. At the last, it described how this research document was organized. In the following chapter literature review that was done for this study will discuss.

Chapter 2

Literature Review

This chapter explores the related work and technologies in the field of authentication of network devices. Many researchers have explored the authentication field and suggested a variety of solutions to current vulnerabilities that exist in the networking devices authentication phase. The related work is simply the research done over the years by various researchers that are linked to the research done in this thesis and helped to the development of a new solution. The aim here is to present the latest research which contributes to the problem statement. Thus, authentication schemes will also be examined to demonstrate the presence of the problems.

2.1 Authentication

In computing, Authentication is the method through which the identification of the user or device is verified. In a wireless network, the authentication process allows one to secure the wireless network so that the network resources can be accessed only to legitimate network nodes and these network nodes easily perform secure communication over the insecure channels. Similarly, user authentication requires that the identity of the user is verified following which a user is provided access to the device.

2.2 Authentication Techniques

Various authentication and authorization protocols techniques are developed and implemented in network security however, they are all tied to a specific application and regarded in a standard environment. Currently, in all types of wireless networks, authentication scheme has been researched with different solutions [9]. Many strategies and schemes for serving as authentication mechanisms have been developed through the years. Because Authentication is the primary countermeasure that ensures that an authentic user has

CHAPTER 2. LITERATURE REVIEW

accessed the device or service and that an unauthorized user has been prevented from doing so [10]. Generally, authentication factors are classified into three categories (something you know, something you have, something you are). Something you know includes PINs, passwords, combinations, secret handshakes, or code words. All physical objects, such as smart cards, token devices, keys, smart phones, and USB drives are included in something you have. And something you are is a piece of information that is in you — it's a unique property that only you and no one else has it. Moreover, some security measure that belongs to something you are authentication categories is biometrics, biological means of identification i.e. voice recognition, fingerprints, and eye retina.

Authentication is one of the most difficult aspects of any information system. Because wireless networks are dynamic and have a wide range of applications so the security of the Wireless Networks (WNs) depends upon the authentication scheme used in this network. This is the reason in recent years, there has been a lot of research on the design and security analysis of authentication techniques for Wireless Networks (WNs). In most cases, analyzing the security vulnerabilities of one or more protocols leads to the development of new protocols. The following sections visit some of the most common authentications.

2.2.1 Hash-chain Based Authentication

In Computer security, a hash chain is a way to make several unique keys from a single key or password. A hash function can be used to record the chronology of the presence of data successively on additional data for non-repudiation. Leslie Lamport [11] first recommended utilizing the hash chains to provide a safe way to authenticate the device or user in the network with the help of one-time passwords when the Eve is capable to hack the communication between the network nodes. Hash is considered a simple and secure method because it's easy to compute and hard to invert.

For IoT-cloud architecture situations [12] authors provide a novel and robust authentication technique that is combined with cloud servers. For achieving maximum efficiency Lightweight crypto modules, such as the one-way hash function and exclusive OR operation, are used in this authentication scheme. By using these lightweight crypto methods their proposed scheme is best for limited power objects like IoT devices and sensors. The

CHAPTER 2. LITERATURE REVIEW

security discussion and verification analysis of this research proved that the suggested authentication technique is secure against numerous attacks while also achieving essential security aspects such as user tracking, forgery, and insider attacks mutual authentication, and session security. Drawbacks of using this scheme are that communication cost is high, computation cost at cloud is high and also in this proposed scheme, there is no consideration of DOS and DDoS attacks.

In [11] authors propose an approach for lightweight node authentication associated with cryptographically secure one-way hash chains and Elliptical Curve Cryptography (ECC) without using any digital signature algorithm or any public-key cryptography. This hash-chain-based authentication scheme protects against Man-in-the-middle attacks due to the usage of hidden generator points derived from hash-chains, malicious node injection. It also provides instant authentication. But the main disadvantage of this scheme by using Elliptic Curve Cryptography (ECC) is that it increases the size of the encrypted message significantly more than RSA encryption.

In [13] for IoT devices, authors develop a secure and mutual authentication scheme using the one-way hash function. The secret key value between the tag and the reader can be updated dynamically using this mutual authentication scheme. The evaluation findings revealed that the suggested protocol can survive against a variety of attacks, including replay attacks, Man-in-the-middle, tracing and desynchronization attacks, and eavesdropping. There is one weak point of this protocol, i.e. the Secret Value (SV) is dynamically modified in such a way that the sequence number increment is easy to estimate by an adversary.

2.2.2 Multi-factor Authentication

The issues encountered while implementing traditional authentication schemes that depend upon the concept of something possessed, something owned, or something owned by the node that needs to be authenticated has been the main reason for the growth of the multi-factor authentication protocols. [14]

To ensure lightweight device security, in [15] authors design an authentication technique that integrates many factors. This is a secure and efficient multi-factor device authentication scheme. Their authentication scheme relies on digital signatures and the

CHAPTER 2. LITERATURE REVIEW

device's unique ability to authenticate devices quickly and efficiently. Moreover, the combination of a multi-factor approach and device capacity has notably strengthened their technique's resistance to attack vectors such as Man-in-the-middle and replay attacks. However, the flaw in their authentication scheme is that they employ standard public-key encryption, which is frequently unsuitable for IoT devices due to their inability to do complicated computations efficiently.

When compared to traditional authentication procedures, multi-factor authentication provides greater security [16]. When compared to traditional authentication procedures, multi-factor authentication provides greater security. However, the incorporation of multi-factor authentication systems increases the attack surface and introduces additional attack vectors. Because multi-factor authentication solutions frequently rely on side-channel communication methods, side-channel vulnerabilities can be exploited to attack them [17]. For example, software-defined base stations have greater signal strength, authentication SMS and authentication calls easily take-off. Authentication processes that rely significantly on out-of-band channels and their integrity can be readily targeted utilizing these attack vectors [18].

2.2.3 Public and Symmetric key-based Authentication

Key-based authentication techniques are a type of technique that is based on something you know. In symmetric-key cryptography, a single key is used for both encrypting and decrypting the data that communicate between network nodes. Symmetric-key-based encryption also allows for some level of authentication. As one symmetric key encrypted information cannot be decrypted using another symmetrical key. While asymmetric encryption or public-key encryption is also used for authentication and it's overcome the symmetric key cryptography disadvantages and constraints.

Delgado-Mohatar et. al. [19] present a lightweight authentication model for wireless sensor networks (WSNs) that consists of key management and an authentication protocol. It is based on the usage of basic symmetric cryptographic primitives with very minimal processing needs, which obtains better outcomes. The main goal of this study is to provide message confidentiality and authenticity and also the proposal has a good resilience against

CHAPTER 2. LITERATURE REVIEW

node capture attacks. Specifically, it provides perfect resilience against node capture. But this is designed for static or quasi-static scenarios, in which the expected rate of new nodes and authentications is low.

In [9] for Cognitive Radio (CR) an efficient and secure authentication technique is proposed. In this study, the proposed technique is based on public and symmetric key encryption instead of employing a digital signature-based technique. To increase security in terms of accessibility, and resource availability, it encrypts data between communication nodes. The proposed scheme provides a perfect resilience against common attacks (Man-in-the-middle attack (MITM), Denial-of-Service (DoS)), and reflection attack). The drawback of using this scheme is that its deployment and integration are too complex and required high maintenance resources. Because in the proposed technique authentication procedure is carried out in multiple layers (physical, data link, network, and application).

2.2.4 Password-based Authentication

In computer networks, the most common and reliable authentication method is password-based authentication. A password-based authentication scheme offers an easy way of authenticating the network devices. Password-based authentication is simple to implement however, it is a fast-aging authentication technique. In password-based authentication protocol, the user of the network device must provide a password for each server, and the administrator must keep a record of each user's name and password, generally on different servers. To provide strength to passwords it is now commonly suggested that the password should incorporate special characters, numbers, and alphabets in both upper case and lower case. This is generally done to defeat dictionary-based attacks for password theft.

In [20] authors present a security authentication scheme in machine-to-machine or M2M home network service. In this paper, the authors construct the M2M application model for remote access to the intelligence home network service using the existing TD-SCDMA (time division - synchronous code division multiple access) networks. In this authentication protocol, a password-based authentication and key establishment protocol are designed to identify the communicating parties. This protocol can resist many attacks and owns some practical merits. But energy cost is too high when we use this scheme. Recent research [21]

CHAPTER 2. LITERATURE REVIEW

investigated many password-based authentication systems and claim that the tradition of utilizing mathematical operations that are computationally exhausting in password authentication methods might result in security flaws in the system.

It is a known fact that written and stored passwords pose a serious security concern. Hence, passwords should primarily be memorized. As, length of passwords increases, memorizing alphabets, numbers, special characters and alphanumeric data with difference combination become tedious.

Moreover, for fast authentication between nodes, short passwords are a good option because they consume fewer computing resources for authentication. But there are many drawbacks of using weak passwords. When network devices use weak passwords then guessing attacks, dictionary attacks, and brute force are easily launched by the attackers [22].

2.2.5 Digital Signature-based Authentication

A digital signature is a determined cryptographic value, based on data and a secret only known to the signatory. It is used to verify, integrity, authenticity, and non-repudiation. The digital signature ensures that the message is transmitted by the known user and has not been altered, whereas a digital certificate is used to validate the identity of the user, who might be the sender or recipient.

Parvin et al. [23], [24] have developed a scheme that is based upon the digital signature, and in this scheme for authentication process they generate the asymmetric keys with the help of RSA algorithm which is implemented on the data link and physical layers, to permit and find the authentic users existing in Cognitive Radio Networks (CRNs) for entering the spectrum. Regarding the relevance of this work in securing CRN communication, its performance reviews reveal that message transmission with a digital signature takes longer than a typical message transmission without a digital signature. Also, In the simulation, they did not take the trust value into account for integrity considerations.

Mahmud and Morogan [25] have presented an access control and user authentication scheme, which is dependent on the identity-based signature (IBS). In the proposed scheme to sign and verify a message, they used the ECC-based digital signature algorithm. Users and

CHAPTER 2. LITERATURE REVIEW

sensor nodes are both registered to the Base Station (*BS*) at the time of initialization, *BS* is responsible to provide the access rights and group identity to the users. User revocation occurs in the scheme when the user's access time assigned by the *BS* at the time of registration expires. The authenticated user is not permitted to get the requested access without the proper access rights. This authentication scheme provides strong resilience against Denial-of-service (*DoS*) and node capture attacks. But the drawbacks of using this scheme are that the password change procedure and user registration are not enabled. Moreover, for the registration of the new user, the base station needs to retransmit the parameters of the user such as the user id, the group id, and the system timestamp, which lead to more network communication overheads.

2.2.6 Biometric Authentication

Biometric-based authentication techniques are a type of technique that is based on “something you are”. Biometric authentication is a type of security that depends on an individual's unique biological traits to verify that they are who they claim to be. Typically, it is used to manage access to digital and physical resources. Everyone has unique qualities that may be used to distinguish one person from another. These characteristics and traits are broadly divided into two types of biometrics, namely behavioral and physiological. Biometric characteristics can include fingerprints, DNA, face, iris, retina, signatures, palm area, sounds, and keystroke recognition.

Rathod et al. [26] conducted a comprehensive study of fingerprint recognition systems. In their research, they discovered that fingerprints are the oldest and most widely utilized biometric recognition technique. The false rejection rate and a false acceptance rate of the biometric recognition systems, as well as flaws and security gaps of each scheme that they have analyzed, are also discussed.

Multiple biometric traits [27] can be utilized to verify a person more safely and effectively, rather than a single biometric feature. In instances when numerous biometric characteristics are used, the attacker will need to fabricate and distort all types of utilized biometric information to authenticate as a valid user. For example, it becomes difficult for an attacker to obtain a high-quality fingerprint and an image of the iris and at the same time as a

CHAPTER 2. LITERATURE REVIEW

result, the attack will be difficult to carry out. Moreover, the authors also presented a multi-biometric framework, as well as various problems such as identification of identical twins, soft multi-biometrics, multi-data database, multi-algorithm fusion methods, embedded hybrid recognition system, and indexing search, are discussed which must be kept in mind at the time of designing a multi-biometric framework.

2.2.7 Hardware Authentication

Hardware-based authentication techniques are a type of technique that is based on “something you have”. In addition to a simple password, hardware authentication is a kind of user authentication that depends on a specialized physical device (such as a token) held by an authorized user to enable access to computer resources. For authentication, items such as smart cards[28], USB token keys [29], and RFID tags [30] can be used.

A smart card is a microcontroller that is used for storing, generating, and operating on encryption keys. Smart card authentication provides users with smart card gadgets for authentication. Users link their smart card to a computer that serves as a host. To authenticate the user, software on the host computer interacts with the keys material and other secrets contained on the smart card.

Token-based authentication is a technique that allows users to prove their identity and obtain a unique access token in exchange. Users may then access the website or app for which the token was granted during the token's lifetime, instead of just having to re-enter details each time they visit the same webpage, app, or other resource protected by the token.

Radio-frequency identification (RFID) uses radio waves to transmit a unique identifier between the tags placed in the RFID card and the RFID reader, allowing a user's identity to be verified and access granted. Moreover, Tags and card readers are both included in an RFID-based access control solution. Tags are inserted on plastic cards or tokens and include a unique identity. The transmitter on the RFID reader continually releases a short-range radio frequency field.

To achieve hardware authentication physical device attributes such as PUF [31] can be used. PUFs are created based on the equipment's characteristics. It's difficult to duplicate

CHAPTER 2. LITERATURE REVIEW

these characteristics. These features rely on many factors like materials, inherent characteristics introduced by fabrication, and environmental noise. Although this is still an active area of study, much has been done for the standardization of hardware-based authentication.

2.3 Summary

This chapter covers the related work and background of the study. Research related literature with critical analysis has been presented in this chapter. First of all, the Authentication technique is explained, and after that related techniques are discussed. Many researchers have explored the authentication field in computer networks and suggested a variety of solutions to current vulnerabilities that exist in this domain. In their studies, researchers tried to figure out the problems and proposed different solutions. Previous studies and techniques used in the literature help to formulate the solution for the identified problem.

In the next chapter, we will present the research methodology that has been followed during the completion of the thesis.

Chapter 3

Research Methodology

Chapter 3 describes the method of research that is used to carry out this thesis work. After a complete analysis of current research methodologies, a hybrid approach is chosen for the presented thesis. Because each research method is appropriate for the various research scenarios in this thesis. As a result, all of these research methodologies are used at various times. A summary of the methods utilized in our research, as well as the stages of the research processes i.e. identifying the research problem, develop a hypothesis, making important observations, and evaluating the authentication scheme, scheme design, and implementation are presented in this chapter.

3.1 Introduction

Research is a systematic inquiry process that involves data gathering, documenting essential information, and analysis and interpretation of that data/information under appropriate techniques established by certain professional sectors and academic fields. It may be defined as a scientific exploration to find new information and facts [32]. Whenever an issue has to be answered and a solution found, research is conducted [33]. According to Clifford Woody [34], the process of defining and redefining an existing problem, generating hypotheses and proposing solutions to the known problems, analyzing the collected data and making assumptions, constructing a conclusion, and finally testing the results for the verification of the hypothesis, is referred to as research.

3.2 Research Types

In the literature, different research methodologies were proposed. These research methodologies are given below and illustrated in figure 3.1.

Research Types			
Qualitative vs Quantitative	Descriptive vs Analytical	Fundamental vs Applied	Conceptual vs Empirical

Figure 1 Research Types

3.2.1 Qualitative vs Quantitative

Quantitative research is focused on the quantitative estimation of some features. It is possible to do so in fields where objects may be expressed in terms of quantity. It is non-descriptive numerical, applies statistics and mathematics, and uses numbers. In this research method tables and graphs are frequently used to display the results. It checks the what, who, when, and where of decision-making. While in qualitative research methods, items are evaluated based on their quality, such as human behavior or thoughts on specific topics, as well as the reason behind those opinions. It is descriptive, non-numerical, and reasoning-based and employs words. It is exploratory and cannot be graphed in nature. Moreover, It focuses on the how and why of decision-making [32].

3.2.2 Descriptive vs Analytical

The current work is discovered in the descriptive study, and short reviews are done to find the vital and related information and evidence. The goal of the descriptive method is to define the work in a certain field of study that may then be used in future research. The fundamental

CHAPTER 3. RESEARCH METHODOLOGY

characteristics of this research are that the analyst has no discretion over the data and existing literature; instead, they can only find evidence and techniques. While in analytical research, the researcher takes all of the material gathered from the assessments and performs critical analysis and evaluation to come up with a conclusion [32], [33].

3.2.3 Fundamental vs Applied

Depending upon the depth of knowledge the research can either be applied or fundamental. Fundamental study leads to a new hypothesis, a new attribute of matter, or even the discovery of a new substance that was previously unknown or unreported. The major goal of this research is to gather basic information and discover the fundamentals of scientific phenomena. While in applied research, accepted or well-known theories and concepts are used to tackle specific issues. The majority of experimental research, case studies, and cross-disciplinary research are applied research. In this research, method researcher tries to find out the appropriate solution to the problem that other researchers, society, or organizations are facing. In Applied research, the researcher conducts several experiments to study and evaluate the problem and gain a depth understanding of the problem area. Moreover, solving the problems practically this method is very helpful and mostly carried out for solving practical problems [32], [33].

3.2.4 Conceptual vs Empirical

Conceptual research is founded on abstract concepts or the ideas commonly employed by theorists. Normally conceptual research is done to generate new ideas or redesign existing ones. As compared to conceptual, empirical research is based solely on observations and experiments, with no dependence on any scheme or idea. This research method is based entirely on their observations, experiments, and conclusions. In the empirical study, first, a hypothesis is formed based on the data, and then the outcomes are assumed. The researcher next gathers evidence to support or refute the theory [32].

3.3 Research Methods and Research Methodology Overview

For researcher purposes, different methods, techniques, and procedures are followed by the researcher that is known as a research methodology. The research method is a process that

CHAPTER 3. RESEARCH METHODOLOGY

begins with conducting the reviews and continues until the findings are obtained. The principles and procedures for doing research using a scientific approach are defined as the research methodology. It contains all of the steps utilized by the researcher to solve the specific problem. For different types of research problems research methodology is different, and the researcher must be aware of the related research methodology for carrying out the research. The researcher's study aim should be extremely clear when it comes to selecting a research methodology [32], [33]. Following research methodology steps are used in this thesis:

- Explore the computer networks, wireless networks, security of networks, authentication and importance of authentication in any kind of computer networks, network protocols and network protocols for secure authentication, authentication layer security, attacks, and challenges to gather information for the targeted domain (authentication).
- Narrow down the study to focus on a few key issues and attacks and provide strong resilience against these attacks i.e. Replay attack, Man-in-the-middle, false data injection attack (FDIA), fake node additions, etc. These are the common attacks at the authentication layer.
- Construct a hypothesis based on a review of the literature.
- Design the optimized and secure authentication scheme for network devices using the developed hypothesis.
- Finally, validate the proposed hypothesis after the implementation of the proposed scheme.

3.4 Thesis Research Methodology

Throughout the study, this thesis employed a hybrid strategy, which includes conceptual, fundamental, and applied methods. This thesis consists of some steps that are followed throughout the research phases beginning with the collection of information and ending with the evaluation of the results. All of the steps in our study procedure are outlined here.

- Find out the research area
- Define the topic
- Literature survey

CHAPTER 3. RESEARCH METHODOLOGY

- Determine the research problem
- Develop hypothesis
- Observations
- Prototype design and implementation
- Hypothesis validation and testing
- Results and conclusion

3.5 Proposed Scheme Development Strategies

Generally, after studying the target areas for thesis or research the next step is to find out the research problems in that areas. When a researcher develops any kind of hypothesis in security for the validity of this hypothesis the researcher needs to implement it and shows the results for others. If they fail to generate the results then their hypothesis failed and is no more accepted. So, formal outputs or results are very important in information security (IS).

I follow the same approach firstly I study the literature and then determine the research problems. In my case for overcoming these problems, it's required to develop an authentication scheme that is optimized and secure. This study verifies that these kinds of problems currently exist in wirelessly connected devices. Moreover, in the end, the results of the scheme proof the correctness of this scheme and study.

3.5.1 Overview of the Scheme Development Tool Scyther

The tool that is used for the simulation of the scheme is the Scyther [35]. Scyther is a tool for formalizing security protocols based on the perfect cryptography assumption, which holds that all cryptographic functions are flawless: unless the adversary or Eve knows the decryption key, the adversary learns nothing from an encrypted message. The tool can be used to identify issues that arise as a result of the protocol's design. In general, this problem is unsolvable, but in practice, many protocols can be proven correct or attack discovered [36]. In [37] author describes the basic security properties, entire protocol model, including its assumptions and algorithm.

In information security, there are many benefits of using simulations technologies as a safe way to check any kind of scheme or protocols when you do not have access to

CHAPTER 3. RESEARCH METHODOLOGY

specialized hardware i.e. network devices, servers, and communication infrastructures. By using a security simulator, we can validate the correctness of the scheme which is otherwise not possible until we have real hardware devices operating systems, and applications software.

Using simulators, we easily test and implement our desired schemes, easily change security requirements without any hardware cost. Simulation is also the best option in the case of critical infrastructure where any kind of failure leads to problems. So, in such cases firstly we perform test cases upon the simulator and then in real-life environments.

3.5.2 Scheme Development Language

As earlier discussed, the tool used for the implementation is the Scyther. Scyther has built-in language for writing protocols, sending and receiving messages, roles, and types of parameters, and so on. The input language of Scyther for writing the protocol scripts is loosely based on a syntax like C/Java [36]. The language's main purpose is to describe protocols, which are formulated based on roles. Roles are defined by a series of events, the majority of which involve the sending or receiving of terms. For verification of protocols upon Scyther, the protocol must be written in the Scyther input language. The protocol description code can be written directly into the Scyther built-in editor or can be into any text editor i.e. notepad, notepad++. The most important thing for writing the protocol description code is that the input file must be saved with .spdl (Security Protocol Description Language). By convention, input files have the extension. spdl, but it can have any name.

3.5.3 Why Scyther Tool is selected?

When it comes to verifying the security of protocols, there are two basic techniques: Formal methods and provable security. Scyther is a formal verification tool that is developed to verify security protocols automatically. Scyther adversary model is predefined which is based upon the Dolev-Yao intruder model [38]. This technique has simplified the formalization of security protocols and makes it simpler for new users to begin working with Scyther. In comparison to other formal verification tools, such as SPIN [39] (language Promela), the Scyther specification language is simple and easy to understand. Scyther also exceeded other state-of-the-art tools, such as the ProVerif tool [40]. Scyther may also give classes of protocol behavior, whereas other tools just provide specific attack traces. Scyther has previously been

CHAPTER 3. RESEARCH METHODOLOGY

used to test many protocols, including authentication protocols (e.g., IKEv1, IKEv2 protocol suites, and the ISO/IEC 9798 [35] family). Also, Scyther is popular and commonly used due to ease of installation. Scyther is available for the Linux, Mac OS, and Windows platforms [36].

3.6 Summary

In this chapter, we have discussed various research methodologies that have been suggested for research and that researchers can use according to the nature of the problem. As every research method is suitable for research scenarios of this thesis, hence at different times, all these research methods are followed.

The tool that I used for the implementation of the scheme is the Scyther. This is a tool to analyze security protocols, security needs, and potential vulnerabilities formally and also provide specification language for describing the security protocols. And the proposed solution to the problem that has been identified in the previous chapters will be discussed in the next chapter.

Chapter 4

Proposed Solution

Chapter 4 explains the proposed scheme framework that has been designed to solve the problem statement and also mitigate different attack vectors. This chapter also goes over the primitives that are included in the framework and these are necessary for the understanding of how the framework works. Security features of the proposed framework are also detailed in this chapter.

4.1 Scheme Primitives

One by one, the primitives utilized in the proposed system are explained below. Understanding the proposed approach requires knowledge of these primitives. Because these primitives are the fundamentals building blocks of the proposed scheme. So, if anyone who wants to learn about the proposed scheme working these primitives helps to him.

4.1.1 Timestamps

A timestamp [41] is a packet or token of information used to ensure timeliness; it comprises timestamped data, including signature, and a time produced by a Trusted Timestamp Authority (TTA). A timestamp is the current time of an occurrence that a system has recorded. Timestamps are useful for keeping track of when data is shared, generated, or destroyed over the internet. In many situations, these records are just useful for us to know about. But in some conditions, the value of a timestamp is higher. There are many usages of the timestamp in security. To prevent replay attacks, a timestamp is utilized. A timestamp, for example, is employed in Kerberos to avoid replay attacks. The timestamp method is also helpful for a wide range of synchronization purposes. The proposed scheme makes use of timestamps for achieving similar objectives

4.1.2 Hash Functions

A hash function [42] converts a variable-length message into a fixed-length hash value. Inverting the algorithm or finding two messages with the same hash value (a collision) should be challenging. One of the first applications of hash functions was to generate fixed-size, compact, collision-resistant message digests (MDs) which may be used in place of huge variable-length messages in digital signature systems or schemes. Later, similar functions began to be utilized frequently in various applications, such as message authentication codes, randomly generated bit creation, and secret key derivation.

A hash, often known as a message digest, is a tiny fixed-length representation of a huge message. Hashes are also referred to as one-way functions since the original message cannot be retrieved from a digest. Hashes are used to guarantee the information's integrity and validity [43]. The hash changes substantially even a little in the original message owing to the avalanche effect. Hashes are not used to ensure confidentiality. There are several hashing algorithms, such as SHA1, SHA2, and SHA3, and MD4, MD5, that take arbitrary length input and produce fixed-length output. The proposed scheme makes use of hashes for achieving similar kinds of objectives.

4.1.3 Symmetric Cryptography

Symmetric key cryptography encrypts and decrypts the text using the same key [44]. This implies that to decrypt data; one must have the same key used to encrypt it. As a result, it's often referred to as the same key, shared key or single key. It's also known as private or secret key encryption since the key is kept confidential. Symmetric cryptography algorithms are cost-effective, simple, and are fast in terms of efficiency. The disadvantages of shared keys include key exchange, the usage of too many keys, and the inability to verify that messages came from a user because both sender and recipient share the same key. When utilizing a symmetric key, the key's exposure is undetectable. For making the algorithm and protocols efficient symmetric keys play a vital role in information security [45]. The purpose of using a symmetric key in the proposed is also to make the scheme optimized.

4.1.4 Random Numbers

A random number is a value that changes over time and has a minimal likelihood of repeating. For example, a random value that is produced a new for each use, a sequence number, a timestamp, or some combination of these [41]. Random numbers are used in cryptography to produce cryptographic keys, as well as a nonce (to verify timestamp), salts (which are used as arbitrary inputs in hash functions), and onetime pads. To obscure predictable patterns, random numbers are also used. They're also utilized to increase the duration of pad messages to remove human biases.

4.2 Scheme Features

The proposed scheme provides the following functionalities.

- The proposed authentication scheme is secure and optimized as compared to existing authentication protocols for network devices. Because most of the protocols studied in the literature provide authentication security features maximum based upon the public key cryptography.
- Strong authentication and continuous authentication.
- The proposed authentication scheme proved mutual and continues authentication to network devise until communication is performed securely over the insecure network.
- The scheme is optimized/ efficient in terms of computational processing.
- The scheme will provide strong protection against common attacks (Man-in-the-middle, replay attack, false node injection, and false data detection).
- Implementable upon all the environments where need Wireless communication i.e. (Military radar system, IoT, Industry 4.0, Environmental WSN, Smart cities, Cognitive Radio Networks (CRNs), Tracking and monitoring where WNs transmission link fragile makes its performance unstable).
- Eliminating the need for Public-key cryptography for secure communication.
- Extending security features and minimizing the wireless communication security challenges.
- Easily implementable and always welcome to change.

CHAPTER 4. PROPOSED SOLUTION

- There is no need to change network infrastructures when required to add new nodes in the networks.

4.3 The Proposed Approach

Our secure and efficient authentication scheme is explained in this section. It is based upon symmetric key cryptography and hashing. For completing the authentication process, minimizes the crypto primitives and packet payload.

Figure 2 illustrates our system model. Following are the four major components in our model depicted in figure 2.

1. Base station (*BS*)
2. Authentication server (*AS*)
3. Token Server (*TS*)
4. Network Node (*NN*)

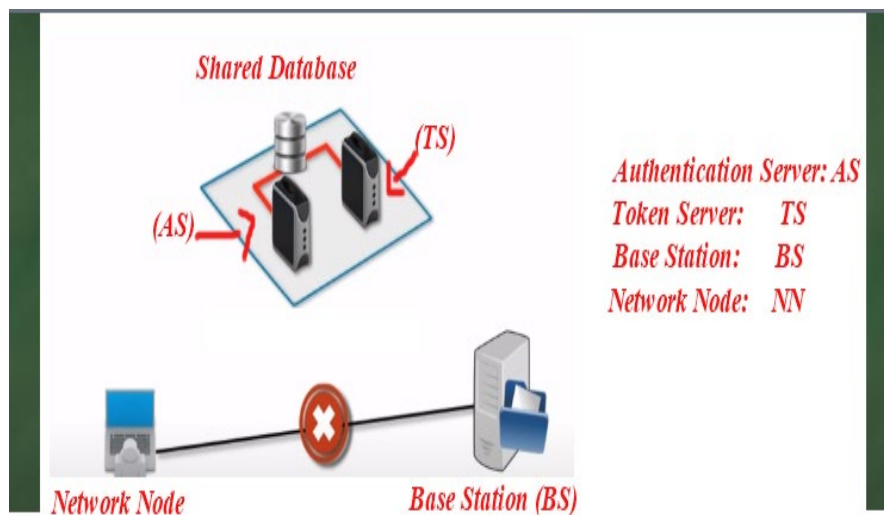


Figure 2 System Model

In this network Base Station (*BS*) is responsible for controlling and taking action after receiving the secrets data from the network nodes. A network node is any network device (sensor, IoT device, cognitive radio network, industry 4.0 device), etc. that is the part of the

CHAPTER 4. PROPOSED SOLUTION

network and responsible for sensing the data from the critical environment and send it to the base station for further actions. These network devices are deployed in different geographical locations at one time and then remotely work through a wireless network. Because there is no physical connection between the nodes and base station, therefore, a lot of attacks i.e. (man-in-the-middle, replay attack, false data injection attack, fake node injection) are possible when nodes send secret data to the base station. For mitigation of these attacks' nodes must be authenticated before becoming part of a network and performing other activities.

In figure 2 it's clearly shown no network node directly communicated to the base station. For that, it must be authenticated and got permission through servers (Authentication server, Token server). Authentication Server (*AS*) is responsible for authenticating the interested nodes and make sure these devices are trusted and become part of the network through the network administrator priorly. Token Server (*TS*) works as a second layer of security and provides continuous authentication. First, it verifies that the node is already authenticated from the Authentication Sever (*AS*) after that it checks device is live and wants to communicate with the base station. If it verifies then Token Sever (*TS*) grants the communication token for a limited time to the node so that it can perform the communication with the base station. Second, Token Server (*TS*) also helps the Base Station (*BS*) to verify the granted token when the node puts a request for communication to the Base Station (*BS*).

There are two main phases of the proposed scheme A. Preface 2. Scheme description. These two phases are discussed here.

4.3.1 Preface

There are 4 major components in the proposed scheme. The first one is Base Station (*BS*), two servers (*AS* & *TS*), and network end nodes (more precisely monitoring sensor, IoT device, industry 4.0 device), etc. This phase is assumed or carried out before the deployment of the wireless network physically, more precisely during the node's manufacturing time. At the manufacturing phase lets, we assume the manufacturer of the nodes assigns or preloads a unique id i.e. $N_1, N_2, N_3, \dots, N_f$. And also preload a secret key in every nodes buffer. Let us assume between the Authentication Server (*AS*) and Token Server (*TS*) a secret key is already shared successfully. And assume a database is created according to the requirements and

CHAPTER 4. PROPOSED SOLUTION

shared between both servers (*AS* & *TS*). This database is secured at any point. Let us assume between the Token Server (*TS*) and Base Station (*BS*) a secret key is also shared successfully. Figure 3 illustrates the scheme secret key set.

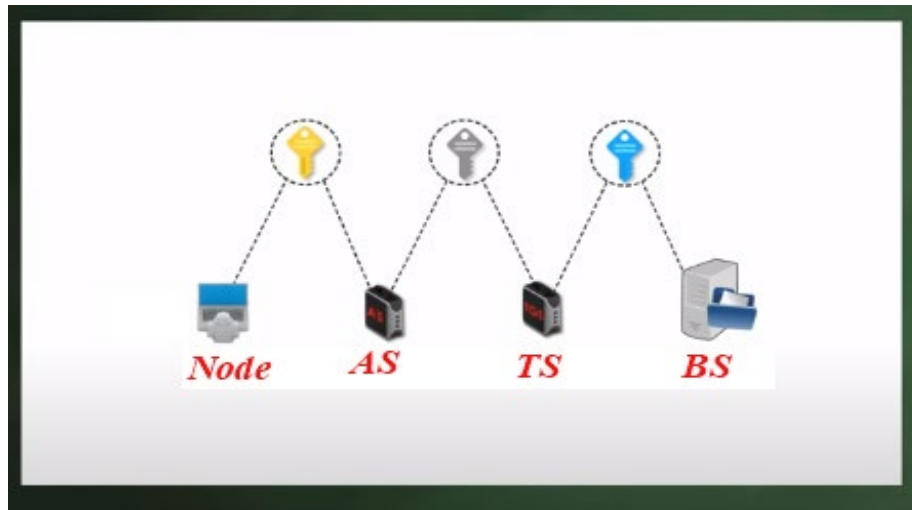


Figure 3 Scheme Key Set

Whenever new networks are deployed or need to add new nodes into the network or are required to add new devices in the already build network then for each node network administrator assigns the unique key or password manually and then add the node id and hash of their key ($H(nK)$) in the network database. And also, node's keys or passwords and ids are loaded to the BS buffer or BS database. After that this initiation or assumption phase is completed after the main phase of scheme description started.

4.3.2 Scheme Description

In this section proposed scheme will be described in detail with all parameters.

4.3.2.1 Proposed Scheme Sequence Diagram

Figure 4 (the sequence diagram of the proposed scheme) illustrates the working of the proposed scheme description phase.

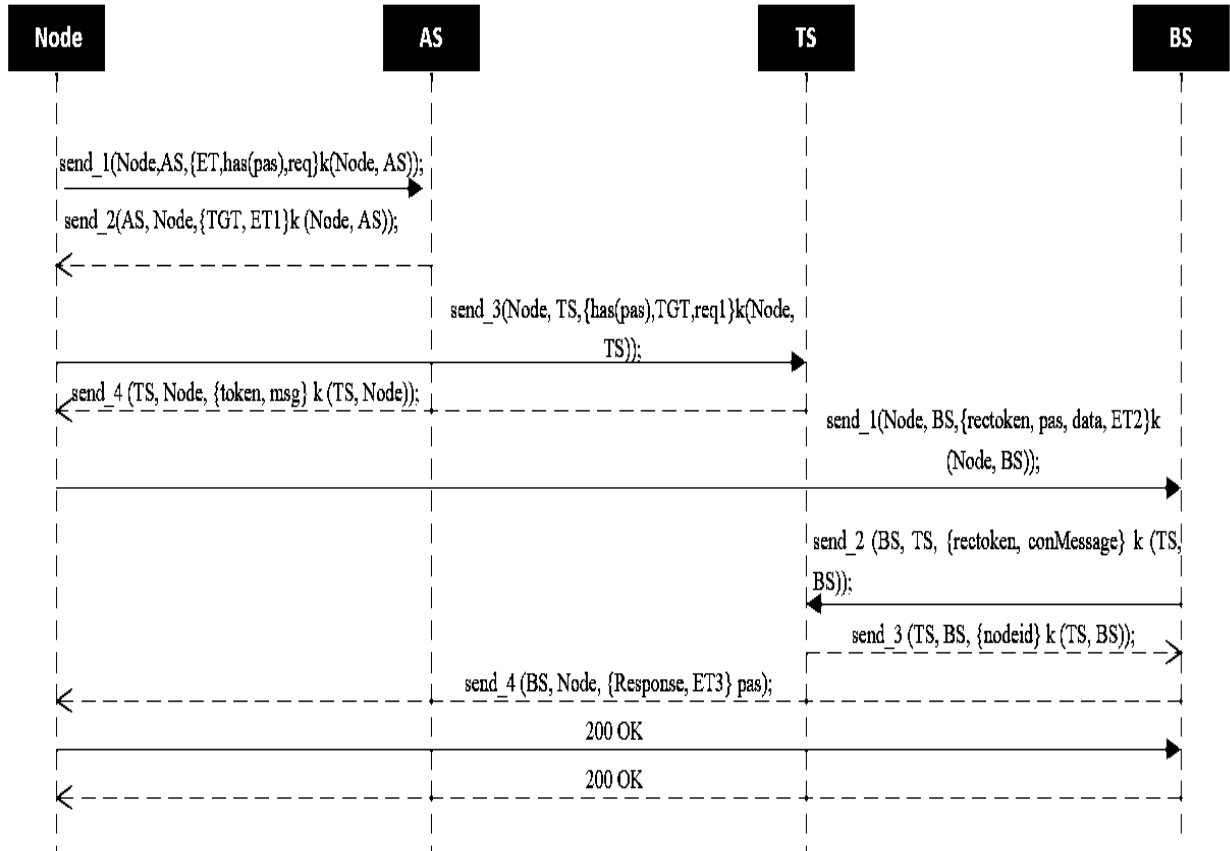


Figure 4 The Sequence Diagram of the Proposed Scheme.

4.3.2.2 Proposed Scheme Important Terms

The following are the related terms that will be utilized in the proposed scheme. Before explanation of each step of the proposed scheme, it's necessary to explain these first.

- $K ()$: represents the secret key between two components.
- $Send_X ()$: it is used to send the message from one entity to another. X means 1, 2, 3...n
- pas : the password
- $has()$: used for taking a hash of some value.
- $has (pas)$: the hash value of a password.
- TGT : Ticket granting ticket.
- $ET, ET1, \text{ and } ET2$: used tickets.
- $req1$: request

CHAPTER 4. PROPOSED SOLUTION

- msg: represents communication messages.
- rectoken: represents the received token.
- nodeid: used for the representation of the id of the network node.

4.3.2.3 Proposed Scheme Details

Scheme description is the main phase of the proposed scheme. It is carried out every time (when a new node requests to join the network or when new networks are deployed from start) once the previous phase has been finalized. When any node wants to communicate (sensing data from the environment) with the base station then it must be authenticated in the following way.

Step 1. The node sends the request to the Authentication Server (*AS*) in encrypted format for the ticket.

```
Node → AS: send_1 (Node, AS, {ET, has (pas), req} k (Node, AS));
```

Authentication Server (*AS*) receive this packet in the following way at their own end.

```
recv_1 (Node, AS, {ET, has (pas), req} k (Node, AS));
```

Step 2. When *AS* receives a node request it authenticates the node by matching the received hash value with the stored database hash. Because node id is already stored in the database against the hash. So, *AS* decrypted the timestamp with the help of this stored id (the purpose of this is to overcome the replay attack). After verification of the authentic node request that receives. *AS* sends a TGT which is encrypted with another secret key back to the sender with an encrypted timestamp (the purpose of this is to overcome the replay attack). And also make entry into the database column for *TS*.

```
AS → Node: send_2 (AS, Node, {TGT, ET1} k (Node, AS));
```

Node received this packet from the *AS* in the following way at their own end:

```
recv_2 (AS, Node, {TGT, ET1} k (Node, AS));
```

Step 3. After receiving encrypted TGT, Node sends it to the Token Server (*TS*) with requests that want communication with the Base station (*BS*).

CHAPTER 4. PROPOSED SOLUTION

Node \rightarrow TS: send_3 (Node, TS, {has (pas), TGT, req1} k (Node, TS));

Token server (TS) received this request payload like that:

recv_3 (Node, TS, {has (pas), TGT, req1} k (Node, TS));

Step 4. When the TS gets the encrypted ticket, it decrypts the ticket with a secret key shared with the Authentication Server (AS) (already shared). And also match the hash from the database against this ticket (this entry is done in step No 2) either its authentic node or not. If there is no problem then its issues the client token (for a certain period and date) which is encrypted with another secrete key for communication with Base Station (BS). And also make an entry of this token into another column of the database against node id.

TS \rightarrow Node: send_4 (TS, Node, {token, msg} k (TS, Node));

Requesting node received this packet from Token server (TS) in the following way:

recv_4 (TS, Node, {token, msg} k (TS, Node));

Step 5. After receiving an encrypted token (the purpose of the encrypted token is to overcome the MITM) from the TS client able to communicate with BS with the help of this token for a certain period. With the token, it's also sent encrypted data to BS using their password.

Node \rightarrow BS: send_1 (Node, BS, {rectoken, pas, data, ET2} k (Node, BS));

Base station received this request from the node like that:

recv_1 (Node, BS, {rectoken, pas, data, ET2} k (Node, BS));

Step 6. When the Base Station (BS) receives the token firstly it decrypts the token with the help of a shared secret key between the BS and TS for token validity. And for checking whether the sending node is actually the owner of the token or not. BS confirms from the TS. After that, it decrypts the second part of the packet with the help of the node password (BS has all nodes passwords because in the first phase all passwords are loaded into BS memory).

BS \rightarrow TS: send_2 (BS, TS, {rectoken, conMessage} k (TS, BS));

CHAPTER 4. PROPOSED SOLUTION

Token server (Server) received this payload from the BS like that:

```
recv_2 (BS, TS, {rectoken, conMessage} k (TS, BS));
```

Step 7. When TGS receives the same token from *BS*. It checks from the database previously it sends to which device. After matching its share, the id of this node to *BS* in an encrypted format (this id is encrypted with a shared secret of *BS* and *TS*).

```
TS→ BS: send_3 (TS, BS, {nodeid} k (TS, BS));
```

Base station (*BS*) get this response from the *TS* like that:

```
recv_3 (TS, BS, {nodeid} k (TS, BS));
```

Step 8. When the *BS* receives the response from the *TS* and decrypts the message and got the id. After that *BS* found the node password against the id from their buffer for decrypting the message that it's received from the node in step 5. And send to the response with that node password.

```
BS→ Node: send_4 (BS, Node, {Response, ET3} pas);
```

Node get requested response from the *BS* like that:

```
recv_4 (BS, Node, {Response, ET3} pas);
```

Step 9. Node decrypts the response from their own password. After that from a certain period (up to token validity) node communicates with *BS* by repeating steps 5, 6, 7, and 8.

```
Node→ BS: 200 OK, BS→ Node: 200 OK.
```

4.4 Table of Notations

The important notations used throughout the framework are explained in Table 1. These notations are widely used in the presented schemes.

Table 1 Table of Notations

Symbol	Notation
AS	Authentication Server
TS	Token Server
BS	Base Station
NN	Network Node
send _X (a,b)	Message send function between a and b, X= 1, 2, 3 n
Recv _X (a,b)	Receive function between a and b, X= 1, 2, 3, ... n
K (a, b)	Shared or Symmetric key between a and b
pas	Password
ET, ET1, ET2	Encrypted tickets
msg	message
req1	request
TGT	Ticket granting ticket
has ()	Hash function
rectoken	Received token
nodeid	Network node id

4.5 Summary

In this chapter, the proposed solution for the identified problem statement is described. For solving the problem statement an efficient and secure authentication scheme is proposed that is implementable in all the environments where need wireless communication i.e. (Military radar system, IoT, Industry 4.0, Environmental WSN, Smart cities, Cognitive Radio Networks (CRNs), Tracking and monitoring where WNs transmission link fragile makes its performance unstable). This authentication scheme is secure and optimized as compared to existing authentication protocols for network devices.

The important terms and sequence diagrams that are used in the proposed solution are explained for a better understanding of the proposed scheme. This would help to understand the flow of the proposed scheme. The notations used in the proposed schemes are also presented here. These notations are frequently used in the solution.

The different steps of the proposed solution are also explained in detail. Proposed scheme-related symbols and notations are explained at the last of a chapter. The implementation and test results of the proposed framework will be discussed in the next chapter.

Chapter 5

Implementation and Results

Technical details and implementations of the proposed solution are discussed in chapter 5. In this chapter, we also discuss the results that we obtained from the testing environments. Analysis of the proposed scheme and its terms, events, and claims, security properties, and their attributes are also presented in this chapter. At the last of the chapter, we also explain a hypothetical case study that helps in understanding the system and its security features.

5.1 Scheme Analysis

A network protocol analyzing tool is used to examine the proposed scheme known as Scyther [35]. The tool operates by running a script that adheres to a set of rules. Scyther is a tool that checks a cryptographic protocol for several types of attacks including, secrecy, aliveness, replay, man-in-the-middle attack, etc. To validate the system's security, a Network Threat Model [46] is used to verify the proposed, scheme. The following is assumed:

- The attacker has completed or partial control over the network.
- The attacker is resourceful, as detailed in the Dolev-Yao intruder model [47], and can learn, deflect and generate messages.

5.2 Scheme Attributes

In this section, we presented all the important attributes of the proposed scheme with details. Using these attributes final results are generated at the end.

5.2.1 A minimal input file

Protocol definitions are the most important parts of a Scyther input file [36]. Following is the simple example code for how to define a protocol in Scyther.

CHAPTER 5. IMPLEMENTATION AND RESULTS

```
protocol ExampleProtocol (I, R) {  
  role I {};  
  role R {};  
};
```

We have defined a protocol named "ExampleProtocol" with two roles, "I" and "R," by naming them after the protocol name in brackets. Note that we haven't yet defined the behavior of these roles. Within the curly brackets, their behaviors are defined when we need to use these roles later in the protocol implementation.

```
protocol secure (Node, AS, TS)  
{  
  role Node {};  
  role AS {};  
  role TS {};  
}  
Protocol secure2 (Node, BS, TS)  
{  
  role Node {};  
  role BS {};  
  role TS {};  
}
```

The above code is the definition of the protocol of the proposed scheme. Because the proposed scheme consists of four components that's why here in the input files four roles are created i.e. Node, AS, TS and BS.

5.2.2 Terms

Scyther manipulates terms [36] at the most fundamental level. Many terms are used for completing the definition of protocols in Scyther but here we just present only those terms that are related to the proposed solution.

5.2.2.1 Atomic Terms

Any identifier, which is generally a string of alphanumeric characters, can be used as an atomic term. Operators like pairing and encryption can combine atomic phrases into more complicated terms. Following are the most important terms.

a. Constants (Freshly generated values)

Most security protocols depend on creating random values. They are frequently used by generating them within the role body with the help of fresh declaration. For example, to declare a random value NA of type Nonce we write the constants script like that:

```
role X (...) {  
  fresh NA: Nonce;  
  send_1 (x, y, NA);  
}
```

b. Variables

Variables are used to store received terms. The below variable script illustrates how to receive a nonce into the variable with the name NA that we use in the constants script.

```
role Y (...) {  
  var NA: Nonce;  
  rec_1(X, Y, NA)  
}
```

5.2.3 Symmetric keys

For symmetric encryption [36] any term can be used as a key. A symmetric-key or shared key infrastructure is predefined and looks like: $k(\text{Alice}, \text{Bob})$ denotes the long-term symmetric key shared between Alice and Bob.

In the following script one proposed scheme Scyther script where the symmetric key used for encryption is shown.

```
send_1 (Node, AS, {ET, has (pas), req} k (Node, AS));
```

5.2.4 Hash function

Hash functions are simply encryptions with a function whose inverse is unknown to anybody. In Scyther protocol specification language hash function can declare globally with the help of the keyword hash function. E.g. hash function H1;

Because all agents and protocols should need to access such functions that's why the declaration of these functions is usually global in scope. i.e. declaration outside of any protocol. After declaring we can use a hash function like that: H (pass). In the following one proposed scheme Scyther script where a hash function is used for encryption is shown.

```
recv_1 (Node, AS, {ET, has (pas), req} k (Node, AS));
```

5.2.5 Events

In this section, we explain those events that are used in the proposed scheme solution.

5.2.5.1 Received and Send Events

Communication can be performed between two or more roles or parties using the two functions. i.e. send and recv. Send function is used for sending the message and recv function can be used for receiving the function. In the vast majority of situations, each sends or transmit event will be followed by a similar recv event. Because the script is designed in such a way that when a send function is run, an agreeing function should be called at the receiving end.

The following message send and received script illustrates how communication is performed between two roles using the send and recv events.

```
send_1 (Node, AS, {ET, has (pas), req} k (Node, AS));
```

```
recv_1(Node, AS, {ET, has(pas), req} k (Node, AS));  
send_2(AS, Node, {TGT, ET1} k (Node, AS));  
recv_2(AS, Node, {TGT, ET1} k (Node, AS));
```

5.3 Security Properties

When validating a protocol, Scythe's characteristics such as claim events, synchronization, secrecy aliveness, and protection against man-in-the-middle are taken into account. In this section all these security properties that used to check the validity of security protocols.

5.3.1 Security Claims

A series of claim events are generally followed by a sequence of occurrences inside a role. Claim events are used to describe a role's security features, such as whether a specific value should be deemed secret or that certain properties hold for authentication [48]. And in role specifications, such claim events are used to simulate specified security features.

For example, the following claim event script illustrates that the claim event model that ET1 is meant to be secret.

```
claim (Node, Secret, ET1);
```

There are several predefined claim types [37]. These are explained below.

5.3.1.1 Secrecy

The first and most basic security claim is Secrecy. Secrecy states that the specified attribute is to be kept secret from the adversary, even if the attacker controls the communication network. However, if one of the agents is penetrated by the adversary and the protocol is carried out between an authentic agent and the attacker, it will eventually learn what was supposed to be hidden from it [49]. If there is no kind of encryption used between the communication parties then such claims fail obviously.

As shown in final results figures [11-13] Tickets, tokens, passwords, messages, and rectoken that were utilized in the exchange stayed undisclosed. Hence proposed scheme fully

CHAPTER 5. IMPLEMENTATION AND RESULTS

satisfied this claim. So, the first assurance offered by the proposed system is that user credentials are kept confidential.

Following are the proposed scheme scripts that represent all the secrecy claims of the proposed scheme.

```
claim (Node, Secret, TGT);
claim (Node, Secret, ET1);
claim (Node, Secret, Response);
claim (Node, Secret, ET3);
claim (Node, Secret, ET2);
claim (Node, Secret, rectoken);
claim (Node, Secret, pas);
claim (Node, Secret, data);
claim (AS, Secret, req);
claim (AS, Secret, ET);
claim (AS, Secret, has(pas));
claim (AS, Secret, ET1);
claim (AS, Secret, TGT);
claim (TS, Secret, req1);
claim (TS, Secret, TGT);
claim (TS, Secret, token);
claim (TS, Secret, msg);
claim (TS, Secret, has(pas));
claim (TS, Secret, rectoken);
claim (TS, Secret, conMessage);
claim (BS, Secret, rectoken);
claim (BS, Secret, pas);
claim (BS, Secret, data);
claim (BS, Secret, Response);
claim (BS, Secret, ET2);
```

5.3.1.2 *Aliveness*

The second assurance offered by the proposed scheme is the property of aliveness. Aliveness as defined by [50] (of all roles). The life attribute ensures that the reply from the receiving party is the consequence of the request made by the communication initiation party. It also ensures that communication between both parties does not tamper and that communications are digitally signed and are accurately timestamped.

Figure13 shows the Scyther script for the Aliveness property. Following are the proposed scheme scripts that represent all the aliveness claims of the proposed scheme.

```
Claim (Node, Alive);
```

```
Claim (TS, Alive);
```

```
Claim (BS, Alive);
```

Final Figures [11-13] illustrate that all communication parties in the proposed fully hold this property.

5.3.1.3 *Weak Agreement*

The third guarantee offered by the proposed scheme is the property of weakagree. The authentication form introduced as aliveness is strengthened by weak agreement [48]. We assert that the protocol operates under the weak agreement if the sender (U) completes a run with the intended responder (V), and responder (V) believes it has previously run the protocol with the same sender (U). Such a claim would prohibit an adversary from acting as a responder by performing a man-in-the-middle attack by running another run of the protocol in parallel with a run with U.

Some famous protocols such as Needham-Schroeder failed on this claim. Following are the proposed scheme scripts that represent all the weak agreement claims of the proposed scheme.

```
claim (Node, Weakagree);
```

```
claim (TS, Weakagree);
```

CHAPTER 5. IMPLEMENTATION AND RESULTS

`claim (BS, Weakagree);`

Figures [11-13] illustrate that there is no attack against Weakagree.

5.3.1.4 Non-injective Agreement

Another guarantee offered by the scheme is the Niagree. Results show that there is no attack against this claim in the proposed scheme. The non-injective agreement specifies which of the two roles or communicating parties behaved as initiator and responder when the authentication is given by weak agreement. It ensures that if the initiator (U) finishes a protocol run, presumably with the responder (V), then V has finished a run with U, in which he acted as a responder.

The non-injective agreement also guarantees that if the sender (U) also transmits a set of variables to the receiver (V) in the finished run, they will both agree that the exchanged data values correlate to all of the variables in the set.

Following are the proposed scheme scripts that represent all the non-injective agreement claims of the proposed scheme.

`Claim (AS, Nisynch);`

`Claim (TS, Niagree);`

`Claim (Node, Weakagree);`

`Claim (BS, Niagree);`

Final Figures [11-13] illustrate that there is no attack against non-injective agreement property.

5.3.1.5 Non-injective Synchronization

Synchronization demands that all protocol messages arrive in the correct sequence and with the measured value and that the response is the same as if the protocol were implemented without any adversary present [51]. The injective synchronization feature says that the protocol operates as planned throughout numerous runs, implying that an attacker will not be

CHAPTER 5. IMPLEMENTATION AND RESULTS

able to interrupt the present protocol execution by using knowledge from prior runs [49]. Such a kind of attack is known as a replay attack. “A replay attack is a type of attack in which an adversary injects traffic into a protocol's execution to cause unwanted or unexpected behavior.”

Following are the proposed scheme scripts that represent all the non-injective synchronization claims of the proposed scheme.

Claim (BS, Nisynch);

Claim (Node, Nisynch);

Claim (AS, Nisynch);

Claim (TS, Nisynch);

Results of the proposed scheme that are presented through figures [11-13] illustrate that there is no attack replay attack upon the scheme.

5.3.1.6 Running and Commit

Running and Commit signals (in Scyther modeled as claims) can be utilized as a type of authentication over variables that are sent in the communication. By using these claims, we can check that a variable sent from sender (U) to receiver (V), and then returned to U, has not been altered from its initial value during transmission. This may be viewed as a non-injective agreement on a set of terms from a formal viewpoint [52].

Following are the proposed scheme scripts that represent all the running and commits claims of the proposed scheme.

Claim (Node, Commit, AS, TGT, ET1);

Claim (Node, Running, AS, pas, req, ET);

Claim (Node, Running, TS, token, msg);

Claim (Node, Commit, BS, rectoken, pas, data, ET2, Response, ET3);

CHAPTER 5. IMPLEMENTATION AND RESULTS

```
Claim (BS, Running, TS, rectoken, pas, data, ET2, conMessage);
```

```
Claim (BS, Commit, TS, rectoken, pas, data, ET2, conMessage);
```

Results of the proposed scheme that are presented through figures [11-13] illustrate that there is no attack (that is related to the value alteration during the communication) against this property upon the scheme.

5.4 Scyther Scripts

Properties of Scyther i.e. aliveness, synchronization, protection against man-in-the-middle, commit and running, weakagree, non-injective agreement, and secrecy are tested and validated upon all the components of the scheme using the Scyther scripts that are shown individually against protocols roles (*BS, Node, AS, TS*) in the following figures.

```
claim(Node, Running, TS, token , msg);  
  
claim(Node, Alive);  
claim(Node,Weakagree);  
claim(Node, Niagree);  
claim(Node, Nisynch);  
claim(Node, Commit,AS,TGT,ET1);  
claim(Node,Secret,TGT );  
claim(Node, Secret, ET1);
```

Figure 5 Scyther Script-1

```
claim(AS, Secret, req);  
claim(AS, Secret,ET);  
claim(AS, Secret, has(pas));  
claim(AS,Secret,ET1);  
claim(AS,Secret,TGT);  
claim(AS, Niagree);  
claim(AS, Nisynch);
```

Figure 6 Scyther Script-2

```
claim(TS, Alive);
claim(TS, Weakagree);
claim(TS, Niagree);
claim(TS, Nisynch);
claim (TS, Secret, req1);
claim(TS, Secret,TGT);
claim(TS,Secret,token );
claim(TS, Secret, msg);
claim(TS, Secret, has(pas));
```

Figure 7 Scyther Script-3

```
claim(Node, Running, BS, rectoken ,pas,data,ET2,Response,ET3);

  claim(Node, Alive);
claim(Node,Weakagree);
claim(Node, Niagree);
claim(Node, Nisynch);
claim(Node, Commit,BS, rectoken, pas, data, ET2, Response, ET3);
claim(Node,Secret,Response );
claim(Node,Secret,ET3 );
claim(Node, Secret,ET2);
claim(Node,Secret, rectoken);
claim(Node, Secret,pas);
claim(Node, Secret,data);
```

Figure 8 Scyther Script-4


```
claim(BS, Running, TS, rectoken ,pas,data,ET2,conMessage);  
  
claim(BS,Alive);  
claim(BS,Weakagree);  
claim(BS, Niagree);  
claim(BS, Nisynch);  
claim(BS, Commit,TS, rectoken, pas, data, ET2,conMessage);
```

Figure 9 Scyther Script-5

```
claim(TS, Secret,rectoken);  
claim(TS, Secret, conMessage);
```

Figure 10 Scyther Script-6

5.5 Scyther Results

The findings produced by Scyther are shown in the following figures [11-13]. These Scyther generated results validate and verifies properties of Scyther i.e. Aliveness, Weak Agreement, Running and commit, Secrecy, Non-injective Synchronization, Non-injective Agreement, protection against Man-in-the-middle for both sides who are communicating.

The results show that the presented scheme successfully tested and provides strong resistance against targeted attacks (man-in-the-middle, replay attack, false data injection attack, fake node injection). Results prove that this scheme is safe and secure against them. In the next section, we examine these threats and explain how they are countered by our authentication system.

CHAPTER 5. IMPLEMENTATION AND RESULTS

Claim				Status	Comments	
secure	Node	secure,Node3	Alive	Ok	Verified	No attacks.
		secure,Node4	Weakagree	Ok	Verified	No attacks.
		secure,Node5	Niagree	Ok	Verified	No attacks.
		secure,Node6	Nisynch	Ok	Verified	No attacks.
		secure,Node7	Commit AS,TGT,ET1	Ok	Verified	No attacks.
		secure,Node8	Secret TGT	Ok	Verified	No attacks.
		secure,Node9	Secret ET1	Ok	Verified	No attacks.
AS		secure,AS1	Secret req	Ok	Verified	No attacks.
		secure,AS2	Secret ET	Ok	Verified	No attacks.
		secure,AS3	Secret {pas}has	Ok	Verified	No attacks.
		secure,AS4	Secret ET1	Ok	Verified	No attacks.
		secure,AS5	Secret TGT	Ok	Verified	No attacks.
		secure,AS6	Niagree	Ok	Verified	No attacks.
		secure,AS7	Nisynch	Ok	Verified	No attacks.
TS		secure,TS1	Alive	Ok	Verified	No attacks.
		secure,TS2	Weakagree	Ok	Verified	No attacks.
		secure,TS3	Niagree	Ok	Verified	No attacks.
		secure,TS4	Nisynch	Ok	Verified	No attacks.
		secure,TS5	Secret req1	Ok	Verified	No attacks.
		secure,TS6	Secret TGT	Ok	Verified	No attacks.

Done.

Figure 11 Scyther Results-1

CHAPTER 5. IMPLEMENTATION AND RESULTS

secure	Node	secure,Node3	Alive	Ok	Verified	No attacks.	
		secure,Node4	Weakagree	Ok	Verified	No attacks.	
		secure,Node5	Niagree	Ok	Verified	No attacks.	
		secure,Node6	Nisynch	Ok	Verified	No attacks.	
		secure,Node7	Commit AS,TGT,ET 1	Ok	Verified	No attacks.	
		secure,Node8	Secret TGT	Ok	Verified	No attacks.	
		secure,Node9	Secret ET 1	Ok	Verified	No attacks.	
		AS	secure,AS1	Secret req	Ok	Verified	No attacks.
			secure,AS2	Secret ET	Ok	Verified	No attacks.
secure,AS3	Secret {pas}has		Ok	Verified	No attacks.		
secure,AS4	Secret ET 1		Ok	Verified	No attacks.		
secure,AS5	Secret TGT		Ok	Verified	No attacks.		
secure,AS6	Niagree		Ok	Verified	No attacks.		
secure,AS7	Nisynch		Ok	Verified	No attacks.		
TS	secure,TS1	Alive	Ok	Verified	No attacks.		
	secure,TS2	Weakagree	Ok	Verified	No attacks.		
	secure,TS3	Niagree	Ok	Verified	No attacks.		
	secure,TS4	Nisynch	Ok	Verified	No attacks.		
	secure,TS5	Secret req1	Ok	Verified	No attacks.		
	secure,TS6	Secret TGT	Ok	Verified	No attacks.		
	secure,TS7	Secret token	Ok	Verified	No attacks.		
	secure,TS8	Secret msg	Ok	Verified	No attacks.		
Done.							

Figure 12 Scyther Results-2

CHAPTER 5. IMPLEMENTATION AND RESULTS

Claim				Status	Comments
secure2	Node	secure2,Node2	Alive	Ok	Verified No attacks.
		secure2,Node3	Weakagree	Ok	Verified No attacks.
		secure2,Node4	Niagree	Ok	Verified No attacks.
		secure2,Node5	Nisynch	Ok	Verified No attacks.
		secure2,Node6	Commit BS,rectoken,pas,data,ET2,Response,ET3	Ok	Verified No attacks.
		secure2,Node7	Secret Response	Ok	Verified No attacks.
		secure2,Node8	Secret ET3	Ok	Verified No attacks.
		secure2,Node9	Secret ET2	Ok	Verified No attacks.
		secure2,Node10	Secret rectoken	Ok	Verified No attacks.
		secure2,Node11	Secret pas	Ok	Verified No attacks.
		secure2,Node12	Secret data	Ok	Verified No attacks.
		BS		secure2,BS2	Alive
secure2,BS3	Weakagree			Ok	No attacks within bounds.
secure2,BS4	Niagree			Ok	No attacks within bounds.
secure2,BS5	Nisynch			Ok	No attacks within bounds.
secure2,BS6	Commit TS,rectoken,pas,data,ET2,conMessage			Ok	No attacks within bounds.
TS				secure2,TS1	Secret rectoken
		secure2,TS2	Secret conMessage	Ok	No attacks within bounds.

Done.

Figure 13 Scyther Results-3

5.6 Security Analysis

We analyzed the suggested authentication scheme's potential to defend against the attacks mentioned in the previous section. In this section, we present the types of attacks that our authentication scheme prevents.

5.6.1 Man-in-the-Middle Attack

Man-in-the-middle-attack is a kind of attack in which a malicious node penetrates or invades the communication between two parties [53]. It takes on the identities of both parties and obtains access to information that they were attempting to communicate to each other. It enables a malicious agent to send, receive and intercept, data intended for anyone else, or data that was never intended to be sent at all, without either party knowing until the operation is finished. Through the proposed authentication scheme all the communication between the parties is encrypted and secure. Only those who can decrypt the communication can understand the complete message.

As a result, our suggested authentication method can easily identify and prevent this attack. Moreover, practically there is no attack against weak agreement claim property that discuss in the previous section, and their results are shown in the Scyther results figures.

5.6.2 Replay Attack

A replay attack is a type of network attack in which legitimate data transfer is replayed or delayed intentionally or fraudulently [54]. This can be done by the source or by an adversary who hijacks the data and re-transmits it. Because our scheme holds the synchronization security claim and results show that there is no attack against this claim. Also, we are using timestamps in our scheme to mitigate this kind of attack.

To avoid replay attacks in the information networks timestamps are very effective [55]. After the critical analysis and as a result, the replay attack is not possible with our proposed authentication protocol.

5.6.3 False Data Injection Attack

False data injection attack (FDIA) refers to the situation in which an attacker manipulates sensor data in such a way that undiscovered mistakes are introduced into computations of state variables and values. False data injection attacks (FDIA) typically alter sensor data, causing CPSs to become unstable [56]. Sometimes attackers add false data to the communication packet for increasing the data packet size. Because our proposed scheme guarantees the secrecy property which means that the specified attribute is to be kept secret from the adversary, even if the attacker controls the communication network. And results against secrete claim shows that there is no attack against this security claim.

Moreover, the proposed scheme uses the running and commit signals which means that the values of the variables that send from the sender to the receiver and receiver to the sender are the same. No, any intercept was done during the send and receive events. Because communication variables are used to holds the data items if at any point Eve altered or inject malicious data and try to perform a false data injection attack then this attack is easily identified.

5.6.4 Fake Node Injection

In this type of attack, the attacker adds a fake node by spoofing the legal node-id [57]. For performing such kinds of attacks attackers sometimes hijack the legal node fully take charge by adding their own fake node in the network. When its fake node becomes part of the network then using this node, he intercepts all the traffic easily. In our proposed shames nodes only add with the help of the network administrator. At the time when a node becomes a part of the network, its buffer is loaded with some predefined parameters i.e. id and password. So, becoming part of a network needs some predefined parameters and administrators' rights. For communication to other components required these predefined parameters. Gaining both at the same time is too difficult for the Eve.

Moreover, the proposed scheme holds the aliveness security property which means that the reply from the receiving party is the consequence of the request made by the communication initiation party. So, the fake node never receives any kind of response from

other any component of the scheme because it never initiates the communication with the wrong parameters. As a result, our scheme provides resilience against this attack.

5.7 Proposed Scheme Performance Evaluation

The performance impact of the proposed authentication scheme is also examined for checking the effectiveness of the scheme. In this study, two important aspects are considered first one is security and the second one is efficiency. Security of the proposed scheme tested in the previous section using Scyther tool now in this section efficiency of the proposed scheme is tested. A comparison is also done with already proposed schemes for efficient authentication. Numerical results of the proposed scheme that are presented in Table 3 prove that the scheme is more optimized than the other comparison schemes.

5.7.1 Resource Accessibility and Availability

Network resources are exclusively allocated to authenticated nodes in the proposed approach. In the suggested solution, network resources are only allocated to authenticated nodes. As a result, the resources are only accessible to authenticated nodes. This improves network performance, security and optimized the scheme in terms of computing resources also makes it optimized. Moreover, for the development of the scheme, there is no usage of public-key cryptographies mostly used for strong authentication. Proofs in the form of numerical results that are shown in the Tale 3 proves that the proposed scheme is more optimized and optimized.

5.7.2 Numerical Results

In this research proposed authentication scheme is also compared to the approaches presented in [9] [24] and [58] for checking the better efficiency. This comparison depends upon the total authentication time and the number of cryptographic primitives required by each scheme. In this study for performance evaluation, we utilize the benchmarks from [59] where the cryptographic methods are implemented in C++, the system specs are an Intel Core2 Duo 1.83 GHz, CPU is running upon the Windows Vista in 32-bit mode and the compiler is Microsoft Visual C++ 2005 SP1.

CHAPTER 5. IMPLEMENTATION AND RESULTS

Because authors of the schemes with which comparison are performed for efficiency also using the same benchmarks for performance evaluation. So, for generating the numerals results same benchmark is very important for accurate results. In this study cryptographic algorithm for performing each cryptographic primitive in the proposed scheme as well as the crypto algorithm and primitives that are used in the comparison schemes are presented in the Table 2.

Table 2 Cryptographic Primitive and Algorithm

Cryptographic Primitive	Cryptographic Algorithm
Certificate Validation	RSA 1024
Hash Function	HMAC(SHA-1)
Message Encryption with Symmetric Key	AES/EAX
Message Encryption with Public Key	RSA 1024
Message Decryption with Symmetric Key	AES/EAX
Message Decryption with Public Key	RSA 1024
Digital Signature Generation and Verification	RSA 1024

We can calculate how many times each cryptographic primitive is done in total by evaluating the authentication schemes provided in [9], [24], and [58] and in this study proposed scheme, considering the benchmarks from [59], as presented in Table 3. Moreover, to calculate the time required to complete the authentication process in each proposed scheme, we take the values from Tables 2 and 3.

For completing the authentication process the proposed schemes in [9],[24], and [58] use twenty-four, twenty-nine, and thirty-nine cryptographic primitives respectively.

Table 3 Cryptographic Primitives Count

Cryptographic Primitive	Comparison Schemes			
	[24]	[58]	[9]	Proposed Scheme
Certificate Validation	5	4	2	0
Hash Function	2	13	2	4
Message Encryption with Symmetric Key	0	6	6	6
Message Encryption with Public Key	7	4	4	0
Message Decryption with Symmetric Key	0	6	6	6
Message Decryption with Public Key	7	4	4	0
Digital Signature Generation	4	1	0	0
Digital Signature Verification	4	1	0	0
Total	29	39	24	16

However, in the proposed scheme only sixteen primitives are required for completing the authentication process which means approximately 25% less computation and calculation cost.

Next, the time required to complete the authentication process is examined, also known as authentication delay. It is divided into two parts, the transmission time and the processing time. The processing time is the most important component because it reflects the time required to perform cryptographic primitives. And the transmission time is defined as “The time required to send the message between the communication nodes. “For numerical results, it is assumed that in the proposed scheme and the all the comparison schemes have

CHAPTER 5. IMPLEMENTATION AND RESULTS

same transmission time so that for calculation of the authentication delay transmission time was omitted.

According to [59], the time for the message encryption with the public key is 0.08ms, the time for the message encryption with symmetric key is 1.8 μ s, for the message decryption with public key time is 1.46ms, the message decryption with symmetric key takes 1.8 μ s, the hashing time using HMAC (SHA-1) is 0.509 μ s, the time required for signature generation is 1.48ms and the verification time using RSA 1024 is 0.07ms.

In [24] the authentication time was 17.3ms, the authentication time of the proposed scheme in [58] was 8.02ms and in [9] it was 7.23ms respectively. And the authentication time in the proposed scheme is approximately 27.236 μ s or 0.027236ms. After these results, it is proof that the proposed scheme is approximately 84%, 66%, and 62% faster in comparison to that in [24],[58], and [9], respectively.

From the result, it is clear that the proposed approach cuts down the authentication time. Moreover, symmetric-key cryptography is utilized to encrypt and decrypt the majority of the messages transmitted between communication parties. Symmetric key cryptography has less memory use less power utilization and less memory occupation. Hence the proposed scheme is optimized and less complicated than that of comparison schemes.

5.8 Summary

This chapter discusses the implementation of the proposed solution and the results in detail, which are related to our objectives mentioned at the beginning of Chapter 1. Scyther, a network protocol analysis tool, is used to test the scheme. Explanations that are related to the used tool are also included in this chapter for the understanding of the working of this tool. Attacks list that is the part of scheme features also explained in this chapter.

Recourse accessibility and availability are explained at the last of the chapter that explains how the proposed scheme is optimized and efficient. From the results of the comparisons with other proposed schemes, it is clear that the proposed approach reduces the authentication time. The proposed scheme is less complicated than that of comparison schemes. Symmetric-key cryptography is utilized to encrypt and decrypt the majority of the

CHAPTER 5. IMPLEMENTATION AND RESULTS

messages transmitted between communication parties. Symmetric key cryptography has less memory use less power utilization and less memory occupation. Hence the proposed scheme is less complicated than that of comparison schemes. The study is concluded in the next chapter.

Chapter 6

Conclusion & Future Work

The thesis is concluded in chapter 6 with a discussion of possible future research areas. It identifies open research challenges that need to be answered by the scientific community and presents alternative research opportunities for our research.

6.1 Conclusion

Secure communication with minimum computing resources between any kind of network node is very important. Because sometimes very confidential and secret data communicate through network devices. So, for the verification of the device's authentication mechanism is used commonly in networking. A lot of techniques and schemes are proposed for authentication to achieve the security goals in the information networks. But most of the proposed authentication schemes are based upon public-key cryptography and digital signatures. Studied authentication schemes provide secure authentication but are vulnerable to different attacks. Also, for implementation of public-key cryptography i.e. RSA communication payload size increases, and sometimes end nodes that are battery-held do not support for a long time.

Moreover, implementation of these schemes upon the small level networks is also a challenge. In the literature, some authentication schemes that are efficient and good for small and sensitive types of networks are vulnerable to a common type of attack. Hence, those authentication frameworks that provide strong authentication are not optimized and demand extensive resources. Those that fulfill the optimized property are vulnerable to attacks. Hence in these schemes, some security weaknesses exist and require an implementation that is optimized and optimized in terms of computing resources and provides strong resilience against known attacks.

CHAPTER 6. CONCLUSION & FUTURE WORK

Thus, in this research, we have proposed an optimized and secure authentication scheme for network devices. In comparison to previous techniques, the suggested authentication scheme decreases the number of cryptographic primitives and the computation required to complete the authentication process. In our proposed schemes there is not any kind of digital signature and public key infrastructure is used for secrecy its only used symmetric key and hash function that makes it lightweight. Also proposed scheme provides strong resilience against a common type of attack. Scyther protocol analyzer tool was used to verify the scheme. Mitigated attacks through this scheme are man-in-the-middle, replay attacks, false node injection, and false data detection. Finally, the results of the Scyther prove the validity of the scheme. Following are the main contribution of this study.

- The proposed scheme eliminates the need for public-key cryptography for secure communication.
- This study provides an authentication framework that is optimized, optimized, less complex, takes less time for authentication time, and is secure for wireless network devices communication.
- Provide extending security features that minimize the wireless communication security challenges using less authentication time, power utilization, and less memory occupation.
- The scheme is implementable in all the environments based on wireless communication like smart agriculture, IoT, Industry 4.0, Environmental WSN, Smart cities, Cognitive Radio Networks (CRNs), etc.

6.1.1 Future Work

The future work that may be done with this system is to study hardware properties of network devices in-depth to see whether they can be utilized as a source of authentication information for this approach to minimize the server's workload. Because PGP (Pretty Good Privacy) requires an initial key exchange, this technique may also be applied with PGP and Blockchain.

CHAPTER 6. CONCLUSION & FUTURE WORK

This technique may also be used to create secure communication apps for IOS and Android. This scheme can also be studied for group communication protocols where we need continuous authentication and need security in layers.

6.2 Summary

In this chapter, this study's conclusion has presented. This chapter also briefly explained that why this study is carried out and how to achieve the target that discusses in the problem statement. What are the main vulnerabilities? That exists in the previous solutions and how this study mitigates the targeted challenges effectively and efficiently. After carrying out this study main contribution is listed here. It also provides the road map of how this study can be further used in different real-life computer applications.

Furthermore, it discusses possible future study directions for the researchers and scholars in which this theory may be expanded.

Bibliography

- [1] H.-N. Dai, R. C.-W. Wong, H. Wang, Z. Zheng, and A. V. Vasilakos, “Big Data Analytics for Large-scale Wireless Networks,” *ACM Comput. Surv.*, vol. 52, no. 5, pp. 1–36, 2019, doi: 10.1145/3337065.
- [2] S. Abidin, V. R. Vadi, and A. Rana, “On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN,” in *Advances in Computer, Communication and Computational Sciences*, Springer, 2021, pp. 87–97.
- [3] C. Biswas, U. Das Gupta, and M. M. Haque, “An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography,” in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2019, pp. 1–5.
- [4] J. Cui, L. Shao, H. Zhong, Y. Xu, and L. Liu, “Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks,” *Peer-to-Peer Netw. Appl.*, vol. 11, no. 5, pp. 1022–1037, 2018.
- [5] J. Zhao and G. Cao, “Robust topology control in multi-hop cognitive radio networks,” *IEEE Trans. Mob. Comput.*, vol. 13, no. 11, pp. 2634–2647, 2014.
- [6] A. J. Olaode, “AVAILABILITY OF INFORMATION AND ITS SECURITY MEASURES,” in *СОВРЕМЕННЫЕ ТЕХНОЛОГИИ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ*, 2019, pp. 37–42.
- [7] M. Khasawneh, I. Kajman, R. Alkhudaiby, and A. Althubyani, “A survey on Wi-Fi protocols: WPA and WPA2,” in *International Conference on Security in Computer Networks and Distributed Systems*, 2014, pp. 496–511.
- [8] H. Z. U. Khan and H. Zahid, “Comparative study of authentication techniques,” *Int. J. Video Image Process. Netw. Secur. IJVIPNS*, vol. 10, no. 04, pp. 9–13, 2010.
- [9] M. Khasawneh and A. Agarwal, “A secure and efficient authentication mechanism applied to cognitive radio networks,” *IEEE Access*, vol. 5, pp. 15597–15608, 2017.
- [10] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, “Continuous and transparent multimodal authentication: reviewing the state of the art,” *Cluster Comput.*, vol. 19, no. 1, pp. 455–474, 2016.
- [11] A. H. Moon, U. Iqbal, and G. M. Bhat, “Implementation of node authentication for WSN using hash chains,” *Procedia Comput. Sci.*, vol. 89, pp. 90–98, 2016.
- [12] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance,” *Futur. Gener. Comput. Syst.*, vol. 91, pp. 244–251, 2019.
- [13] N. A. M. Risalat, M. T. Hasan, M. S. Hossain, and M. M. Rahman, “Advanced real

BIBLIOGRAPHY

- time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process,” in *2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2017, pp. 788–793.
- [14] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey,” *Cryptography*, vol. 2, no. 1, p. 1, 2018.
- [15] Z. A. Alizai, N. F. Tareen, and I. Jadoon, “Improved IoT device authentication scheme using device capability and digital signatures,” in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, 2018, pp. 1–5.
- [16] D. Wang and P. Wang, “Two birds with one stone: Two-factor authentication with security beyond conventional bound,” *IEEE Trans. dependable Secur. Comput.*, vol. 15, no. 4, pp. 708–722, 2016.
- [17] Z. Li *et al.*, “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild.,” 2017.
- [18] M. Pannu, R. Bird, B. Gill, and K. Patel, “Investigating vulnerabilities in gsm security,” in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 2015, pp. 1–7.
- [19] O. Delgado-Mohatar, A. Fúster-Sabater, and J. M. Sierra, “A light-weight authentication scheme for wireless sensor networks,” *Ad Hoc Networks*, vol. 9, no. 5, pp. 727–735, 2011.
- [20] X. Sun, S. Men, C. Zhao, and Z. Zhou, “A security authentication scheme in machine-to-machine home network service,” *Secur. Commun. Networks*, vol. 8, no. 16, pp. 2678–2686, 2015.
- [21] K. Garrett, S. R. Talluri, and S. Roy, “On vulnerability analysis of several password authentication protocols,” *Innov. Syst. Softw. Eng.*, vol. 11, no. 3, pp. 167–176, 2015.
- [22] H.-J. Mun, S. Hong, and J. Shin, “A novel secure and efficient hash function with extra padding against rainbow table attacks,” *Cluster Comput.*, vol. 21, no. 1, pp. 1161–1173, 2018.
- [23] S. Parvin and F. K. Hussain, “Digital signature-based secure communication in cognitive radio networks,” in *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*, 2011, pp. 230–235.
- [24] S. Parvin, F. K. Hussain, and O. K. Hussain, “Digital signature-based authentication framework in cognitive radio networks,” in *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, 2012, pp. 136–142.
- [25] A. Al-Mahmud and M. C. Morogan, “Identity-based authentication and access control in wireless sensor networks,” *Int. J. Comput. Appl.*, vol. 41, no. 13, 2012.
- [26] V. J. Rathod, N. C. Iyer, and S. M. Meena, “A survey on fingerprint biometric recognition system,” in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 323–326.
- [27] A. El-Sayed, “Multi-biometric systems: a state of the art survey and research

BIBLIOGRAPHY

- directions,” *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 6, 2015.
- [28] Q. Jiang, J. Ma, G. Li, and X. Li, “Improvement of robust smart-card-based password authentication scheme,” *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 383–393, 2015.
- [29] M. A. Wala’a and H. Abusaimh, “Modified USB security token for user authentication,” *Comput. Inf. Sci.*, vol. 8, no. 3, p. 51, 2015.
- [30] A. X. Liu and L. A. Bailey, “PAP: A privacy and authentication protocol for passive RFID tags,” *Comput. Commun.*, vol. 32, no. 7–10, pp. 1194–1199, 2009.
- [31] P. Gope, J. Lee, and T. Q. S. Quek, “Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2831–2843, 2018.
- [32] S. Rajasekar, P. Philominathan, and V. Chinnathambi, “Research Methodology, Tamilnadu, India,” *Soc. Res. Methods Ser.*, vol. 5, 2013.
- [33] W. C. Booth, W. C. Booth, G. G. Colomb, J. M. Williams, G. G. Colomb, and J. M. Williams, *The craft of research*. University of Chicago press, 2003.
- [34] “Research Methodology: An Introduction,” vol. IX, pp. 1–23, 1952.
- [35] H. Yang, V. Oleshchuk, and A. Prinz, “Verifying group authentication protocols by Scyther,” *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 7, no. 2, pp. 3–19, 2016, doi: 10.22667/JOWUA.2016.06.31.003.
- [36] C. Cremers, “Scyther User Manual,” pp. 2–52, 2014, [Online]. Available: <http://users.ox.ac.uk/~coml0529/scyther/index.html%0AUsers>.
- [37] C. Cremers and S. Mauw, “Security properties,” in *Operational Semantics and Verification of Security Protocols*, Springer, 2012, pp. 37–65.
- [38] C. Cremers, *Scyther: Semantics and verification of security protocols*, no. november. 2006.
- [39] S. A. Thorat, P. J. Kulkarni, and S. V Yadav, “Formal verification of opportunistic routing protocol using SPIN model checker,” in *2017 international conference on energy, communication, data analytics and soft computing (ICECDS)*, 2017, pp. 2717–2722.
- [40] P. Lafourcade, V. Terrade, and S. Vigier, “Comparison of cryptographic verification tools dealing with algebraic properties,” in *International Workshop on Formal Aspects in Security and Trust*, 2009, pp. 173–185.
- [41] E. Barker, G. Locke, and P. D. Gallagher, “Recommendation for Digital Signature Timeliness,” *NIST Spec. Publ.*, no. September, pp. 800–102, 2009.
- [42] N. Mouha, M. S. Raunak, D. R. Kuhn, and R. Kacker, “Finding bugs in cryptographic hash function implementations,” *IEEE Trans. Reliab.*, vol. 67, no. 3, pp. 870–884, 2018.
- [43] S. Santhanalakshmi, K. Sangeeta, and G. K. Patra, “Design of secure Cryptographic hash function using soft computing techniques,” *Int. J. Adv. Soft Comput. its Appl.*, vol.

BIBLIOGRAPHY

- 9, no. 2, pp. 188–203, 2017.
- [44] M. Ilayaraja, K. Shankar, and G. Devika, “A modified symmetric key cryptography method for secure data transmission,” *Int. J. Pure Appl. Math.*, vol. 116, no. 10, pp. 301–308, 2017.
- [45] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and A. Mosavi, “Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography,” *Sensors*, vol. 19, no. 21, p. 4752, 2019.
- [46] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Trans. Inf. theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [47] I. Cervesato, “The Dolev-Yao intruder is the most powerful attacker,” in *16th Annual Symposium on Logic in Computer Science—LICS*, 2001, vol. 1.
- [48] E. Klevstad, “Security and Key Establishment in IEEE,” no. June, 2016.
- [49] C. Cremers and S. Mauw, “Operational semantics of security protocols,” in *Scenarios: Models, Transformations and Tools*, Springer, 2005, pp. 66–89.
- [50] G. Lowe, “A hierarchy of authentication specifications,” in *Proceedings 10th Computer Security Foundations Workshop*, 1997, pp. 31–43.
- [51] C. J. F. Cremers, S. Mauw, and E. P. de Vink, “Injective synchronisation: an extension of the authentication hierarchy,” *Theor. Comput. Sci.*, vol. 367, no. 1–2, pp. 139–161, 2006.
- [52] C. J. F. Cremers, “Scyther user manual, 2014.” 2014.
- [53] A. Mallik, “Man-in-the-middle-attack: Understanding in simple words,” *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 2, no. 2, pp. 109–134, 2019.
- [54] F. Farha, H. Ning, W. Zhang, and K.-K. R. Choo, “Timestamp scheme to mitigate replay attacks in secure zigbee networks,” *IEEE Trans. Mob. Comput.*, 2020.
- [55] F. Farha and H. Ning, “Enhanced timestamp scheme for mitigating replay attacks in secure zigbee networks,” in *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 2019, pp. 469–473.
- [56] D. Ye and T.-Y. Zhang, “Summation detector for false data-injection attack in cyber-physical systems,” *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, 2019.
- [57] V.-T. Nguyen, V.-H. Bui, T.-T. Nguyen, and T.-M. Hoang, “A Novel Watermarking Scheme to against Fake Node Identification Attacks in WSNs,” in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 2018, pp. 1–5.
- [58] K. Chatterjee, A. De, and D. Gupta, “A secure and efficient authentication protocol in wireless sensor network,” *Wirel. Pers. Commun.*, vol. 81, no. 1, pp. 17–37, 2015.
- [59] W. Dai, “Crypto++ 5.6. 0 Benchmarks,” <http://www.cryptopp.com/benchmarks.html>, 2009.

Appendices

```
/*
A Lightweight and more Secure Authentication Scheme for Network
  devices.
*/

// The protocol description Part 1

usertype Timestamp;      // for using timestamp in the protocol

usertype Hashfunction; // for using hashfunction in the protocol

//usertype key;

// Nonde-> Device  AS -> Authentication Server & TS -> Tocken
Server

protocol secure (Node, AS, TS )
{

role Node

{

fresh pas: Nonce;

fresh req: Nonce;

fresh ET: Timestamp;
```

APPENDICES

fresh has: Hashfunction;

fresh req1: Nonce;

fresh TGT: Nonce;

var TGT: Nonce;

var ET1: Nonce;

var token: Nonce;

var msg: Nonce;

send_1(Node, AS, { ET, has(pas) , req} k(Node,AS));

recv_2(AS,Node, {TGT, ET1} k(Node,AS));

claim(Node,Running,AS, pas,req,ET);

send_3(Node, TS , {has(pas), TGT , req1}k(Node,TS));

recv_4(TS, Node , {token, msg}k(TS,Node));

claim(Node, Running, TS, token , msg);

claim(Node, Alive);

claim(Node,Weakagree);

claim(Node, Niagree);

APPENDICES

```
claim(Node, Nisynch);

claim(Node, Commit, AS, TGT, ET1);

claim(Node, Secret, TGT );

claim(Node, Secret, ET1);

}

role AS
{

var ET: Timestamp;

var req: Nonce;

var has: Hashfunction;

var pas: Nonce;

fresh TGT: Nonce;

fresh ET1: Nonce;

recv_1(Node, AS, { ET, has(pas) , req} k(Node,AS) );

send_2(AS, Node, {TGT, ET1} k(Node,AS) );

claim(AS, Secret, req);

claim(AS, Secret, ET);

claim(AS, Secret, has(pas));
```

APPENDICES

```
claim(AS, Secret, ET1);  
claim(AS, Secret, TGT);  
claim(AS, Niagree);  
claim(AS, Nisynch);  
}  
  
role TS  
{  
fresh token: Nonce;  
  
fresh msg: Nonce;  
  
var has: Hashfunction;  
  
var TGT: Nonce;  
  
var pas: Nonce;  
  
var req1: Nonce;  
  
recv_3(Node, TS , {has(pas), TGT , req1}k(Node,TS));  
  
send_4(TS, Node , {token, msg}k(TS,Node));  
  
claim(TS, Alive);  
claim(TS, Weakagree);  
claim(TS, Niagree);
```

APPENDICES

```
claim(TS, Nisynch);

claim (TS, Secret, req1);

claim(TS, Secret,TGT);

claim(TS,Secret,token );

claim(TS, Secret, msg);

claim(TS, Secret, has(pas));

}

}

/*
A Lightweight and more Secure Authentication Scheme for Network
  devices .
*/
// The protocol description Part 2

// Here is the protocol description

usertype Timestamp;      // for using timestamp in the protocol

usertype Hashfunction; // for using hashfunction in the protocol

//usertype key;

// Nonde-> Device: & TS -> Token Server & BS-> Base station

protocol secure2 (Node, BS, TS )
{
```

APPENDICES

```
role Node

{

fresh data: Nonce;

fresh rectoken:Nonce;

fresh ET2: Timestamp;

fresh pas: Nonce;

fresh has:Hashfunction;

var Response: Nonce;

var ET3: Timestamp;

var pas:Nonce;

send_1(Node, BS, {rectoken, pas, data, ET2} k (Node,BS) );

recv_4(BS, Node, { Response, ET3} pas );

claim(Node, Running, BS, rectoken ,pas,data,ET2,Response,ET3);

claim(Node, Alive);

claim(Node,Weakagree);

claim(Node, Niagree);

claim(Node, Nisynch);
```


APPENDICES

```
claim(Node, Commit,BS, rectoken, pas, data, ET2, Response,  
      ET3);
```

```
claim(Node,Secret,Response );
```

```
claim(Node,Secret,ET3 );
```

```
claim(Node, Secret,ET2);
```

```
claim(Node,Secret, rectoken);
```

```
claim(Node, Secret,pas);
```

```
claim(Node, Secret,data);
```

```
}
```

```
role BS
```

```
{
```

```
var rectoken: Nonce;
```

```
var pas: Nonce;
```

```
var data: Nonce;
```

```
var nodeid: Nonce;
```

```
var ET2: Timestamp;
```

```
var has: Hashfunction;
```

```
fresh rectoken: Nonce;
```

```
fresh conMessage: Nonce;
```

APPENDICES

fresh ET3: Timestamp;

fresh Response: Nonce;

fresh pas: Nonce;

recv_1(Node, BS, {rectoken, pas, data, ET2} k (Node,BS));

send_2(BS, TS , {rectoken, conMessage} k(TS, BS));

recv_3 (TS, BS, { nodeid} k(TS,BS));

send_4(BS, Node , {Response, ET3} pas);

claim(BS, Running, TS, rectoken , pas, data, ET2, conMessage);

claim(BS, Alive);

claim(BS, Weakagree);

claim(BS, Niagree);

claim(BS, Nisynch);

claim(BS, Commit, TS, rectoken, pas, data, ET2, conMessage);

}

role TS

{

APPENDICES

```
fresh nodeid:Nonce;
```

```
var rectoken:Nonce;
```

```
var conMessage;
```

```
recv_2 (BS,TS, {rectoken,conMessage} k(TS, BS) );
```

```
send_3 (TS,BS, { nodeid} k(TS,BS) );
```

```
claim(TS, Secret,rectoken);
```

```
claim(TS, Secret, conMessage);
```

```
}
```

```
}
```

Certificate for Plagiarism

It is certified that PhD/M.Phil/MS Thesis Titled "A Secure and Optimized Authentication Scheme for Network Devices" by NAVEED HUSAIN has been examined by us. We undertake the follows:

- a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled/analyzed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

Name & Signature of Supervisor

Dr. Dr Hasan Tahir

Signature :

