An Enhanced Authentication Scheme for Ensuring Network Devices Security and Performance Optimization

Naveed Husain[1*], Farrukh Liaqat[1], Zeeshan Akram[2]
[1]School of Systems and Technology, University of Management and Technology, Lahore, Pakistan.
[2]Department of Computer Science, Lahore Leads University, Lahore, Pakistan.
***Correspondence**: naveed.husain@umt.edu.pk

Citation | Husain, N, Liaqat. F, Akram. Z, "An Enhanced Authentication Scheme for Ensuring Network Devices Security and Performance Optimization", IJIST, Vol. 5 Issue. 3, pp. 178-192, Sep 2023.
Received | Aug 27, 2023**; Revised |** Sep 18, 2023**; Accepted |** Sep 19, 2023; **Published |** Sep 20, 2023.

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 have 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 in network-connected devices. The research will study how a wide variety of devices like those in IoT, WSN, industrial IoT, and 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.

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 Server
IBS	Identity-Based Signature

Keywords: Wireless Networks (WNs), Message Digests (MDs), Secret Value, Base Station, Token Server, Authentication Server, Network Node

Introduction:

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. 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 WN networks, which have undergone rapid development. Wireless Networks (WNs) are emerging 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 have increased 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 increases at the same speed. Security plays an important role in WN 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. The wireless nature of communication, resource limitation, secure communication, high risk of node addition/removal, etc. is major challenges. Because network resources and their communication data are very confidential, moving upon an insecure network can create problems. If any network node or secret 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 is very important due to which we protect our network from different types of attacks.

Many principles should be used to ensure secure communication between WN 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 needed 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]. The last important security requirement is authentication which 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 that needs proper authentication first [7]. In this study, our focus is on authentication. For secure communication in wireless networks authentication of nodes is very important. 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 should be strong. Provisioning of resources to an adversary or a lack of providing to a legal user may be the result of poor 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. However, most studied schemes in the literature are based upon public-key cryptography that during communication packet size increases rapidly which is not feasible mostly in small wireless networks. Most wireless network nodes have limited resources (processing power, memory) that's why handling payloads is very challenging for these nodes.

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

Literature Review:

Many researchers have explored the authentication field and suggested a variety of solutions to current vulnerabilities that exist in the networking devices authentication phase [9][10][11][12]. The related work is simply the research done over the years by various researchers that are linked to the research done in this paper and helped to the development of a new solution.

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 by legitimate network nodes and these network nodes easily perform secure communication over insecure channels. Similarly, user authentication requires that the identity of the user is verified following which a user is provided access to the device.

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. Authentication is the primary countermeasure that ensures that an authentic user has 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, smartphones, 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. The following sections visit some of the most common authentications.

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. 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. The main disadvantage of this scheme of using Elliptic Curve Cryptography (ECC) is that it increases the size of the encrypted message significantly more than RSA encryption. 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. The drawbacks of using this scheme are that communication cost is high, computation cost at the cloud is high

and also in this proposed scheme, there is no consideration of denial-of-service (DOS) and distributed denial-of-service (DDoS) attacks. In [13] for IoT devices, authors develop a secure and mutual authentication scheme using the one-way hash function.

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 have 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.

When compared to traditional authentication procedures, multi-factor authentication provides greater security [16]. 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, and authentication Short Message Service (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].

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. Asymmetric encryption or public-key encryption is also used for authentication, and it has 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. 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 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. The proposed scheme provides perfect resilience against common attacks (Man-in-the-middle attack (MITM), Denial-of-Service (DoS)), and reflection attacks). The drawback of using this scheme is that its deployment and integration are too complex and require high maintenance resources.

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 [20] authors present a security authentication scheme in machine-to-machine (M2M) home network service. 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 has some practical merits. But energy cost is too high when we use this scheme.

Recent research [21] investigated many password-based authentication systems and claims 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 the length of passwords increases, memorizing alphabets, numbers, special characters, and alphanumeric data with different combinations becomes tedious. When network devices use weak passwords guessing attacks, dictionary attacks, and brute force are easily launched by the attackers [22].

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. Parvin et al. [23][24] have developed a scheme that is based upon the digital signature, and in this

scheme for the authentication process, they generate the asymmetric keys with the help of the Rivest-Shamir-Adleman (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.

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. This authentication scheme provides strong resilience against Denial-of-service (DoS) and node-capture attacks. However, the drawbacks of using this scheme are that the password change procedure and user registration are not enabled.

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. 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 the 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.

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 encryption keys. 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. 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 these characteristics. These features rely on many factors like materials, inherent characteristics introduced by fabrication, and environmental noise.

Objectives:

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." Following are the main objectives of the proposed solution:

- 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.
- 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.

Materials & Methods:

The proposed solution includes Strong authentication and continuous authentication and provides 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 device communication. It also provides extending security features that minimize the wireless communication security challenges using less authentication time, power utilization, and less memory occupation. Moreover, the proposed authentication scheme proved mutual and continues authentication to network devices until communication is performed securely over the insecure network.

Our secure and efficient authentication scheme is explained in this section. It is based on symmetric key cryptography and hashing. Completing the authentication process minimizes the crypto primitives and packet payload. In the proposed system model, there are four major components. The base station (BS) 2. An authentication server (AS) 3. Token Server (TS) 4. Network Node (NN).

In this network, the Base Station (BS) is responsible for controlling and acting after receiving the secret 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 part of the network and responsible for sensing the data from the critical environment and sending it to the base station for further actions. The authentication server (AS) is responsible for authenticating the interested nodes and making sure these devices are trusted and become part of the network through the network administrator priory. Token Server (TS) works as a second layer of security and provides continuous authentication. There are two main phases of the proposed scheme 1. Preliminary Phase 2. Scheme Implementation Details. These two phases are discussed below.

Preliminary Phase:

There are 4 major components in the proposed protocol. The first one is the 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, we assume the manufacturer of the nodes assigns or preloads a unique ID i.e., N1, N2, N3……. Nf. And also preload a secret key in every node's buffer. Let us assume between the Authentication Server (AS) and Token Server (TS) a secret key is already shared successfully. Assume a database is created according to the requirements and 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 2 illustrates the scheme secret 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 built network for each node network administrator assigns the unique key or password manually and then adds the node ID and hash of their key (H (nK)) in the network database. Also, the 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 the scheme description starts.

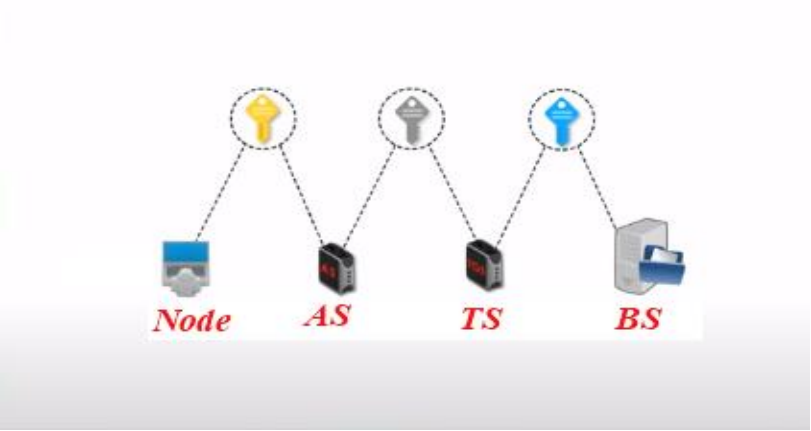

Figure 1. Scheme Keyset

Preliminary Phase:

Scheme description is the main phase of the scheme and it is carried out every time (when a new node requests to join the network or when new networks are deployed from the start) once the previous phase has been finalized. When any node wants to communicate 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) receives this packet in the following way at their 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 is received. 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). Also, make an 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 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).

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

The token server (TS) received this request payload like this:

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). Also, match the hash from the database against this ticket (this entry is done in step No. 2) either it's an authentic node or not. If there is no problem then it issues the client token (for a certain period and date) which is encrypted with another secret key for communication with the Base Station (BS). Also, make an entry of this token into another column of the database against node ID.

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

The requesting node received this packet from the 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 also sent encrypted data to BS using their password.
Node → BS: send_1 (Node, BS, {rectoken, pas, data, ET2} k (Node, BS));
The base station received this request from the node:
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 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 node's passwords because, in the first phase, all passwords are loaded into BS memory).
BS→ TS: send_2 (BS, TS, {rectoken, conMessage} k (TS, BS));
Token server (Server) received this payload from the BS like this:
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 sent to which device. After matching its share, the id of this node to BS is 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));
The base station (BS) gets 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 decrypts the message and gets 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 the response with that node password.
BS→ Node: send_4 (BS, Node, {Response, ET3} pas);
Node gets requested a response from the BS like this:
recv_4 (BS, Node, {Response, ET3} pas);
Step 9. Node decrypts the response from their 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.
Figure 2 (the sequence diagram of the proposed scheme) illustrates the working of the proposed scheme description phase.

Results & Discussion:

In this section, we discuss the results that we obtained from the testing environments. Analysis of the proposed scheme with its attributes is also discussed.

Scheme Analysis:

A network protocol analyzing tool is used to examine the proposed scheme known as Scyther [32]. 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. A minimal input file Protocol definitions are the most important parts of a Scyther input file [33]. To validate the system's security, a Network Threat Model [34] is used to verify the proposed, scheme. The following is assumed:

- The attacker has complete or partial control over the network.
- The attacker is resourceful, as detailed in the Dolev-Yao intruder model [35], and can learn, deflect, and generate messages.

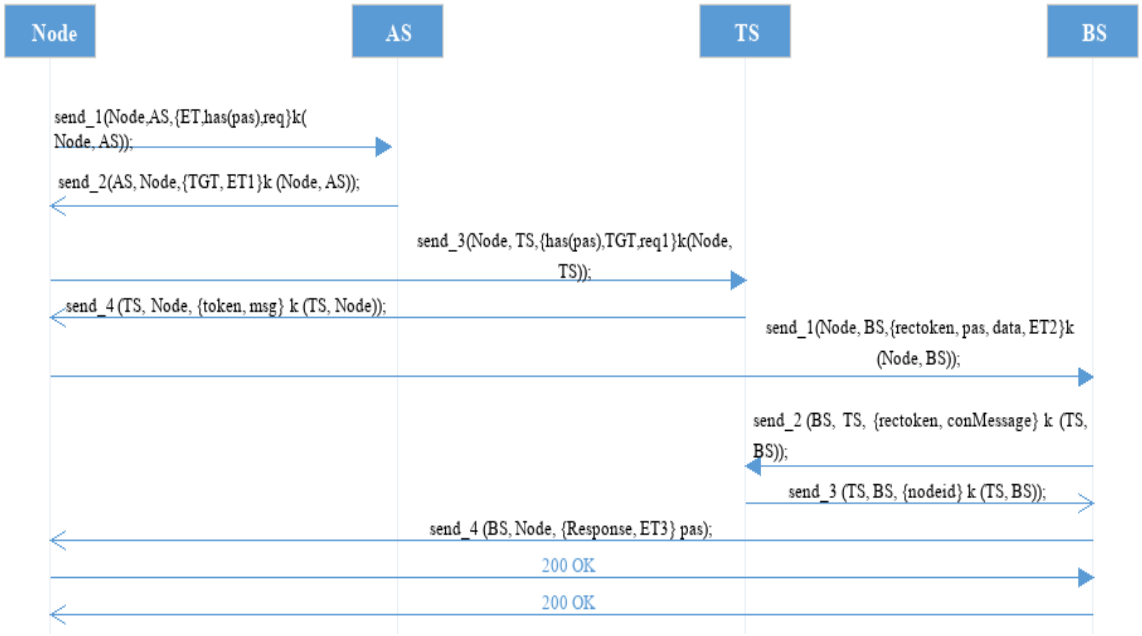

Figure 2. The Sequence Diagram of the Proposed Solution

Scheme Attributes:

In this section, we presented all the important attributes of the proposed scheme in detail. Using these attributes final results are generated at the end. Following is the simple example code for how to define a protocol in Scyther.

```
protocol Example Protocol (I, R) {
role I {};
role R {};
};
```

We have defined a protocol named "Example Protocol" 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 {};
}
```

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.

Scyther Results:

The findings produced by Scyther [33] are shown in Figures 2,3 and 4. 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 is 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.

Figure 3. Scyther Results-1

Figure 4. Scyther Results-2

Discussion:

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. The security of the proposed scheme is tested in the previous section using the Scyther tool and the efficiency of the proposed scheme is tested by comparison with already proposed schemes in [9][24][36].

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 and security, and optimizing 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 Table 2 prove that the proposed scheme is more optimized and optimized.

Numerical Results:

In this research, the proposed authentication scheme is also compared to the approaches presented in [9][24] and [36] to check 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 [37] where the cryptographic methods are implemented in C++, the system specs are an Intel Core2 Duo 1.83 GHz, the CPU is running upon Windows Vista in 32-bit mode and the compiler is Microsoft Visual C++ 2005 SP1.

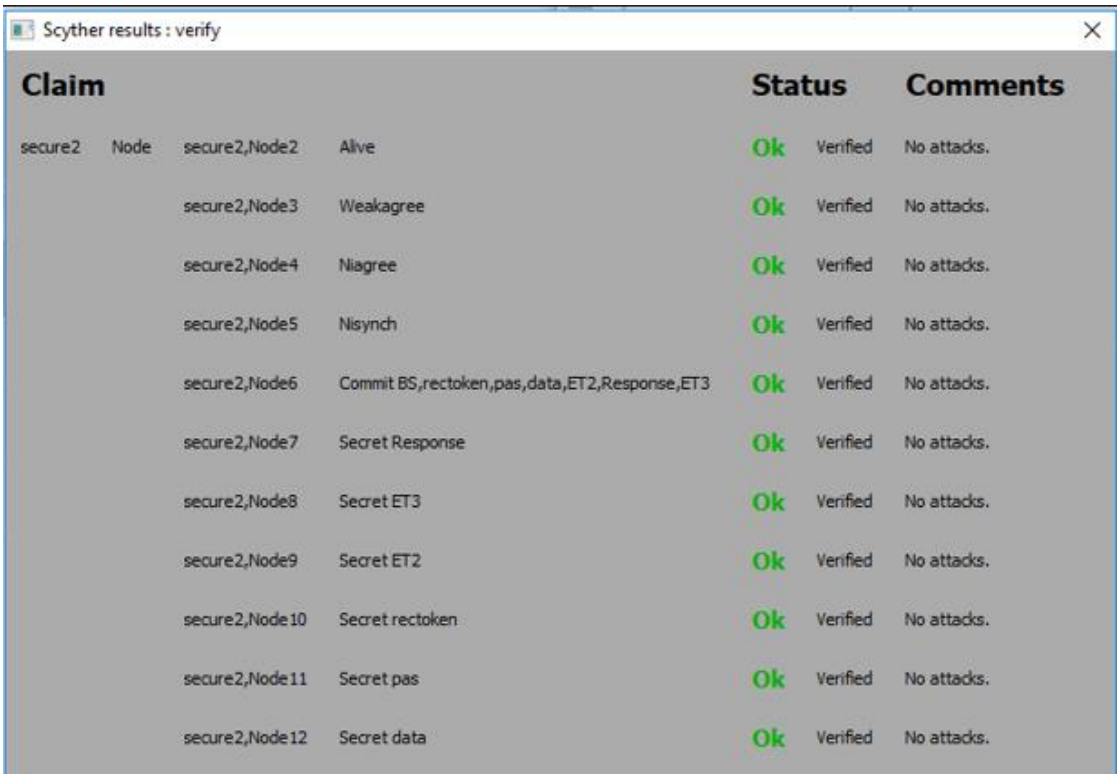

Figure 5. Scyther Results-3

Because authors of the schemes with which comparisons are performed for efficiency also use the same benchmarks for performance evaluation. Because for accurate results the same benchmark is very important. 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 Table 1.

Table 1. 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 [36] and in this study proposed scheme, considering the benchmarks from [37], as presented in Table 2. For completing the

authentication process the proposed schemes in [9][24] and [36] use twenty-four, twenty-nine, and thirty-nine cryptographic primitives respectively.

Table 2. Cryptographic Primitives Count

Cryptographic Primitive	Comparison Schemes			
	[24]	[36]	[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 eighteen primitives are required to complete 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. 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 all the comparison schemes have the same transmission time so for calculation of the authentication delay transmission time was omitted.

According to [37], the time for message encryption with the public key is 0.08ms, the time for message encryption with a symmetric key is 1.8μs, for the message decryption with a public key time is 1.46ms, the message decryption with symmetric key takes 1.8μs, the hashing time using HMAC (SHA-1) is 0.509μs, 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 [36] was 8.02ms and in [9] it was 7.23ms respectively. And the authentication time in the proposed scheme is approximately 27.236 μs or 0.027236ms. These results, it is proof that the proposed scheme is approximately 84%, 66%, and 62% faster in comparison to that in [24] [36] 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. From the future perspective, due to the importance of machine learning (ML) in different fields and network advancement [38][39][40][41][42][43][44] we have planned to work with ML models.

Conclusion:

The proposed scheme revolutionizes secure communication by bypassing the need for public-key cryptography. It introduces an optimized authentication framework, reducing complexity and authentication time while bolstering security for wireless devices. The scheme's extended security features effectively address wireless communication challenges, maintaining minimal requirements for time, power, and memory. Its versatility allows implementation in diverse environments like IoT, smart cities, and more. Future work involves exploring network device hardware for authentication, integrating with PGP and Blockchain, creating secure

mobile apps, and studying its application in continuous authentication for group communication protocols. This scheme's impact spans domains and offers a promising direction for advancing wireless communication security.

References:

[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, Sep. 2019, doi: 10.1145/3337065.

[2] S. Abidin, V. R. Vadi, and A. Rana, "On Confidentiality, Integrity, Authenticity, and Freshness (CIAF) in WSN," Adv. Intell. Syst. Comput., vol. 1158, pp. 87–97, 2021, doi: 10.1007/978-981-15-4409-5_8/COVER.

[3] C. Biswas, U. Das Gupta, and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019, Apr. 2019, doi: 10.1109/ECACE.2019.8679136.

[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, Sep. 2018, doi: 10.1007/S12083-017-0581-5/TABLES/7.

[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, Nov. 2014, doi: 10.1109/TMC.2014.2312715.

[6] A. J. Olaode, "AVAILABILITY OF INFORMATION AND ITS SECURITY MEASURES," СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ, pp. 37–42, 2019.

[7] M. Khasawneh, I. Kajman, R. Alkhudaidy, and A. Althubyani, "A Survey on Wi-Fi Protocols: WPA and WPA2," Commun. Comput. Inf. Sci., vol. 420 CCIS, pp. 496–511, 2014, doi: 10.1007/978-3-642-54525-2_44/COVER.

[8] H. Z. U. K. and H. Zahid, "Comparative study of authentication techniques," Int. J. Video Image Process. Netw. Secur. IJVIPNS, vol. 10, no. 4, 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, Jul. 2017, doi: 10.1109/ACCESS.2017.2723322.

[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, Mar. 2016, doi: 10.1007/S10586-015-0510-4/METRICS.

[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, Jan. 2016, doi: 10.1016/J.PROCS.2016.06.013.

[12] and W. C. L. Zhou, X. Li, K.-H. Yeh, C. Su, "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 time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process," ECCE 2017 - Int. Conf. Electr. Comput. Commun. Eng., pp. 788–793, Apr. 2017, doi: 10.1109/ECACE.2017.7913010.

[14] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," Cryptogr. 2018, Vol. 2, Page 1, vol. 2, no. 1, p. 1, Jan. 2018, doi: 10.3390/CRYPTOGRAPHY2010001.

[15] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT Device Authentication Scheme

Using Device Capability and Digital Signatures," ICAEM 2018 - 2018 Int. Conf. Appl. Eng. Math. Proc., pp. 115–119, Nov. 2018, doi: 10.1109/ICAEM.2018.8536261.

[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, Jul. 2018, doi: 10.1109/TDSC.2016.2605087.

[17] Z. L. 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," 2015 Int. Conf. Work. Comput. Commun. IEMCON 2015, Dec. 2015, doi: 10.1109/IEMCON.2015.7344480.

[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, Jul. 2011, doi: 10.1016/J.ADHOC.2010.08.020.

[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, Nov. 2015, doi: 10.1002/SEC.551.

[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, Sep. 2015, doi: 10.1007/S11334-015-0250-X/METRICS.

[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, Mar. 2018, doi: 10.1007/S10586-017-0886-4/METRICS.

[23] S. Parvin and F. K. Hussain, "Digital signature-based secure communication in cognitive radio networks," Proc. - 2011 Int. Conf. Broadband Wirel. Comput. Commun. Appl. BWCCA 2011, pp. 230–235, 2011, doi: 10.1109/BWCCA.2011.95.

[24] S. Parvin, F. K. Hussain, and O. K. Hussain, "Digital signature-based authentication framework in cognitive radio networks," ACM Int. Conf. Proceeding Ser., pp. 136–142, 2012, doi: 10.1145/2428955.2428985.

[25] A. A.-M. 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," Proc. 2015 Int. Conf. Green Comput. Internet Things, ICGCIoT 2015, pp. 323–326, Jan. 2016, doi: 10.1109/ICGCIOT.2015.7380482.

[27] A. El-Sayed, "Multi-biometric systems: a state of the art survey and research irections," 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, Jan. 2015, doi: 10.1002/DAC.2644.

[29] W. M. AlOmari and H. Abusaimeh, "Modified USB Security Token for User Authentication," Comput. Inf. Sci., vol. 8, no. 3, p. p51, Aug. 2015, doi: 10.5539/CIS.V8N3P51.

[30] A. X. Liu and L. R. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," Comput. Commun., vol. 32, no. 7–10, pp. 1194–1199, May 2009, doi: 10.1016/J.COMCOM.2009.03.006.

[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, Nov. 2018, doi: 10.1109/TIFS.2018.2832849.

[32] and A. P. H. Yang, V. Oleshchuk, "Verifying group authentication protocols by Scyther," J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl, vol. 7, no.

2, pp. 3–19, 2019.
[33] C. Cremers, "Scyther User Manual. 18 February 2014. - References - Scientific Research Publishing," 2014. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/ReferencesPapers.aspx?ReferenceID=1424654 (accessed Sep. 14, 2023).
[34] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, 1983, doi: 10.1109/TIT.1983.1056650.
[35] I. Cervesato, "The Dolev-Yao intruder is the most powerful attacker," 16th Annu. Symp. Log. Comput. Sci., vol. 1, 2001.
[36] 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, Mar. 2015, doi: 10.1007/S11277-014-2115-2/METRICS.
[37] "Speed Comparison of Popular Crypto Algorithms." https://www.cryptopp.com/benchmarks.html (accessed Sep. 14, 2023).
[38] M. T. Ubaid, A. Kiran, M. T. Raja, U. A. Asim, A. Darboe, and M. A. Arshed, "Automatic Helmet Detection using EfficientDet," 4th Int. Conf. Innov. Comput. ICIC 2021, 2021, doi: 10.1109/ICIC53490.2021.9693093.
[39] M. T. Ubaid, M. Z. Khan, M. Rumaan, M. A. Arshed, M. U. G. Khan, and A. Darboe, "COVID-19 SOP's Violations Detection in Terms of Face Mask Using Deep Learning," 4th Int. Conf. Innov. Comput. ICIC 2021, 2021, doi: 10.1109/ICIC53490.2021.9692999.
[40] M. A. Arshed, W. Qureshi, M. U. G. Khan, and M. A. Jabbar, "Symptoms Based Covid-19 Disease Diagnosis Using Machine Learning Approach," 4th Int. Conf. Innov. Comput. ICIC 2021, 2021, doi: 10.1109/ICIC53490.2021.9692986.
[41] M. Mubeen, M. A. Arshed, and H. A. Rehman, "DeepFireNet - A Light-Weight Neural Network for Fire-Smoke Detection," Commun. Comput. Inf. Sci., vol. 1616 CCIS, pp. 171–181, 2022, doi: 10.1007/978-3-031-10525-8_14/COVER.
[42] M. A. Arshed, S. Mumtaz, M. S. Liaqat, and I. Haq, "LSTM Based Sentiment Analysis Model to Monitor COVID-19 Emotion LSTM Based Sentiment Analysis Model to Monitor COVID-19 Emotion," no. May, 2022.
[43] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A Robust Authenticated Key Management Protocol for the Internet of Drones," IEEE Internet Things J., vol. 9, no. 2, pp. 1339–1353, Jan. 2022, doi: 10.1109/JIOT.2021.3084946.
[44] M. Tanveer, H. Alasmary, N. Kumar, and A. Nayak, "SAAF-IoD: Secure and Anonymous Authentication Framework for the Internet of Drones," IEEE Trans. Veh. Technol., 2023, doi: 10.1109/TVT.2023.3306813.

Copyright © by authors and 50Sea. This work is licensed under Creative Commons Attribution 4.0 International License.