ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/364638022

SWINC: Secured Wireless Intelligent Network Using Cryptography

Chapter · October 2022

DOI: 10.1007/978-3-031-19958-5_15

CITATION
1

READS
140

5 authors, including:

Israt Zarin
Uttara University
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Kazi Sazzad Hosen
3 PUBLICATIONS **1** CITATION
SEE PROFILE

Ahsan Ul Islam
Sam Houston State University
3 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Shahadat Hossain
Daffodil International University
22 PUBLICATIONS **13** CITATIONS
SEE PROFILE

All content following this page was uploaded by Israt Zarin on 08 August 2023.

The user has requested enhancement of the downloaded file.

SWINC: Secured Wireless Intelligent Network Using Cryptography

Israt Zarin[1], Onisha Akter[2], Kazi Sazzad Hosen[2], Ahsan Ul Islam[3], and Shahadat Hossain[4(✉)]

[1] Uttara University, Dhaka, Bangladesh
isratzarin@uttarauniversity.edu.bd
[2] American International University-Bangladesh (AIUB), Dhaka, Bangladesh
[3] Sam Houston State University, Huntsville, TX, USA
[4] City University, Dhaka, Bangladesh
hossain_shahadat92@outlook.com

Abstract. According to the International Telecommunication Union, wireless intelligence networks (WINs) are the most significant technology in wireless communication technology in the twenty-first century. Because of the potential applications, it is becoming increasingly influential and appealing. It is becoming a progressively important issue in the automation of homes and factories and environmental monitoring. As a result, this wireless network technology's popularity continues to grow worldwide. Despite this, it has been discovered that the wireless intelligence network does not have proper protection and is vulnerable to hacking attacks. The authentication conundrum is one of them, and it becomes a big issue in wireless security when it is not appropriately addressed. In this study, we propose a model named SWINC (Secured Wireless Intelligent Network using Cryptography) to overcome the uncertainties associated with authentication. The elliptic curve digital signature technique, one of the most well-known and straightforward cryptographic approaches, is included in our proposed solution.

Keywords: Wireless intelligent network (WIN) · Security · Cryptography · Authentication · Elliptic curve digital signature

1 Introduction

The intelligent wireless network is a network that uses smart network capabilities to provide unified human services, personal mobility, and enhanced network services within the cell environment. As a result, the Telecommunications Industry Association (TIA) created WINs with intelligent characteristics. The primary purpose of developing it is to increase flexibility, shorter service conveyance times, functionalities that may be set independently, efficient network intake, stability, rapid service manufacturing, distribution, and delivering a large number of data [1]. The intelligent wireless network has specialized resource capabilities,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
P. Vasant et al. (Eds.): ICO 2022, LNNS 569, pp. 152–161, 2023.
https://doi.org/10.1007/978-3-031-19958-5_15

such as text-to-speech conversion, which can be included for increased efficiency and cost savings. It also uses little electricity and improves network functionality [2]. Everyone nowadays uses mobile phones to connect. As a result, it is critical to secure the mobile environment and protect information. Cryptography is a well-known technology for safeguarding networks, and it is growing in popularity due to mathematical ideas [3]. As encryption is required in many wireless network applications such as digital transactions, electronic commerce, and fingerprint identification, new cryptographic algorithms are developed to provide greater security. There are numerous reasons to choose cryptography, including establishing secure communication, achieving security goals, preserving authentic information, avoiding data threats, denying service, protecting data during transmissions, preventing third-person attacks, etc. Faynberg et al. [4] developed an intelligent model for well-known basic services but can not support supplementary services. A wireless awareness framework for WINs is introduced [5], allowing wireless services to be aware of the presence and properties of wireless channels in the transmission link. Still, they did not clarify the security during transmission.

Some security concerns have been highlighted, and one of the security issues discovered is the authentication problem. It is occasionally overloaded or impossible to prove authentication to many users while providing security [2]. No user authentication is performed when the number of users exceeds the maximum. It raises a security threat to the users' accounts. As a result, users continue to wait while an attacker can enter the network and assault the network system. During that waiting time, many types of attacks, such as a black hole and wormhole attacks, have been carried out [6]. Hardware authentication is both expensive and challenging [7]. That is the reason for resolving the authentication issue. The main focus of this study is on the security difficulties of intelligent wireless networks, and it proposes a method to give security to them by employing a cryptographic algorithm. According to Joselin et al. [8], the digital signature method achieves network security needs such as data integrity, authentication, and non-repudiation. For example, paper-based authentication is accomplished, and new ways are offered based on user authentication by the use of a digital signature [9,10]. Hence, password and image-based authentication had been performed on digital signatures, with excellent results [11,12]. *Elliptic Curve Cryptography (ECC)* outperforms other cryptographic methods [13,14]. Based on prior experimental results, it is evident that the computation time of the Elliptic Curve Digital Signature Algorithm (ECDSA) is faster than that of any other cryptographic algorithm [15,16]. The proposed model in this paper is based on the digital ECDSA handling the authentication problem.

2 Methodology

The digital signature cryptographic approach with elliptic curve cryptography (ECC) is proposed in this study to handle WIN authentication problems. Among the most efficient methods in this field is ECC. The digital signature is utilized

to validate the user in this case. The system must authenticate all users before they may enter it. The ECDSA process is divided into three groups [17].

- Key Generation
- Signing and encryption
- Decryption and signature verification.

On the other hand, the first is concerned with the sender's side, while the second is concerned with the receiver's side.

2.1 Public Key Generation Process

A public key must be produced from a private key in ECDSA [18]. For example, if x is the private key, it will generate a public key. First, choose a number x less than the curve's order n. Then compute P using the formula 1,

$$P = x \times G \tag{1}$$

Here G is the curve generator. ECDSA takes less time to generate the key. The key generation technique is depicted in Fig. 1.

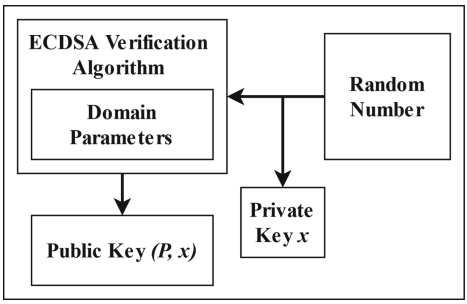

Fig. 1. Key generation process of ECDSA.

2.2 Sender Side

The digital signature is based on keys known as the public-private key pair. When the sender transmits a message, it is encrypted using its private key. The following step is to build a digest message using a hash function. The encrypted message digest is a signed digest or sender's signature. As a result, the receiver receives both the original message and the message digest. Figure 2 depicts the digital signature procedure from the sender's perspective.

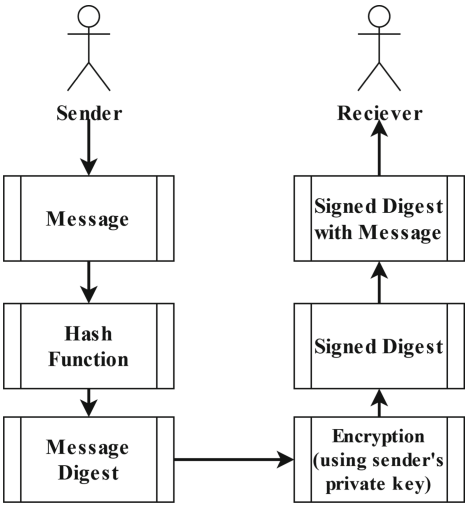

Fig. 2. Digital signature process at sender's side.

2.3 Receiver Side

The receiver decrypts the message digest using the sender's public key after receiving the original message and the message digest. As a result, the Hash function turns the message into a digest message. Then, compare the two message digests. If both messages match, the receiver can validate them. The procedure on the receiver side is depicted in Fig. 3.

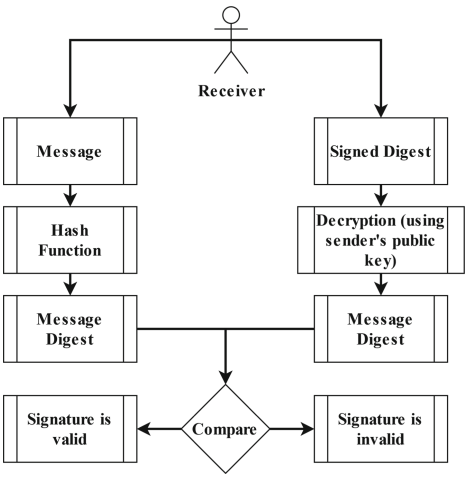

Fig. 3. Digital signature process at receiver's side.

ECDSA takes less time to make a key than Rivest-Shamir-Adleman (RSA). Table 1 shows how long it takes to encrypt ECDSA and RSA, and we see that ECDSA takes less time. ECDSA's key size range is 163 to 571, and RSA's range is 1024 to 15360. So, ECDSA takes less time to figure out the public key than RSA, which takes longer. In addition, when the size grows, the time it takes to make a key in RSA increases. Last, we looked at how long ECDSA took, and RSA took 2029.090 s, so we know that ECDSA is faster than RSA. ECDSA has more advantages than RSA, so that is the case.

Table 1. The computation time required for the key generation of ECDSA and RSA.

Key length (bits)		Computation time (sec)	
ECDSA	RSA	ECDSA	RSA
163	1024	0.219	0.958
233	2240	0.257	1.615
283	3072	0.197	6.122
409	7680	0.224	162.357
571	15360	0.156	2029.909

2.4 Signature Generation Process

The variable length of the message is converted to message digest using the hash function during the signature generation procedure [19]. ECDSA outperforms other encryption algorithms like RSA [15]. When the length of the key is extended, the time required for RSA signature creation increases. Table 2 demonstrates that ECDSA outperforms RSA in signature generation.

Table 2. Signature generation process in ECDSA and RSA.

Key length (bits)		Signature generation time (sec)	
ECDSA	RSA	ECDSA	RSA
163	1024	0.009	0.036
233	2240	0.01	0.037
283	3072	0.01	0.067
409	7680	0.014	0.479
571	15360	0.018	0.015

Table 3. Signature verification process in ECDSA and RSA.

Key length (bits)		Signature verification time (sec)	
ECDSA	RSA	ECDSA	RSA
163	1024	0.0053	0.007
233	2240	0.005	0.004
283	3072	0.008	0.006
409	7680	0.017	0.01
571	15360	0.025	0.015

2.5 Signature Verification Process

The signature verification method determines whether the hashing of the message and the signed message are identical and makes an acceptance or denial decision [18]. ECDSA performs superior in signature verification, according to [13]. Furthermore, the signature verification time for ECDSA is compared to RSA, and we see that ECDSA performs better in signature verification. Table 3 summarizes the experimental results of signature verification performance measurement.

3 ECDSA System Model

The system model primarily explains how ECDSA interacts with WIN for user authentication. It will initially generate a message digest in the sender section. The message and signature message will then be delivered to WIN. Finally, the receiver section checks to see if the message is legitimate. Besides, the signing encodes a random point together into a number which conducts elliptic-curve processes that mainly use the private key and the hash message. The signature verification relates the public key and the message hash to decrypt the number from the signature and return it to its previous point. Figure 4 depicts the overall system model of ECDSA.

4 Proposed Model

The intelligent wireless network is made up of various network and functional components such as service control points (SCP), intelligent peripherals (IP), signal transfer points (STP), Mobile Switching Centers (MSC), Visitor Location Registers (VLR), Home Location Registers (HLR), and so on. Each component is associated with a different service [3]. Amyot et al. [10] describe a network reference model that defines network entities and functional entities. They primarily attempt to match network entities like VLR and HLR to functional entities like service switching points (SSP), service control points (SCP), etc. The previous reference model for WIN is shown in Fig. 5.

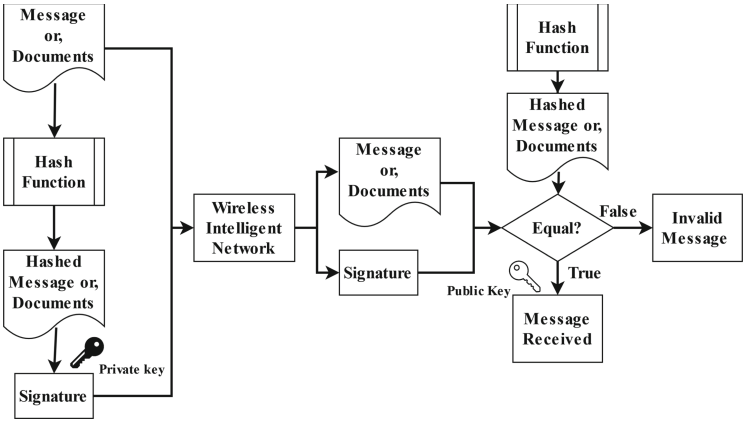

Fig. 4. System model for WIN authentication using ECDSA.

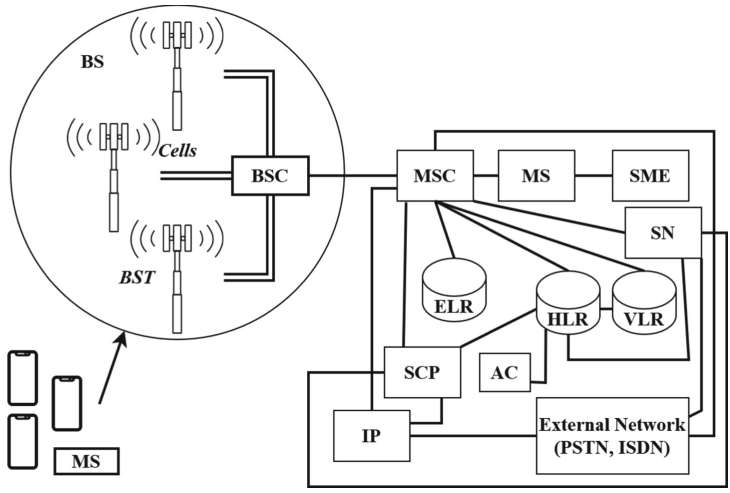

Fig. 5. Existing reference model.

- **Authentication Center (AC):** It primarily controls the Mobile Station's authentication information (MS).
- **Base Station (BS):** A Base Station comprises Base Station Transceivers (BST) and a central station.
- **Equipment Identity Register (EIR):** It is the world's most advanced software solution for recognizing network devices.
- **Home Location Register (HLR):** The location register is related to the user's identification for record-keeping purposes, such as profile information, current location, authorization term, etc.

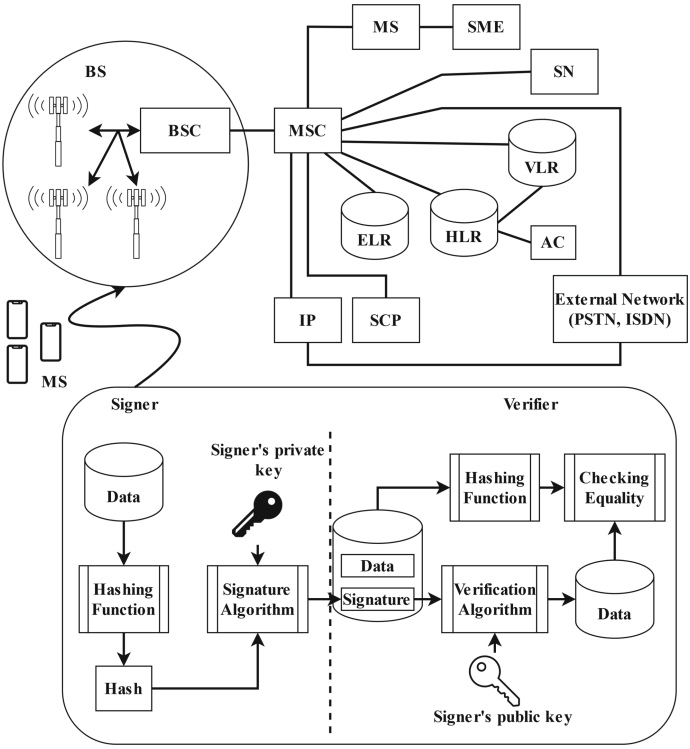

Fig. 6. Proposed model with ECDSA.

- **Intelligent Peripheral (IP):** This includes things like playing announcements, recording and storing voice messages, offering facsimile and data services, and so on.
- **Mobile station (MS):** A mobile station is the user's whole equipment (mobile phone, SIM card, etc.) and software required to connect to a network. It also provides user-side interface devices for terminating the radio link.
- **Mobile switching center (MSC):** An automated system that connects user traffic between a mobile network and other public switched networks or other MSCs within the same or different mobile networks (Fig. 6).
- **Service Control Point (SCP):** It is a virtual node in an intelligent network that contains an activity database with the customer or user data records.
- **Short Message Entities (SME):** This entity is used to compose and dissect messages.
- **Service Node (SN):** It is concerned with service-related activities such as service data, service control, calls, and specialized resources.
- **Visitor Location Register (VLR):** This register retrieves information primarily for handling calls to or from a visiting subscriber.

The security of a key is determined by its length and method. Some methods are more accessible to crack than others, necessitating larger keys to achieve the same level of security. ECDSA takes quite a long time to break through a brute force attack. To break an RSA key, it is needed to factor in a large number. In that case, ECDSA is more effective. ECDSA can provide the same security protection as RSA while using smaller keys. There must be required a few adequate security factors for ECDSA. The mobile station (MS) refers to mobile equipment such as phones, SIM cards, etc. When a user transmits a message, it is routed to the base station, where a base station (BS) acts as a receiver. ECDSA must be configured between MS and BS to overcome the authentication problem. Authentication Center(AC) mainly handles authentication and encryption. The ECDSA sends information to the Authentication Center (AC). The figure depicts our proposed ECDSA approach. We could not run the suggested framework due to insufficient simulation software, components, and WIN setup laboratory.

5 Future Research Direction and Conclusion

In any scientific field, no boundary may be drawn. Our findings bring new aspects to the rule of wireless networks. We provided a strategy for securing the WINs. However, no practical implementations have been carried out in this research, which is one of our respective future efforts for this study.

The intelligent wireless network is one of the most astonishing wireless technology developments. As technology advances beyond our imagination, the problems that arise with technology become far more vital to tackle, except the invention for absolute good can be highly distracting sometimes. Many researchers have offered numerous solutions for resolving the authentication challenge. We have proposed a model named SWINC for dealing with the authentication challenge in WINs using digital signatures. In WINs, the digital signature mechanism can overcome the authentication problem. We hope this study may pave the way for more involuntary research on secured WINs.

References

1. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
2. Al-Turjman, F.: Intelligence and security in big 5G-oriented IoNT: an overview. Futur. Gener. Comput. Syst. **102**, 357–368 (2020)
3. Deng, Z., Tan, X.: Overload control for the wireless intelligent network. J. Netw. **9**(2), 353 (2014)
4. Faynberg, I., Gabuzda, L.R., Jacobson, T., Lu, H.-L.: The development of the wireless intelligent network (WIN) and its relation to the international intelligent network standards. Bell Labs Tech. J. **2**(3), 57–80 (1997). https://doi.org/10.1002/bltj.2066

5. Cheng, L.: Wireless awareness for wireless intelligent network. In: 9th Asia-Pacific Conference on Communications (IEEE Cat. No.03EX732), vol. 2, pp. 561–5642 (2003). https://doi.org/10.1109/APCC.2003.1274420
6. Sevgican, S., Turan, M., Gökarslan, K., Yilmaz, H.B., Tugcu, T.: Intelligent network data analytics function in 5g cellular networks using machine learning. J. Commun. Netw. **22**(3), 269–280 (2020)
7. Aciobanitei, I., CatalinBuhus, I., Pura, M.-L.: Lightweight version of SQRL authentication protocol based on cryptography in the cloud. In: 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), pp. 000173–000178 (2018)
8. Joselin.J, S.J.B., Babu, V.M.: Role of digital signature in network security and cryptography. Int. J. Comput. Sci. Inf. Technol. (IJCSIT) **06**, 893–895 (2015)
9. Finandhita, A., Afrianto, I.: Development of e-diploma system model with digital signature authentication. In: IOP Conference Series: Materials Science and Engineering, vol. 407, p. 012109 (2018)
10. Yassin, A.A., Jin, H., Ibrahim, A., Zou, D.: Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. In: 2012 Second International Conference on Cloud and Green Computing, pp. 282–289 (2012)
11. Elhoseny, M., Shankar, K.: Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Trans. Reliab. **69**(3), 1077–1086 (2019)
12. Terrance, A.R., Sharma, S., Sharma, A., Tyagi, K., Shokeen, N., Saini, N.: In-depth analysis of the performance of RSA and ECC in digital signature application. BLOOMSBURY INDIA 15 (2019)
13. Mahto, D., Yadav, D.K.: Performance analysis of RSA and elliptic curve cryptography. Int. J. Netw. Secur. **20**(4), 625–635 (2018)
14. Rashid, M., Imran, M., Jafri, A.R., Al-Somani, T.F.: Flexible architectures for cryptographic algorithms-a systematic literature review. J. Circ. Syst. Comput. **28**(03), 1930003 (2019)
15. Gressl, L., Rech, A., Steger, C., Sinnhofer, A., Weissnegger, R.: Security based design space exploration for cps. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 593–595 (2020)
16. Genç, Y., Afacan, E.: Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In: 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), pp. 1–6 (2021)
17. Bisheh-Niasar, M., Azarderakhsh, R., Mozaffari-Kermani, M.: Cryptographic accelerators for digital signature based on Ed25519. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **29**(7), 1297–1305 (2021)
18. Kumar, P., Sharma, S.K.: An empirical evaluation of various digital signature scheme in wireless sensor network. IETE Tech. Rev. 1–11 (2021)
19. Toradmalle, D., Singh, R., Shastri, H., Naik, N., Panchidi, V.: Prominence of ECDSA over RSA digital signature algorithm. In: 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 253–257 (2018)

View publication stats