Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 1, January 2019, pg.119 – 124

Three-Factor User Authentication Scheme for WSN

Mercy Jeba Malar P (M.Sc,B.Ed), **Dr. Senthil Kumar** (M.Sc,MPhil,PhD).

MPhil - Computer science, Tamil University, Tanjore, pmjmalar@gmail.com

MPhil - Computer science, Tamil University, Tanjore, erodesenthilkumar@gamil.com

Abstract--- Major revolution takes place in technology today is the digital technology taking over analog technology and converting it into centralized cloud and wireless systems. With the rapid advancements in wireless technology, small devices began to be utilized in almost all parts of various regions in day to day life. These small devices are equipped for sensing, computation and communication. This technological invention is widely known as Wireless Sensor Networks (WSNs). This advanced sensor technology is used in various application scenarios such as environment, agriculture and healthcare too. Wireless sensor networks (WSNs) play a vital role in Internet of Things (IoT) and different types of real time applications such as military surveillance, healthcare monitoring and manufacturing. Although the advancements in WSN, it has security threats. Authentication is the very important part in Wireless Sensor Network (WSN) only authenticated user is allowed to access the real-time sensing information. In this paper we propose an effective and secure three-factor authentication and key agreement scheme for WSN.

Keywords— authentication, key management, privacy, wireless sensor networks, security

I. INTRODUCTION

With the rapid development of wireless sensor technologies, wireless sensor networks (WSN) are used in many fields such as industrial, health care, transportation and military. Fig 1: shows Architecture of internet wireless sensor networks. However, security issue is the major problem in WSN, communications between users and sensor nodes are usually in an open channel, and the hacker can easily steal or modify messages in the WSN. Therefore, the security and privacy of WSNs are questionable. In this scenario WSN must need efficient light weight security system in order to prevent various kinds of networking attacks.

A.WSN ARCHITECTURE AND FUNCTION

Wireless sensor network (WSN) consists of a group of dedicated sensors with a communications infrastructure for monitoring and recording the surrounding conditions and store the collected data into central location. There are

different types of sensors like temperature sensor, acoustic sensor and magnetic field sensor [2][3]. The sensor measures and converts physical phenomenon like heat, light, motion, vibration, and sound into electrical signals. These signals are converted into digital format and sent through internet gateway and then stored in central location for future mining. The more modern Sensors are bi-directional. The most recent wireless sensing networks can be even set submerged and underground. Fig. 1 has shows the architecture of wireless sensor networks.

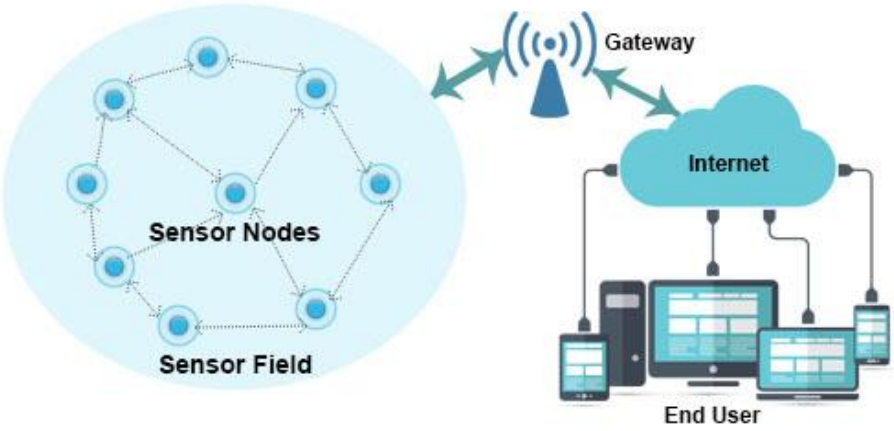

Fig. 1. WSN Architecture

B. ADVERSARY MODEL

Adversary meant to be unauthorized entity, Adversary model refers to the capability of the attacker. It has been used for avoiding the unauthorized entities. Adversary model has the following skills:

- Adversary can easily hack biometric information.
- Adversary has the ability to get the secret key.
- Adversary has the ability to read, modify, edit and delete the secured information.
- Adversary has good ideas about network topologies.

C. Elliptical curve cryptography

Elliptical curve cryptography (ECC) is a public key cryptography based on the algebraic structure of elliptic curves that can be used to create smaller faster and more efficient cryptographic keys[4]. ECC is used for pseudo-random generators, key agreement and digital signatures. ECC generates keys using the properties of the elliptic curve equations. Let p, q be two large primes, and E/Fp indicate an elliptic curve then y 2=x 3+ ax + b over the finite field Fp. We denote by G1 a q-order subgroup of the additive group of points of E/Fp. The discrete logarithm problem (DLP) is required to be hard in G1.

II. LITERATURE REVIEW

In 2009, [5] Das proposed two-factor user authentication protocol for WSN. This method consists of two main parts, Registration phase and Authentication phase. Registration phase is executed when a user wants to register with the WSN. The authentication phase is executed when user wants to perform some query to or access data from the network. Many researchers [6,7,8] identified the security threats and shortcomings in Das's scheme, and then introduced many improved versions.

In 2011, Fan et al. [9] criticized the weakness of previous schemes and designed a new scheme with lightweight operations. With lower computational cost, their method seems to be suitable for a limited resources environment, for example, WSNs. In 2012, Das et al. [10] proposed a novel method which supports the dynamical addition of WSN nodes. Wang et al. [8] identified that the method is vulnerable to many attacks.

In 2013, Xue et al. [12] introduced a new authentication scheme with excellent features and reduced the computational cost. However as it was revealed by Wang et al. [14] proved the proposed method fails to achieve user privacy. Furthermore, Li et al. [13] identified the proposed method is vulnerability to offline dictionary attack,

insider attack, stolen-verifier attack, etc., and proposed a new scheme which still is insecure against offline dictionary attack.

In 2014, Choi et al. [15] showed that a previous scheme [16] undergoes from sensor energy exhausting attack, the session key attack and offline password guessing attack, and then planned a new scheme. After representing the security flaws in Xue et al.'s scheme [12], Jiang et al. [17] also designed an improved one. However, together the scheme of Choi et al. [15] and Jiang et al. [17] were discovered as not being protected as claimed by Wu et al. [17].

In 2015, He et al. [18] termed a temporal-credential-based scheme for WSNs, yet soon was pointed out subject to impersonation attack, tracking attack and smart card lost attack. In the same year, Chang et al. [19] proposed an enhanced dynamic identity authentication, once again, it was proved not safe against offline password guessing attack, user impersonation attack, etc. by Jung et al. [20] and Park et al. [21]. To make stronger the security of the scheme, Jung et al. [20] and Park et al. [21] both added the biological characteristic as a new factor and proposed a three-factor improved version. Furthermore, they both proved the safety of their scheme formally, so they were confident in the security of their scheme.

III. PROPOSED SYSTEM

In this paper we develop lightweight secured protocol for internet integrated WSN by using Eclipse Curve Cryptography. In this case, the encryption and decryption process is very secured and light weight. As this is light weight it is very much suitable for WSN. There are four important modules user registration, server registration, sensor node registration and login. In our proposed work, for three factor authentication we use the following authentication details user credential information (username and password), user biometric information and secret keys. Fig. 2 shows the architecture of the proposed system.

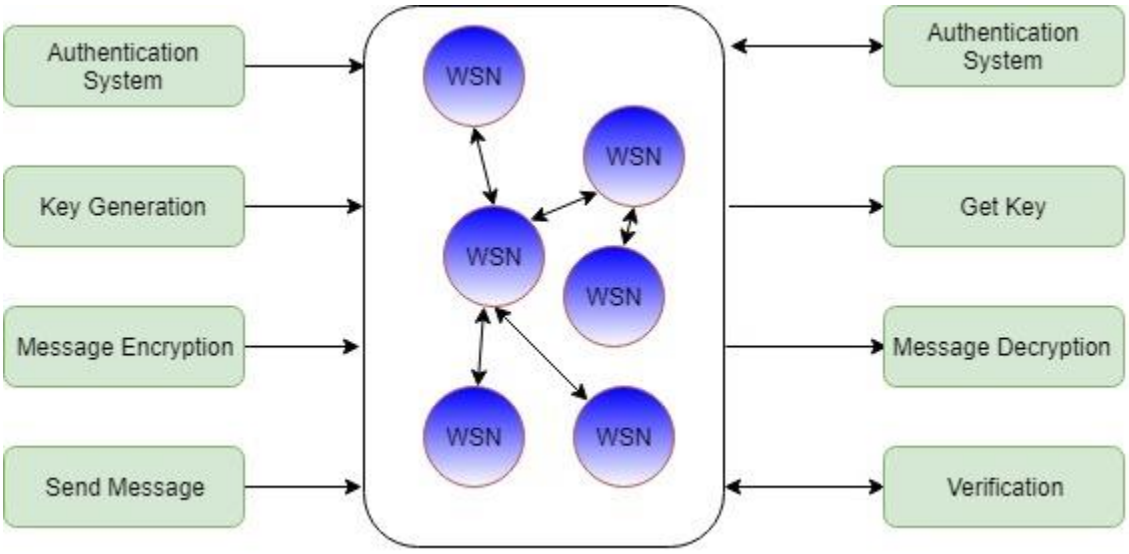

Fig 2 Architecture of proposed work

IV. ANALYSIS AND PERFOMANCE EVALUTION

In this section we evaluate a performance like computational cost and security features with previously proposed methods. The performance evaluation includes Computational coast and security features analysis and Communication performance analysis. The summary of computational comparison shows that our scheme uses only a lightweight hash operation. Where the experiment lays on Windows 10 operating system, Intel i3 3.20 GHz CPU, and 4.0 GB RAM. The running time of H is 0.0359 ms. Fig.3 shows the time consumption for cryptographic operation.

TABLE1 COMPARISON OF COMPUTATIONAL TIME BETWEEN THE PROPOSED SCHEME AND OTHER RELATED SCHEMES

	Proposed Method	**[9]**	**[13]**	**[16]**	**[18]**	**[19]**
User registration	5h	4h	6h	6h	3h	5h
Server registration	-	3h	-	-	-	2h
Sensor node registration	3h	6h	4h	4h	5h	3h
Login and authentication	7h	9h	7h	8h	8h	7h
Total cost	5h+3h+7h	4h+3h+6h+9h	6h+4h+7h	6h+4h+8h	3h+5h+8h	5h+2h+3h+7h
MS	0.534	0.79	0.61	0.65	0.57	0.61

TABLE2 COMPARISON OF SECURITY FEATURES BETWEEN THE PROPOSED SCHEME AND OTHER RELATED SCHEMES

Security Feature	**Proposed Method**	**[9]**	**[13]**	**[16]**	**[18]**	**[19]**
Mutual authentication	Yes	Yes	Yes	No	No	Yes
Key agreement	Yes	Yes	No	Yes	No	Yes
Password protection	Yes	Yes	Yes	Yes	Yes	Yes
Password-change	Yes	No	No	Yes	No	Yes
Dynamic node addition	Yes	No	Yes	No	Yes	Yes
User anonymity	Yes	Yes	No	Yes	Yes	Yes
Replay attack resilience	Yes	Yes	Yes	Yes	Yes	No

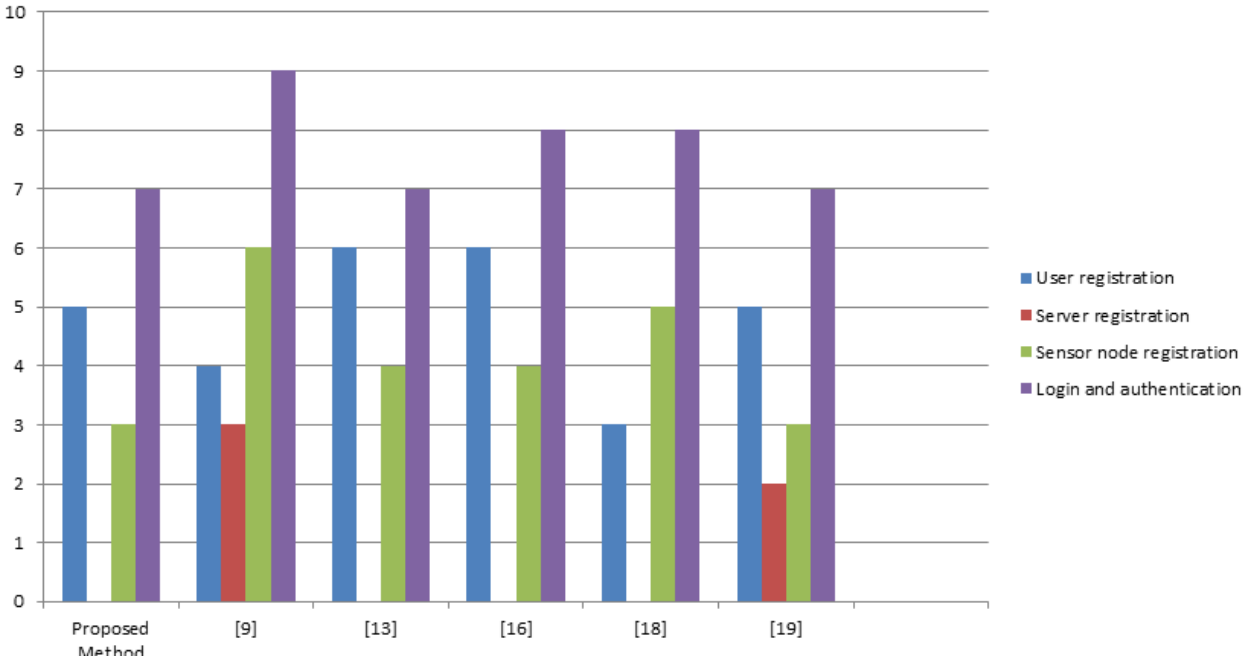

Fig.3 Time consumption for cryptographic operation

V. CONCLUSIONS

In this research paper DOS security authentication scheme where the literature survey shows lots of security problems occurred. These security problems has been completely fulfilled by our proposed protocol. Our Proposed protocol withstands all active and passive attacks.

References

[1] Wireless sensor network, "https://en.wikipedia.org/wiki/Wireless_sensor_network"

[2]. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", Computer Networks., vol. 52, no. 12, pp. 2292-2330, April. 2008.

[3]. A. Flammini and E. Sisinni, "Wireless Sensor Networking in the Internet of Things and Cloud Computing Era", Procedia Engineering., vol. 87, pp. 672-679, 2014.

[4]. Elliptic-curve cryptography, "https://en.wikipedia.org/wiki/Elliptic-curve_cryptography".

[5]. Das M.L. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009;8:1086–1090.

[6]. Lee C., Li C., Chen S. Two attacks on a two-factor user authentication in wireless sensor networks. Parallel Process. Lett. 2011;21:21–26.

[7]. Kumar P., Gurtov A., Ylianttila M., Lee S., Lee H. A strong authentication scheme with user privacy for wireless sensor networks. ETRI J.

[8]. Sun D., Li J., Feng Z., Cao Z., Xu G. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Pers. Ubiquitous Comput. 2013;17:895–905.

[9]. Fan R., He D.P.X.P.L. An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks. J. Zhejiang Univ. Sci. C. 2011;12:550–560.

[10]. Das A.K., Sharma P., Chatterjee S., Sing J.K. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. J. Netw. Comput. Appl. 2012;35:1646–1656.

[11]. Wang D., Wang P. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. Ad Hoc Netw. 2014;20:1–15.

[12]. Xue K., Ma C., Hong P., Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. 2013;36:316–323.

[13]. Li C.T., Weng C.Y., Lee C.C. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors. 2013;13:9589–9603.

[14]. Wang D., Wang P. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Comput. Netw. 2014;73:41–57.

[15]. Choi Y., Lee D., Kim J., Nam J., Won D. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors. 2014;14:10081–10106.

[16]. Jiang Q., Ma J., Lu X., Tian Y. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-Peer Netw. Appl. 2015;8:1070–1081. doi: 10.1007/s12083-014-0285-z.

[17]. Wu F., Xu L., Kumari S., Li X. A new and secure authentication scheme for wireless sensor networks with formal proof. Peer-to-Peer Netw. Appl. 2017;10:16–30. doi: 10.1007/s12083-015-0404-5.

[18]. He D., Kumar N., Chilamkurti N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Inf. Sci. Int. J. 2015;321:263–277. [19]. Chang I., Lee T., Lin T., Liu C. Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks. Sensors. 2015;15:29841–29854.

[20]. Jung J., Moon J., Lee D., Won D. Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks. Sensors. 2017;17.

[21]. Park Y., Park Y. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors. 2016;16:2123 doi: 10.3390/s16122123.

