A Review of Protocols Design in Secure and Efficient Authentication in Wireless Sensor Networks

G. Vijaya Shanthi, K.V.N. Sunitha

Abstract*: Majority of the applications demand confidentiality and integrity of the shared information using Wireless Sensor Networks (WSNs). Key management schemes are one of the core concepts that ensure the security of WSNs. Prior key management schemes failed to provide required security arrangements in WSNs. Authentication is the core parameters that assess the capability of the deployed sensor nodes in the communication fields. In this paper, we review the existing authentication protocols by stating its merits and demerits. It is observed that the need for a secure and efficient authentication protocol is still in demand, owing to the real issues like identity overheads, information retrieval and location mining. This paper will assist the upcoming researchers to have an insight into the significance of lightweight authentication protocols in WSNs.

Keywords*: Wireless Sensor Networks, Authentication protocols, Key management schemes, Security and shared information.

I. INTRODUCTION

Wireless Sensor Networks is defined as the process of low-power wireless communications by combining several numbers of wireless sensor nodes. Each node in the sensors can perform functions like sensing, components, and data processing with limited resource constraints. With these functionalities, different applications like healthcare, military and monitoring systems make use of WSNs for better utilization [1]. Henceforth, resource constraints on energy, susceptibility towards physical data, low computational, and security schemes have to be addressed for taking WSNs into next levels. Most of the conventional cryptographic security protocols are providing limited services in resource-constrained WSNs. In a sensor network environment, the limited network resources make use of asymmetric cryptographic functions that specifically respond to the authorized users, when it is verified by the network initiator. Once after the verification, the secret data is shared via a public channel. In some cases, the responder is not authenticated by the initiator which means that the network environment is more prone to Denial of Service (DoS) [2] attacks. Henceforth, the importance of authentication protocols has been stated by different researchers for autonomous WSNs from different security constraints.

The rest of the paper is arranged as follows: Section II presents the scope of authentication protocols; Section III presents the existing security techniques and its reviews; Section IV presents the comparative analysis of the recently established authentication protocols; Section V presents the conclusion.

II. AUTHENTICATION IN WSNS

This section discusses the different authentication procedures of WSNs. Security of the sessions data is ensured by improving the authentication parameter of security constraints. Authenticating the sensor nodes ensures the confidentiality and validity of the accumulated data from the wireless channel. It also guarantees that authorized users access the sensor data. In the case of heterogeneous environments, multiple times of authentication process occurs [3]. So as to establish multiple sessions, it is essential that the designed protocols should ensure end-to-end security solutions. Different types of authentication models are available according to the wireless network scenario and they are explained as follows:

A. One-way authentication protocols:

One-way authentication is defined as the process of verifying the users based on the certificate issued by the servers. It trusts the users and sends back the secret data along with the issued certificate. It mostly employs a one-way hash function. It is a simpler process that can be computed easily by any network entities. Since the inverse operation is not possible, the chance of resiliency attacks is encountered. It just converts the incoming messages into output data sequences of fixed length. This output sequence is known as the hash value. Along with some coded data and input sequences, the hash functions are stored. The computed hash function should be collision-free i.e either of the parties should not share the same hash functions for two different data sequences.

B. Two-way authentication protocols:

Pertaining to the above protocol, the need for two-way authentication protocols is to minimize the security breaches, if two entities share the same code value for similar messages. Generally, the two-way authentication protocol is defined as the process of securing the data by providing two sorts of credential factors.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author
G Vijaya Shanthi M.Tech*, Department of computer science and Engineering, Rayalaseema university, Kurnool,Andhra Pradesh, India. E-mail: gvshanthi@gmail.com
Dr K.V.N.Sunitha, Department of computer science and engineering, BVRIT Hyderabad College of Engineering for Women Hyderabad, India. E-mail: k.v.n.sunitha@gmail.com

It ensures the privacy of the shared resources and their credentials and is mainly employed for providing control access [4] to the sensitive data systems. It eliminates the attacks related to phishing, password guessing and so on.

C. Three-way authentication protocols:

Three-way authentication protocols are also known as multi-factor authentication protocols. In order to ensure rapid and reliable communication among the network entities, 3-way authentication protocols are employed. Facilitating high-end security by means of voice of a user, hand gestures, biometrics, fingerprints and so on. When a sensor node is employed for communication, the capability of a node is monitored, so as to model the network security constraints.

D. Implicit authentication protocols:

Implicit authentication is an authentication model developed for mobile wireless communication system [5]. In a mobile environment, the behavior of the mobile users is considered for the purpose of analytics. It makes use of machine learning algorithms, so as to derive knowledge about the particular mobile WSNs.

III. VARIOUS AUTHENTICATION PROTOCOLS

This section reviews the existing studies that have developed protocols for effective and secure authentication of wireless sensor networks.

In [6], an anonymous user authentication protocol detected DoS attacks by improving the resilience factors. Privacy of the user is rebuilt by synchronizing the coordination of the participants. Unlinkability property of each sensor node was defined at user-registration phase, remedy phase, and re-loading phase. During the authentication process, a heavy amount of computational and communication overheads occurs. In [7], anonymity preserving three-factor authenticated key exchange protocols were designed using the Internet of Things (IoT). Previous security models did not preserve the security attributes like identity change and the smartcard revocation phases. Storage cost of the key exchange protocols is 640 bits. Network lifetime of the sensor nodes is not guaranteed.

In [8], the authors have stated the significance of key management protocols for hierarchical IoT networks. In some cases, users need to communicate directly with the real-time data and thus, a lightweight user authenticated key management protocols were designed with security attributes like user smart card id, password and personal biometrics. Each user is verified by the real – or – random model. Finally, Automated Validation of Internet Security Protocols and Applications tools was used for validating the formal and informal security schemes. The system has achieved 2592 bits total cost, which is quite better than prior schemes.

In [9], user authentication and key agreement schemes were re-designed to achieve resource-constrained sensor nodes by detecting password guessing attacks and sensor node spoofing attacks. Here, a third gateway node was established between the sensor entities that assured the reduced leakage of identity and their sensitive data. Even in an insecure channel, the system maintained the same security schemes. Performance metrics such as end-to-end delay and throughput were analyzed for limited sensor nodes. As throughput rate increases, the utilization of the sensor nodes was also properly allocated. When compared to previous schemes, the suggested security schemes have achieved 58 bytes storage costs. Since some security schemes were unpublished, limited constraints were set to security modelling.

Lightweight certificateless authentication protocols with the assistance of cloud systems were explored in [10]. Due to limited storage power delivered by WSNs, cloud models were incorporated, to devise the storage systems in terms of information privacy and authentication protocols. Cloud network manager was combined with the sensor entities that have prevented unauthorized parties. Time taken for implementing the cloud services and its computational cost were analyzed. Results stated that the system can accommodate a larger number of users with the same computational costs. Similar study was extended by [11] under multi-gateway based WSNs. Lightweight security schemes were designed using BAN logic that ensured mutual authentication and the validated session keys. It was implemented in the AVISPA tool, which ensured the energy efficiency of the sensor nodes. It gradually decreased communication and computation costs. The resiliency of the security protocols under a dynamic environment is not assured. The author in [12] explored the lightweight security mechanisms for the industrial wireless sensor networks. Thus, a secured mutual authentication protocol was designed for improving the privacy of the industrial sensor networks. Security in the physical layer was improved by cryptographic primitives like hash function, unclonable function and the bitwise exclusive (XOR) operations. Storage cost is not analyzed due to complex hash operations. In some cases, the behavior of attacks changes during cloning attacks, which is also not analyzed. Two-factor authentication schemes were studied by [13] for Industrial Wireless Sensor Networks (IWSNs). The study has devised the prior schemes stated by Wu et al, 2017 & Srinivas et al, 2017. Some security schemes have lowered the functions of the traditional security parameters. The system failed to detect sensitive information.

The author in [14] explored the three-factor anonymous security scheme for IoT environments. Node's efficiency and security of the IoT environment is always a challenging task.

Since biometric information is utilized as security constraints, the authentication process becomes a little trickier and makes an efficient system. Along with this, the fuzzy commitment scheme was suggested for all types of sensory data. The password authentication process is also designed for eliminating the attacks. Compared to prior security schemes, the suggested security schemes removed the higher communication costs for even smaller bits. This scheme is not applicable to the grid area networks. In [15], the authors have instantiated the lightweight three-factor authentication schemes for Internet Integrated WSNs. Here, Rabin cryptosystem was employed for computational symmetrical algorithms. ProVerif protocols were designed to atisfy all the security features of all types of attacks.

Though the scheme ensured the security and efficiency, untraceability and linkability in heterogeneous environments are not established.

IV. COMPARATIVE ANALYSIS

Finally, a comparative table is developed based on the studies discussed above. The studies are compared based on the objectives, protocols developed, applications, results obtained, merits and demerits. The research gaps including future work can be inferred from the comparative table given below.

Table 1: Comparative Analysis

Reference	Objectives	Developed Protocols	Applications	Resulted obtained & Merits	Demerits
[16]	To develop trust and energy-aware secure routing protocols.	Trust and Energy-aware Secure Routing Protocol (TESRP)	Large-scale and small-scale networks	Composite Route Function (CRF) metric that computed the cost of the introduced protocols by calculating trust, energy and hop count. Systems have achieved high throughput due to trusted nodes. Compared to prior routing protocols, TESRP drops 30% packets for 10 faulty nodes	Under heavy network loads, the lifespan of the network is guaranteed. When the network path length is longer than usual, then more route requests are initiated.
[17]	To develop anonymous key exchange authentication protocols.	Elliptic Curve Cryptography based key authentication protocols	Military and healthcare monitoring services.	Reduced communication and computation costs are achieved for packet length of 32 and 64 bits.	Symmetric keys are corrupted and thus, data is being compromised by an adversary. Higher Computation resources are consumed.
[18]	To introduce a novel digital signature schemes using data authentication protocols	Efficient cluster-based security protocols	Tracking based applications	End-to-End data authentication is possible. Random node capture attack is detected with higher probability. In imote2 devices, Signature verification takes 2.86mJ and 3.51mJ with running at 104MHz.	Computational load on storing keys is higher for cluster heads.

[19]	To detect the session key disclosure attacks by three factor authentication models.	Biometric based authentication scheme using Chebyshev chaotic map	Remote monitoring applications	Suggested protocols satisfied the attacked properties such as user anonymity, desynchronization, forgery, impersonation, temporary information hacking and the forward secrecy. Communication overheads are 2048 bits and time taken 157.16 ms which are quite better than prior schemes.	If the network size increases, then the mutual authentication violates the basic criteria. It leads to heavy computational costs.
[20]	To detect various known attacks by a novel authentication schemes with the extension of (Chang et al) security schemes	Password based user authentication protocols; Anonymity based authentication protocols	Heterogeneous knowledge mining applications	Detected attacks like smartcard stolen attacks, offline identity guessing attacks, untraceability, off-line password guessing attack, user impersonation attack, gateway node impersonation attack, sensor node impersonation attacks, insider attacks, session keys computation attacks and session specific information attacks. Storage and communication costs estimation of proposed protocols has yielded 384/512 bits (SNCS); 896/768 (UECS) and 1280/1280 (GWN).	Higher communication costs due to the properties of traceability and session key verification process.
[21]	To ensure a novel key distribution scheme using Elliptic Curve Cryptography.	Key distribution protocol		22 sec setup time is taken. It can work with different mote sensor applications. Packet overhead decreases, even data size increases.	Vulnerabilities of different security schemes are not assessed.

[22]	To develop a secured authentication protocols by detecting session specific information attacks, late detection of message replay, forward secrecy attacks, and backward secrecy attacks	Three factor authentication schemes	Healthcare applications	Legitimacy of the users is assured by the mutual authentication process. Time taken for authenticating 54 users is 69.68 ms.	Anonymity of the users is not guaranteed within a stipulated period of time. Different users can have different retrieved keys that take a high computational verification process.
[23]	To develop secured key authentication protocols by eliminating the attacker's activities.	Biometric based authentication and key agreement protocols		Computational biometric keys have limited collision resistance properties. Computational cost of 29.9432 ms is achieved.	High data collision occurs even for smaller bits. Forward secrecy is not assured, when the biometric keys are compromised.
[24]	To compare three authentication protocols and its computation benefits for WSNs.	Lightweight authentication protocols		Computation key size is reduced for the registration phase. Use of Diffie Hellman based keys has enhanced the security strength.	Limited resistance towards defending the password guessing attacks.
[25]	To develop a self-heal key management system for enhanced forward and backward security transmission.	Implicit authentication protocols based on Elliptic Curve Qu Vantone (ECQV) algorithm		Computational cost of each sensor node under these protocols takes 4 multiplication operators + 3 addition operation + 1 hash operation at 2 rounds.	As nodes increase, the performance of security schemes are reduced.

From the comparative table, the research challenges that still exists in authentication protocols are described as follows:

a) Sensor nodes have lowered computational power, restricted memory, and lowered bandwidth for wireless communications.

b) Due to the wireless environment, the messages are mostly transmitted at a smaller length.

c) Identity overhead: In large-scale environments, multiple nodes are deployed for a reliable communication process. It is observed that some sensor nodes share the similar global address that buzzes the receiver. Henceforth, global addressing schemes needs to be addressed.

d) Location mining: Location is one of the vital parameters in WSNs. Authorized network entities should be aware of its neighboring nodes, so as to eliminate the redundant data. In security aspects, an anonymous node may violate the security constraints by knowing its location. Hence, location aware routing protocols need to be designed. e) Information retrieval: In recent days, services in WSNs are combined with other recent technologies like cloud, IoT, edge computing etc. Aligning with multiple data sources may depletes the energy consumption rate that can bring resource provisioning issues.

V. CONCLUSION

This paper is a review of different authentication protocols in Wireless Sensor Networks (WSNs). Authentication is one of the security parameters in WSNs environment. Robust and reliable communication is possible only when the network entities are mutually communicated in wireless medium. Here, several techniques related to authentication systems are collected and reviewed by stating its merits and demerits. It is observed that mutual authentication enables the network function to eliminate the security related attacks. Since a tremendous amount of data is being shared using wireless medium, an end- to – end security has to be given for all entities presented in WSNs. From the reviews, we can understand the significance of designing authentication protocols and the need for eliminating the issues related to identity overheads, location mining and information retrievals.

REFERENCES

1. Yuan, D., Kanhere, S. S., & Hollick, M. (2017). Instrumenting Wireless Sensor Networks—A survey on the metrics that matter. Pervasive and Mobile Computing, 37, 45-62.W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
2. Chowdhury, T. J., Elkin, C., Devabhaktuni, V., Rawat, D. B., & Oluoch, J. (2016). Advances on localization techniques for wireless sensor networks: A survey. Computer Networks, 110, 284-305.
3. Ramson, S. J., & Moni, D. J. (2017, February). Applications of wireless sensor networks—A survey. In 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT) (pp. 325-329). IEEE.
4. Radhappa, H., Pan, L., Xi Zheng, J., & Wen, S. (2018). Practical overview of security issues in wireless sensor network applications. International journal of computers and applications, 40(4), 202-213.
5. Hari, P. B., & Singh, S. N. (2016, April). Security issues in Wireless Sensor Networks: Current research and challenges. In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring) (pp. 1-6). IEEE.
6. Gope, P., Lee, J., & Quek, T. Q. (2016). Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks. IEEE Sensors journal, 17(2), 498-503..
7. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Computer Networks, 101, 42-62
8. Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2017). Design of secure user authenticated key management protocol for generic iot networks. IEEE Internet of Things Journal, 5(1), 269-282.
9. Kumari, S., Das, A. K., Wazid, M., Li, X., Wu, F., Choo, K. K. R., & Khan, M. K. (2017). On the design of a secure user authentication and key agreement scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience, 29(23), e3930.
10. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106, 117-123
11. Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 36, 58-80.
12. Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE transactions on industrial informatics.
13. Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics, 14(9), 4081-4092.
14. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K. K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 103, 194-204.
15. Jiang, Q., Zeadally, S., Ma, J., & He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access, 5, 3376-3392.
16. Ahmed, A., Bakar, K. A., Channa, M. I., & Khan, A. W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Networks and Applications, 21(2), 272-285
17. Zhang, K., Xu, K., & Wei, F. (2018). A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks. Wireless Communications and Mobile Computing, 2018.
18. Ferng, H. W., & Khoa, N. M. (2017). On security of wireless sensor networks: a data authentication protocol using digital signature. Wireless Networks, 23(4), 1113-1131.
19. FeiFei Wang., Guoai Xu., & Guosheng Xu (2019). A Provably Secure Anonymous Biometrics-Based Authentication Scheme for Wireless Sensor Networks Using Chaotic Map. IEEE access, 2019.
20. Amin, R., Islam, S. H., Kumar, N., & Choo, K. K. R. (2018). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. Journal of Network and Computer Applications, 104, 133-144
21. Louw, J., Niezen, G., Ramotsoela, T. D., & Abu-Mahfouz, A. M. (2016, July). A key distribution scheme using elliptic curve cryptography in wireless sensor networks. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN) (pp. 1166-1170). IEEE
22. Renuka, K., Kumari, S., & Li, X. (2019). Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare. Journal of medical systems, 43(5), 133.
23. Srinivas, J., Mishra, D., Mukhopadhyay, S., & Kumari, S. (2018). Provably secure biometric based authentication and key agreement protocol for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 9(4), 875-895.
24. Li, W., Li, B., Zhao, Y., Wang, P., & Wei, F. (2018). Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks. Wireless Communications and Mobile Computing, 2018
25. Shen, J., Chang, S., Liu, Q., Shen, J., & Ren, Y. (2018). Implicit authentication protocol and self-healing key management for WBANs. Multimedia Tools and Applications, 77(9), 11381-11401

AUTHORS PROFILE

G Vijaya Shanthi received her B.Tech (Computer Science & Engineering) degree from Vigna's Engineering College, Guntur and M.Tech (Computer Science & Technology) degree from GIET, Rajahmundry, JNTUK University. She worked as Assistant Professor at various engineering colleges in Hyderabad.She has 13 years of teaching experience. She is currently a research scholar at the Department of Computer Science and Engineering, Rayalaseema University, Kurnool, Andhra Pradesh, India. Her area of interest includes Network Security, Artificial Intelligence, Neural Networks, Data Warehousing & Data Mining.

Dr. K.V.N Sunitha, M.Tech, Ph.D. 26 years of Teaching Experience as Professor of CSE Dept. She is currently working as Principal in BVRIT Hyderabad College for women. Guided many UG, PG and Ph.D projects as supervisor. Published several papers in international and national journals. Research areas include Natural language Processing, Speech processing, Image Processing, Network & Web Security, Grid Computing.