A REVIEW ON WIRELESS SENSOR NETWORK

Baibaswata Mohapatra, Professor & Dean, Department of Electronics, Electrical and Communications, Galgotias University

ABSTRACT

Due to its unsupervised and hostile deployment in the field, user authentication in wireless sensor networks (WSNs) is a key security challenge. Due to the limited computer power, storage capacity, and communication modules available on sensor nodes, authenticating distant users in such resource-constrained systems is a critical security challenge. M.L. Das has suggested a two-factor user authentication technique for WSNs, claiming that it is safe against a variety of attack types. However, we demonstrate in this work that the M.L. Das-scheme has many serious security flaws and so cannot be recommended for use in real-world applications. We point out that his approach does not allow users to modify or update their passwords, lacks mutual authentication between the gateway and sensor nodes, and is subject to gateway node bypassing and privileged-insider attacks. To address the M.L. Das-intrinsic scheme's security flaws, we suggest enhancements and security updates that address the scheme's vulnerabilities. The suggested security enhancements may be integrated into the M.L. Das-scheme to provide more secure and robust two-factor user authentication in WSNs.

KEYWORDS: WSN, SENSORS, Security Challenges.

INTRODUCTION

Wireless sensor networks (WSNs) have arisen as a highly active research area in light of recent advancements in communication technology. WSNs have several characteristics with wireless ad hoc networks and are often considered a subset of them [1]. A WSN is often composed of a large number of autonomous sensor nodes that are left unattended. Each sensor node has some computer power, a limited amount of storage, and a tiny communication module for communicating with the outside world through an ad hoc wireless network [2]. WSNs are extensively employed in a variety of applications, including military, combat, homeland security, healthcare, environmental monitoring, agricultural and crop production, and industry.

Security is crucial since the sensor network may be operating in a hostile setting, such as a combat battlefield. During the implementation of WSN, robust solutions are required to enable low-latency, resilient, and secure networks. Additionally, the network should be secure against intrusions and spoofing assaults [3]. Access control is a critical cryptographic fundamental upon which all other cryptographic primitives are constructed. A WSN should be intelligent enough to discriminate between legitimate and unauthorised users, posing the issue of user authentication [3]. If a WSN is implemented for a highly secure application, the data acquired by the sensors is important and should be restricted to registered or authorised users. Benenson et al. developed the concept of n-authentication and outlined the security concerns associated with user authentication in WSNs [4]. Later, Watro et al. introduced a TinyPK authentication system using public key cryptography and RSA and Diffie-Hellman algorithms. [5], however, this protocol is vulnerable to a masquerade sensor node attack, which allows an attacker to impersonate the user.

Wong et al. suggested a lightweight dynamic user authentication system for use in a wireless sensor network setting in 2006. They validated their scheme via a security and cost analysis and examined implementation challenges, emphasising the need of using the IEEE 802.15.4 MAC sublayer's security capabilities. Tseng et al. later uncovered security flaws in Wong et almethod, .'s which preclude its use in real-world contexts. They demonstrated that Wong et alapproach .'s is vulnerable to replay and forgery attacks, that passwords are readily exposed by any of the sensor nodes, and that users cannot change their passwords freely. To address these inconsistencies, Tseng et al. proposed an enhanced scheme, claiming that their scheme not only retains the benefits of Wong et alscheme, .'s but also adds the following features: resistance to replay and forgery attacks, reduction of password leakage risk, and improved efficiency of changeable passwords. T.H. Lee recently performed an analysis of Wong et almethod .'s and suggested two simple dynamic user authentication protocols that are variants of Wong et almethod. .'s T.H. Lee simplified the authentication procedure in his initial protocol by decreasing the computing burden on sensor nodes while maintaining the security level achieved by Wong et al. T.H. Lee, on the other hand, presented a mechanism in his second protocol that prevents an intruder from impersonating the gateway node and granting access to unauthorised users.

While L.C. Ko demonstrated that Tseng et alapproach .'s accomplishes some more security features over Wong et alapproach, .'s it remains vulnerable under a plausible attack scenario. L.C. Ko explained how Tseng et alsystem .'s lacks mutual authentication between the Gateway node (GW) and the Sensor node (SN), as well as between the User (U) and the SN. Additionally, L.C. Ko demonstrated that an attacker may falsify communication messages delivered between sensor nodes and gateway nodes.

As a result, L.C. Ko suggested a modified scheme that seeks to address the security shortcomings of Tseng et alprotocol .'s and shown that his method has superior security characteristics than Tseng et alscheme.'s .

Binod et al. performed a cryptanalysis of Wong et aland .'s Tseng et alauthentication .'s techniques and offered a better technique. Binod et al. demonstrated that their scheme is more resilient than previously published schemes and can survive replay attacks, forgery attacks, and man-in-the-middle attacks. Additionally, their approach allows mutual authentication between the login and gateway nodes.

M.L. Das recently presented a strategy for two-factor user authentication in WSNs. M.L. Das also uncovered a vulnerability in Wong et alprotocol .'s to a multiple logged-in users with the same login-id threat, which means that anybody with a valid user's password may simply access to the sensor network. He also uncovered a vulnerability in Wong et alprotocol's to a stolen-verifier attack, since the GW-node and login-node retain the lookup table for all registered users' credentials. As a result, M.L. Das developed his technique to address the scheme's security weaknesses. His approach employs a two-factor authentication concept based on a password and a smart card and is resistant to attacks such as multiple logged-in users sharing the same login identity, stolen-verifier, guessing, replay, and impersonation.

More recently, Nyang and Lee demonstrated that the M.L. Das protocol is vulnerable to offline password guessing attacks, sensor node compromise attacks, and does not protect query response messages by establishing a unique secure channel from the sensor node to the user, which is a critical component of serving a registered user securely and legitimately. As a result, Nyang and Lee devised a better two-factor authentication technique for WSNs that seeks to address the anomalies they discovered in the M.L. Das approach.

However, we demonstrate in this work that the M.L. Das-scheme is still insecure and subject to a number of serious security threats. Along with the issues identified by Nyang and Lee, we demonstrate that the M.L. Das-scheme is defenceless against GW-node bypass attacks, lacks mutual authentication between GW- and sensor nodes, is vulnerable to insider attacks, and lacks provision for changing or updating registered user passwords. We offer security enhancements in this article to address the aforementioned flaws of the M.L. Das-scheme. Our upgraded security patch includes secure capabilities for changing or updating user passwords, protects against insider attacks, defeats GW-node bypass attacks, and establishes mutual authentication between the GW-node and sensor node. The suggested security enhancements may simply be integrated into the M.L. Das-scheme, enabling WSNs to benefit from more secure and robust two-factor user authentication.

CONCLUSION

We have shown in this article that a recently suggested two-factor user authentication system in a WSN context is vulnerable against a variety of attack vectors and should not be utilised in real-world applications. We have showed that the M.L. Das-scheme does not allow users to modify or update their passwords, that it is sensitive to GW-node bypassing attacks, that it lacks mutual authentication between the GW-node and sensor node, and that it is vulnerable to privileged-insider attacks. To address the aforementioned weaknesses, we have offered security updates and enhancements that address the M.L. Das-weak scheme's points. The proposed security enhancements may simply be included into the M.L. Das-scheme to provide a more secure and robust two-factor user authentication mechanism in WSNs.

REFERENCES

1. Adinarayana, J., Sudharsan, D., & Tripathy, A. K. (2009). Rinfol - A one stop information system for rural development - A prototype. *ASABE - 7th World Congress on Computers in Agriculture and Natural Resources 2009, WCCA 2009*, 440–446. https://www.scopus.com/inward/record.uri?eid=2-s2.0-72749104945&partnerID=40&md5=e64d082e454bdce4a6b04be48db9db7a

2. Junfeng, T., & Anyuan, D. (2010). An IEB-oriented ITS model combined data mining with 3S technologies. *CCTAE 2010 - 2010 International Conference on Computer and Communication*

Technologies in Agriculture Engineering, *2*, 316–319. https://doi.org/10.1109/CCTAE.2010.5543340

3. Sabri, N., Aljunid, S. A., Ahmad, R. B., Malek, M. F., Yahya, A., Kamaruddin, R., & Salim, M. S. (2012). Smart prolong fuzzy wireless sensor-actor network for agricultural application. *Journal of Information Science and Engineering*, *28*(2), 295–316. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84859059512&partnerID=40&md5=26bb7701c25afd350f8a2104459c4c73

4. Rathore, M. M., Ahmad, A., Paul, A., Wan, J., & Zhang, D. (2016). Real-time Medical Emergency Response System: Exploiting IoT and Big Data for Public Health. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0647-6

5. Ray, P. P. (2014). Home Health Hub Internet of Things (H3IoT): An architectural framework for monitoring health of elderly people. *2014 International Conference on Science Engineering and Management Research, ICSEMR 2014*. https://doi.org/10.1109/ICSEMR.2014.7043542

6. Shi, Y., Ding, G., Wang, H., Eduardo Roman, H., & Lu, S. (2015). The fog computing service for healthcare. *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare, Ubi-HealthTech 2015*, 70–74. htt

7. Tyagi, S., Agarwal, A., & Maheshwari, P. (2016). A conceptual framework for IoT-based healthcare system using cloud computing. In S. A. Bansal A. (Ed.), *Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence 2016* (pp. 503–507). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CONFLUENCE.2016.7508172

8. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access*, *5*, 26521–26544. https://doi.org/10.1109/ACCESS.2017.2775180

9. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal*, *2*(6), 515–526. https://doi.org/10.1109/JIOT.2015.2417684

10. Chen, M., Wan, J., & Li, F. (2012). Machine-to-machine communications: Architectures, standards and applications. *KSII Transactions on Internet and Information Systems*, *6*(2), 480–497. https://doi.org/10.3837/tiis.2012.02.002

11. Doukas, C., & Maglogiannis, I. (2012). Bringing IoT and cloud computing towards pervasive healthcare. *Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012*, 922–926. https://doi.org/10.1109/IMIS.2012.26