Protocol for Two-factor Authentication in Wireless Sensor Networks

K Hima Bindu[1] and T Mounica Reddy[2]
Department of Electronics and Communication Engineering, MRCOE, Hyderabad
[1]Corresponding Author: himabinduece@gmail.com

To Cite this Article
Hima Bindu and Mounica, "Protocol for Two-factor Authentication in Wireless Sensor Networks", Journal of Innovative Research in Engineering Technology and Management Science, Vol. 01, Issue 03, July 2025, pp:18-19.

***Abstract**: As critical applications in such areas as health care and security are increasingly using wireless sensor networks (WSNs), the need to control access to the networks securely is becoming increasingly important. Since there exists a risk of the device being penetrated, or the password stolen, more often than not, such traditional single-factor authentication methods are no longer adequate. The two-factor authentication (2FA) approach that this piece of work proposes is a technique that integrates knowledge by a user (a password or PIN) and something possessed by the user (smart device or token). It is identified that the proposed protocol has lightweight functionality which is suitable in resource-constrained scenarios and also ensures establishment of a secure communication between users and sensor nodes. These consist of session key agreement, mutual authentication, and security against common attacks, such as, impersonation, replay and man-in-the-middle. The simulation results demonstrate that the protocol can be applied to enhance authentication in modern WSN applications as it secures provision of and efficiency in the process increased.*

***Keywords**: Wireless sensor networks, Cryptanalysis, Vulnerability analysis*

I. Introduction

Wireless Sensor Networks (WSNs) have now become an important necessity to numerous applications including, smart homes, health, military applications, and environmental monitoring. Such networks consist of spatially distributed sensor nodes wirelessly communicating with each other and collecting and transmitting data. It is possible that WSNs are prone to various security threats, the greatest option being unauthorised access, since they are installed in open and often unprotected environments. Password-only authentication protocols are bad because they can be replayed, guessed and stolen. Two-Factor Authentication (2FA) has gained reputation as a safer alternative to those difficulties, given that it uses at least two different authentications, most often something a user knows (such as a password) as well as something a user possesses (such as a smart card or smart phone). To provide safe authentication to the users with a minimum overhead and against the common security challenges, the proposed study considers a lightweight 2FA protocol that fits the limited computational and energy consumption of WSNs [6].

II. Review on Authentication Protocol

Two-factor authentication (2FA) protocols have gained credit as an input to enhancing access control systems, particularly in resource-constrained environments such as wireless sensor networks(WSNs). In order to enhance security, 2FA protocols, instead of traditional single factor schemes combine two distinct authentication schemes, typically a possession factor (such as a smart card or mobile telephone) and a knowledge (such as a password or a PIN). It is a multi-layered approach, in case one of the factors is compromised, one less tool is available to the attackers to use. Some attempts have been made, in the endeavor to reach a compromise between security and efficiency, proposing lightweight 2FA mechanisms designed specifically to WSNs. These protocols often exploit cryptographic technology to form the secure session keys and bi-directional authentication between a user and sensor nodes as hash functions, elliptic curve cryptography, or key agreement protocols. With 2FA, the security of a WSN is improved significantly, but additional disadvantages are also present, such as increased processing load, energy consumption and more complex key management. An intelligent 2FA mechanism should hence minimize such overheads and ensure safety. What the present study seeks to do is optimise authentication technology in terms of

scalability, real time, and compatibility with emerging technologies including the Internet of Things. In any case, 2FA remains necessary and evolving component of secure WSN implementation.

III. Crypt Analysis

Cryptanalysis of Two-Factor Authentication (2FA) protocol involves estimating the degree to which it is resistant to various forms of attack and ensuring that its cryptographic primitives are sound. In case of Wireless Sensor Networks (WSNs), an effective 2FA protocol must address these security threats like offline guessing of passwords, replay attacks, impersonation, man-in-the-middle attack. Most of 2FA protocols rely on lightweight cryptography, such as symmetric cryptography, elliptic curve cryptography (ECC) and hash functions, to limit the low resources of sensor nodes. Initial stage of cryptanalysis involves measuring the strength of these operations. As an illustration, session keys or user credentials may be reverse-engineered by an attacker in the case where protocol involved predictable keys or weak hashes [2-6].

Safe 2FA having personal authentication between the sensor node and the user dictates mutual authentication. A cryptanalysis is used to confirm that a session key changes with every new session and cannot be inferred based on an intercepted data. Resistance to offline attacks is another important feature: the protocol should ensure that with intercepted authentication data no password guessing should be possible without real-time interaction between the victim and her server. To provide safety in its transmission and storage, regulations involving transmission and storage of system-sensitive data such as two examples are examined; one being holding biometric templates and the other being holders of matters having secrets known as the private keys. A detailed cryptography will ensure the entire integrity of the system remains irrespective of failure of one factor which may include a password.

IV. Conclusion

This paper attempts to eliminate the flaws involved in using the traditional single-factor authentication methods and proposes the Two-Factor Authentication (2FA) scheme in Wireless Sensor Networks (WSNs) that is able to provide better security with integration of two individual authentication factors. To allow the secure construction of the session key, validation between two parties, and protection against common attacks in query thought as the replay and impersonation, the protocol resorts to lightweight cryptographic techniques. It is tailored towards addressing the resource constrains of the WSNs [1-4]. It ensures good protection without imposing excessive load on sensor nodes through satisfying balancing act between efficiency and security. Besides increasing user trust on WSN applications on key areas, the approach strengthens access control. To enhance secure communications in the increasingly networked wireless places, future research can focus on the opportunities further optimising the protocol with regard to scalability and compatibility with emerging Internet of Things (IoT) protocols.

References

[1] Y. Choi et al., "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 02, Issue 03, pp321-333, Dec 2002.

[2] Q. Jiang et al., "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks*". International Journal of Network Management*., vol 05, Issue 04, pp742-753, Jan 2001

[3] S. Kumari et al., "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol 09, Issue 01, pp213-233, March 2022

[4] M. L. Das, "Two-factor user authentication in wireless sensor networks". *IEEE Transactions on Wireless Communications*, vol 2(10), 2001.

[5] M. K. Khan, and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks". *Sensors*, vol 10(3), pp.2450-2459, 2010.

[6] T. H.. Chen, and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks*". ETRI journal*, vol 32(5), pp. 704-712, 2010.