International Journal of Safety and Security Engineering
Vol. 11, No. 6, December, 2021, pp. 653-661
Journal homepage: http://iieta.org/journals/ijsse

Secure Multimodal Authentication Scheme for Wireless Sensor Networks

Preetha Shivanna*, Sheela Samudrala Venkatesiah

VTU, Dept. of ISE, B.M.S. College of Engineering, Bull Temple Road, Basavanagudi, Benagaluru 19, India

Corresponding Author Email: preetha.ise@bmsce.ac.in

https://doi.org/10.18280/ijsse.110605

Received: 26 Spetember 2021
Accepted: 2 December 2021

Keywords:
access control, multimodal biometric, security, user authentication, wireless sensor network

ABSTRACT

In the current era, it is necessary to device authorization and authentication techniques to secure resources in information technology. There are several methods to substantiate authorization and authentication. User authentication is essential for authenticating user access control in WSNs. Biometric recognition error, lack of anonymity and vulnerability to attacks, user verification problem, revocation problem and disclosure of session key by the gateway node are some of the security flaws encountered.
In this study, a Multimodal Authentication Scheme for Wireless Sensor Networks (WSN-MAS) is proposed to authenticate legitimate users. The main objective is the fusion of fingerprint and iris biometric features at feature level to enable additional accuracy to verify and match user identity with stored templates. In this paper, multimodal biometric features are used for authentication to improve performance, reduce system error rates to achieve better security in WSN.

1. INTRODUCTION

WSN has varied applications in arenas such as home, environmental observation, industry and disaster relief and military monitoring. Current developments in electronics and wireless communications have supported the progress of small low- cost sensor nodes that communicate over short distances. WSN monitors physical or environmental conditions and consists of numerous sensor nodes which communicate through wireless technology. It comprises organized sensor nodes which collects surrounding environment data and communicate among the nodes. Sensor nodes are devised to communicate with each other, though their main task is to sense, gather and compute data. Data is transferred to sink nodes through multiple hops for further relays. Effective communication is achieved through routing protocols. In WSN, transmission modes are of two types; in Single hop source node transfers data to destination within a hop whereas Multi-hop sensor nodes depend on each other to transfer data to distant destinations. Cooperation of intermediate nodes, support an energy depleted node to transfer data from source and destination thereby improving the performance of WSN. A network is formed with one or more base-stations, low-power sensor nodes and few cluster-heads. Each sensor node comprises a processor, a low-power battery, an actuator, low-capacity memory and a radio. The arrangement of sensor nodes is either arranged manually or in random fashion. Sensor nodes mainly use broadcast communication paradigms and their network topologies change very frequently. Figure 1 represents the basic architecture for user communication in wireless sensor networks.

Earlier WSN's were homogeneous in nature. Sensor nodes and cluster-heads were identical with respect to power consumption, computing capability and storage capacity. Heterogeneous WSN are mounted in unattended environment.

Diverse topologies used to form a network, makes it quite complex. This type of networks undergoes various challenges such as extra battery energy, complex hardware and data leakage through malicious node. Hence privacy of messages, integrity and authentication are essential issues of data transmission. Akyildiz et al. [1] debated the necessity of security and privacy for data communication in WSN. In the current scenario, applications of WSN are vital in various domains like surveillance systems, agriculture, disaster management, environmental monitoring, healthcare, etc. A wireless sensor network comprises tiny-sensors, which are proficient in observing physical and environmental factors such as temperature, motions, vibrations, seismic events, humidity as observed by Yick et al. [2]. Sensors have extended their attention predominantly due to the progress in Micro Electrical Mechanical Systems (MEMS) development, facilitating development of smart sensors. These sensors are cost effective, smaller in size, with limited processing and computing resources.

In recent years, development of smart sensors has pulled progressions of wireless sensor networks. Data collection about an environment of an observed geographical area is the main reason for WSN existence. Several challenges like network management and heterogeneous-node networks are faced as the scale of WSN expands. Chong and Kumar [3] observed that users can witness or request for data when required or when an event has been triggered. WSN implementations are simple to deploy, usually a large number of implementations are managed at the base station points or the gateway node. Real time data collected by the sensors might be critical, valuable and confidential. Protection of such data from unauthorized user's accessibility is handled with security measures. Access control to the network is the solution for authorizing data access. User authentication substantiates the distinctiveness of a user or a machine since users seek permission to the application or machine. Verification of account transactions of ATM machines, hand phone appliances and unauthorized entry to workplace networks are some of the user authentication instances. Traditional authentication schemes were based on passwords. Later cryptographic keys with encryption algorithms were used for authentication. However, both traditional and cryptographic techniques failed to assure strong level of security analysis and vulnerabilities. Traditional methods use passwords which are easy to crack and are compromised. Cryptographic keys are vulnerable to incorrect use of keys, improper re-use, non-rotation, inappropriate storage, inadequate protection, insecure movement, non-destruction, insider threats, lack of resilience and audit logging. Biometric keys proved to be a better solution for claiming the user's identity. Biometric keys are established using behavioral and physiological features of an individual person, like fingerprint, hand geometry, face, palm print, iris etc. Unlike traditional user authentication schemes, biometric based user authentication is reliable and provides additional security. Biometric keys cannot be predicted easily, misplaced or overlooked, it is tough to duplicate or share, and very difficult to forge or distribute. Earlier user authentication security protocols established application of password to provide security. Password guessing attacks aided to break short passwords. Also, passwords could be stolen and shared with other people, and there is no method to identify the legitimate user. Similarly, special hardware support was needed by other authentication protocols. Hence, biometric authentication is the key solution for such security problems; suggested by Bhattacharyya et al. [4] Compared to conventional password-based authentication, biometric authentication is more reliable and secure.

Biometric techniques offer convenient and secure authentication. Several areas like government, banking, defense, finance, and e-commerce applications adopt biometric as the primary choice to provide security. The study in biometric field has expanded the thrust as demand for security and protection of personal data. Multimodal biometrics ensures better accessibility and security to users compared to conventional methods of authentication. Combination of biometric traits such as fingerprint, ear, iris, face, voice, and gait adopts the privilege to expertise the shortfalls of unimodal biometric. Biometric systems are susceptible to attacks, and there is need to design robust systems to provide security.

Unimodal biometrics has several problems such as noisy data, inter class variation, intra class variation, spoofing and non-universality causing the system to be less accurate and secure.

Multimodal biometric system can operate in one of three different modes:

- Serial- The output of one biometric trait is typically used to narrow down the number of possible identities before the next trait is used
- Parallel-Information from multiple traits is used simultaneously to perform recognition
- Hierarchical-Individual classifiers are combined in a treelike structure

Fusion: Multimodal biometric systems integrate information presented by multiple biometric indicators. The information can be consolidated at various levels.

Fusion is divided into three parts:

- Fusion at the feature extraction level
- Fusion at the matching score (confidence or rank) level
- Fusion at the decision (abstract label) level

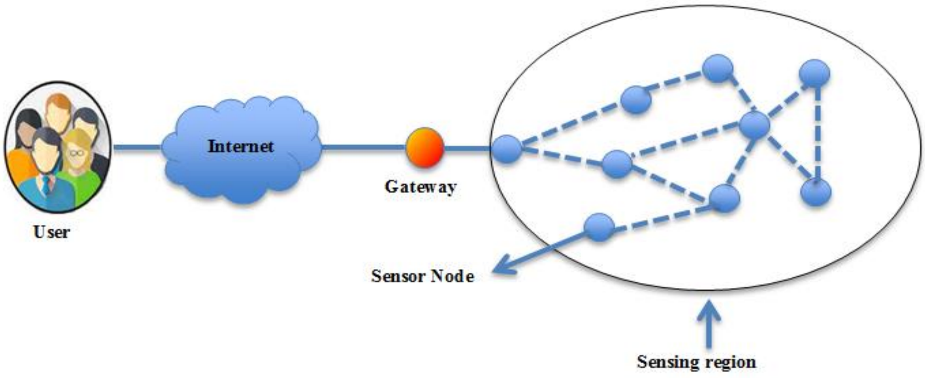

Figure 1. Architecture for user communication in WSN

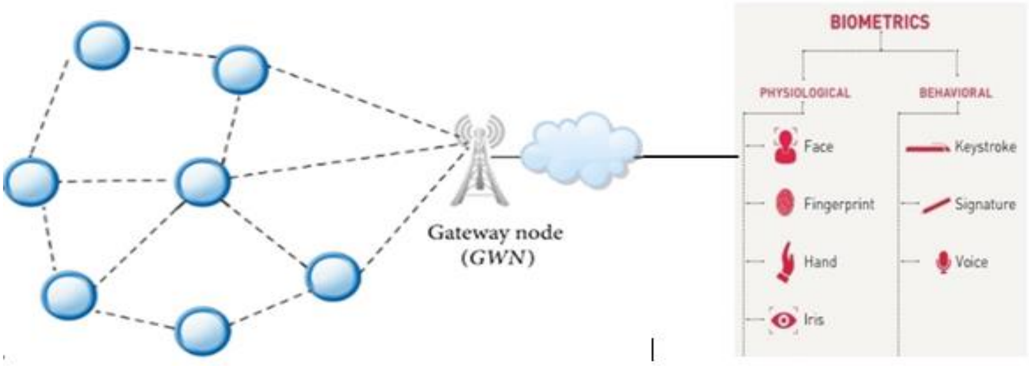

Figure 2. User biometric authentication for WSN through gateway node

Advantages of multimodal-modal biometrics:

- More secure: hard to spoof
- More accurate
- Reduce false accept rate (FAR)
- Reduce false reject rate (FRR)
- Reduce failure to enroll rate (FTE)

Disadvantages of Multimodal Biometrics:

- High Cost
- High enrolment time
- High transit times
- Increase system development and complexity
- Reduced matching level

An example of user biometric authentication for wireless sensor networks is represented in Figure 2. User biometric traits are used to authenticate legitimate users to gain access to information from wireless sensor networks. Gateway node provides authenticity by validating users through passwords, smart cards, protocols, hash functions and cryptosystems. Wireless sensor networks are exposed to attacks like DOS attacks, impersonation, password guessing and replaying, spoofing, stolen-verifier, forge and replay, disclosure, brute force, sensor capture, offline sink, node's secret, traceability key attacks. Several biometric authentication schemes are proposed to provide security and resist attacks.

2. LITERATURE SURVEY

User authentication method formulated using cryptographic hash functions and user password was proposed by Wong et al. [5]. Registered user details table is maintained in the login node and gateway. Hence users might be blocked from changing their password since the user password may be visible by any sensor node. Hence this technique is susceptible to stolen-verifier, forge and replay attacks. A user authentication scheme based on user's password and smart cards for WSN was proposed by Das [6] overcomes the security flaws of schemes suggested by Yuan et al. [7]. But it doesn't overcome some security threats, since there is no secure medium for data transmission, as an invader can certainly modify the data transmitted. Protocol in this scheme is not strong enough since it is influenced by a secret factor which is pre-installed in smart cards and sensor nodes. Security of the whole network will be affected if a node is compromised or captured. In addition, an invader can listen to complete discussion of all individuals on a network. In this scheme, a negotiated node is exposed to various attacks like DOS attacks, impersonation, replaying and password guessing. Yoon and Yoo [8] did not offer common validation and is vulnerable against restricted insider attack. Their method proved that changing passwords is difficult with Das' scheme. Khan and Alghathbar [9] suggested a safety method that strives to surpass all of these security failings. Practicing their recommended procedure, they included a phase for user-password change to Das et al.'s technique to permit easy modification of passwords. However, when some user wants to change the password, the old password is overwritten with new by smart cards. An approach built on hashed value of plain text was proposed by Alghathbar and Khan. This approach eliminated the existing password problem of Das' scheme. In Das's scheme, a network encounters several insider attacks as the gateway receives a meek password deprived of hash value. Hence, the chances of an attack by an insider in a network id is declined by password's hash value. To a certain degree, Khan et al. suggested work deals with the safety of a network system by decreasing the weaknesses of Das et al.'s method; though, this suggested method also has some security defects. For example, mutual authentication is not provided between user and sensor node as the session key is not recognized among the two individuals. Hence messages transmitted among participants undergo lack of confidentiality. Yoon et al. suggested an improved scheme of Yuan's built on biometrics without using password. This protocol considered data integrity. Two secret factors considered with this protocol authenticate every entity of legitimate users within the network. The protocol encounters several kinds of DOS attacks. Privacy is still a concern since the user response message directed by the sensor node is not encoded. He [10] proposed a user's biometric protocol to overcome the shortcomings of Yoon et al.'s protocol. This protocol involves complex hardware and consumes more energy and time. Also their protocol was exposed to several kinds of attacks like replay, guessing and DOS.

A user authentication scheme established on user password and smart card was proposed by Kaul and Awasthi [11]. Security of user identity was not considered and the scheme was vulnerable to session key compromise attack, smart card stolen attack and offline password guessing attack. Yu et al. [12] suggested an authentication protocol based on smart cards for WSN in vehicular communication. Existing protocols involved complex hardware and faced difficulties with issues like message confidentiality, data integrity and node compromise. Several kinds of safety susceptibilities of conventional user authentication protocols were highlighted by Alhobaiti et al. [13]. A novel user authentication method using biometric was proposed for wireless sensor networks. This method is viable for devices with limited resources as it is built on hash function and doesn't need any complicated equipment for biometric encryption. Kang et al. [14] excluded the flaws of Kaul's method and suggested a method with protected user authenticated key agreement. User biometric constructed on Biohash function was used to provide user authentication. Their study presented that their method is sturdy compared to all the attacks that Kaul at el. method was vulnerable to and furthermore it offered a great level of security without compromising synchronization time. A Bi-Phase Authentication scheme (BAS) for authentication in sensor networks was recommended by Riaz et al. [15]. This technique offered resistance against DOS attack by providing early lesser scale authentication of demanded messages entering WSNs. Several methods and various other recent schemes proposed by Pagnin and Mitrokotsa [16] have recommended security enhancements for wireless sensor networks.

Riaz et al. [17] enhanced user authentication scheme (SuBase) for WSN. Identity of users are proved using biometrics. Compared to other existing protocols, estimation of energy consumption and computational cost are considered to be appropriate for resource controlled networks. This scheme improved battery life of a node and reduced network traffic to protect against DOS attacks. Contactless biometrics like face recognition is more suitable for wireless sensor networks in spite of its limitations as suggested by Razzak et al. [18]. Image communication and processing requires more energy and network lifetime is less for such processing. Workload is distributed on the nodes to increase node life time. Distributed face recognition in WSN enables reduction of overloaded communication. A remote user authentication scheme using flexible biometric was proposed by Lin and Lai [19]. This scheme was built using fingerprint verification and El Gamal's cryptosystem. Khan et al's scheme proved that Lin Lai's scheme can be easily cryptanalyzed and vulnerable to various spoofing attacks. The proposed method was an improvement over the weaknesses of the Lin-Lia scheme. Security was enhanced by mutual authentication which created trust between remote system and client. Symmetric key cryptography faces challenges of key distribution. Sharing of secret keys amongst communicating parties need to be reliable and effective. Key distribution and key management are the major problems which arise during cryptographic techniques.

Sarkar and Singh [20] proposed a cancellable fingerprint biometric scheme based on secure communication establishment and session key generation. Generation of a symmetric session key of 128 bit is done using a fingerprint, and a cancellable transformation of the fingerprint template is shared among communicating parties thus securing the privacy of fingerprints. Since communicating parties generate identical session keys from fingerprint and cancellable templates in their end, sharing of secret keys through the insecure channels can be avoided. Banerjee et al. [21] claimed their enhanced security protocol using smart cards for wireless sensor networks resisted attacks like session key disclosure and impersonation. However Yu et al. [22] proved Banerjee's claim against attacks. A secure protocol to avoid several attacks was demonstrated. This protocol provided secure mutual authentication using informal security analysis and prevented several attacks like session key disclosure attack, smart card stolen attack, user impersonation attack and replay attack. Sadri et al. [23] observed that Yu et al. reliable authentication protocol for WSNs in vehicular communications is vulnerable to sensor capture attack, user impersonation attack, offline sink node's secret key guessing attack and traceability attack. Considering the weakness of Yu et al scheme, Mohammad Javad Sadri suggested a novel authentication protocol for Internet of Vehicles (IoV). The proposed method uses biometric template instead of password to provide revocation smart card and registration phase. The analysis of the protocol was done using real-or-random (ROR) and Burrow-Abadi-Needham (BAN) logic. Results proved that the proposed protocol functions well for the IoV system and offers enhanced security features. The work presented by Subhasish claims that the Turkanovic et al. [24] scheme for WSN using smart cards for authenticating users did not resist several attacks. Subhasish's technique provides mutual authentication among entities; reduced overhead occurs during computation. They used ProVrif (2.0) simulation tool to prove secrecy of session keys used during mutual authentication. Role-play of WSN in IoT applications is remarkable. Broadcast of Information is critical in IoT environments to ensure effective security of remote user authentication. Limited energy in WSN marks energy consumption and computational efficiency critical.

The proposed scheme [25] used Burrows–Abadi–Needham (BAN) logic to confirm authenticity and overcomes several security weaknesses. Protocol scheme was built on temporal credential and dynamic ID for WSN in IoT environments. Performance of the scheme with parameters like frugal energy consumption, low computational cost, low communication cost and efficiency proved to be superior in terms of qualitative and quantitative when compared with earlier schemes. To ensure authenticity and data privacy in the medical field, Pirbhulal et al. [26] develops a Heart Rate Variability (HRV) based Biometric Security Mechanism (HBSM). Security of Wireless Body Sensor Networks (WBSN's) was done using HRV as a seed to create unique and random keys. Calculating hamming distances between generated keys tested distinctive of keys while verification of random biometric keys was done using NIST (National Institute of Standards and Technology) statistical test suite. A secured and reliable protocol to share data contents through unsecure wireless sensor device was developed by Prabhu and Senthilnathan [27]. The proposed Flexible and Secured User Authentication Protocol (FSUAP) addressed the issues of Enhanced User Authentication Protocol (EUAP) and password leakage in the WSN environment. This protocol authenticates users in advance prior to permitting the users to access the sensor devices located in different sites. Replacement of two factor authentication with three factor authentication protocol was an effective way to protect the environment from brute force attack. Assurance of anonymity in sensor node identification and provisioning of synchronization, real-time authentication and light weight authentication is essential for WSN. To retain provisioning of anonymity and enhancement of network performance, Shin [28] proposed a real-time authentication protocol using Unique Random Sequence Code (URSC) and variable identifier. To overcome weaknesses of authentication protocol, Zhang et al. [29] proposed a protocol using identity –based cryptography. A comparative study of protocol performances, security and computations were discussed to prove their protocol is more suitable and secure for higher security WSNs.

To address the security concerns in WSN, an authentication scheme based on "Rabin cryptosystem" was proposed by Singh et al. [30]. Encryption, Decryption and Key generation are the factors considered for authentication. Efficiency of the encryption and decryption process is enhanced by the strong integer factorization. The proposed scheme's security analysis was done using an automated tool, AVISPA using a random oracle model, also providing mutual authentication using BAN logic. Cryptanalysis of Kim and Yoon's [31] scheme highlights the flaws such as session key exposure by GW node, no perfect forward secrecy, biometric recognition error and no revocation phase; thereby providing a path for study to be conducted. Das's three-factor user authentication scheme for WSNs had several weaknesses such as de-synchronization attack, destitution of strong forward security and susceptibility to the off-line guessing attack. To eliminate these weaknesses, Wu et al. [32] proposed a standard formal proof in the random oracle model, a formal verification with ProVerif and the informal analysis of security properties to keep away from various security vulnerabilities. Authenticated Key Agreement (AKA) scheme with Perfect Forward Secrecy (PFS) for WSNs was proposed by Yang et al. [33] without using any public key cryptographic primitive. The proposed scheme could identify impersonation occurrences. The scheme was efficiently implemented on sensors since it required XOR operation and hash function. Simulation tool ProVerif (2.0) was used to verify the session key secrecy and entities among mutual authentication [34]. The proposed protocol overcomes the flaws of Turkanovic et al. scheme, minimized storage and computational cost, also enhanced security of the authentication system. A comparison between lightweight energy-efficient key exchange protocols which are suitable for WSN was done by Suganthi and Vembu [35]. The study explained how schemes have to select network requirements and that the usage of asymmetric cryptography does not always result in a high energy consumption.

Network lifetime needs to be maintained to provide security in WSN. The Secret Key Generation (SKG) protocol was proposed by Bashaa et al. [36] and evaluated using an NS2 simulator. The protocol maximized the throughput and minimized the power consumption during key distribution thus extending the lifetime of WSN. A symmetric cryptosystem for WSN was devised by Alotaibi [37] to ensure secure communication and defend against various attacks. The proposed system was assisted with active node addition feature, and a user-friendly password/biometric update facility. AVISPA and BAN-logic analysis processes are used to validate mutual authentication, verify man-in-middle and replay attack. Continuous multimodal biometric authentication (CMBA) schemes assure accurate and possibly lesser invasive authentication mechanisms in contrast to single biometric authentication systems. Ryu et al. [38] analysed CMBA systems and evaluated for real data. A detailed study of features considered from several schemes was done by Kumari et al. [39]. Most of the authentication schemes fail to resist node capture attack, gateway node bypass attack and user impersonation attack. Sensor node, user and gateway node the entities participating in mutual establishment of a session key. Reparability of smart card loss or theft and anonymity of users are the challenges to be addressed. A method to explore node capture attacks in contrast to multi factor user authentication techniques were discussed by Wang et al. [40]. An investigation of several consequences and causes of node capture attacks and classification in terms of adversary's capabilities, attack targets and vulnerabilities was done. Multimodal Fusion-based Continuous Authentication (MFCA) scheme was proposed by Guan et al. [41] to protect data confidentiality and avoid attacks. The scheme verified user identities constantly by collecting multidimensional behaviour characteristics through online procedure, and locks out users if any strange behaviours were noticed. Hand motion and hold posture were combined to capture static and dynamic interaction patterns with mobile devices for continuous authentication [42]. Fusion of features could achieve better accuracy and also reduce equal error rate. Brown et al. [43] presented a system that relied on block chain and machine learning. Decision tree algorithm was used to combine fingerprint and face features to provide a more transparent, secure and convenient authentication method. Singh et al. [44] developed an authentication system that combined face, ear and gait biometric traits to enhance recognition rate. Z-score and Min-max techniques were used to test system performance.

Table 1 summarizes the contribution of various authors towards designing protocol methodologies to provide feasible systems with limited resources and biometric traits to develop enhanced robust security systems to resist several kinds of attacks. Though all of the discussed methods and various recommendations recommend security enhancements for wireless sensor networks; weaknesses still remain with respect to their practices and scope for improvements.

Development of user biometric authentication.

Rapid evolution in biometric technology is extremely effective in securing data and sensitive information. Survey's predicts that more than 70% of enterprises and applications have been using biometric authentication techniques.

Existing Technologies

- Fingerprint recognition – Uses person's unique fingerprint to verify one's identity, extensively used to secure mobile devices, automobiles and buildings
- Face recognition – Facial anatomy is used to identify a person, variety of applications like smartphones, credit card payments and Law enforcement
- Retina/Iris recognition – Unique pattern of iris is used and quite hard implement, basically used in nuclear research

Table 1. Summary of methodologies, biometric traits, findings and attacks

References	Methodologies	Excerpts
[11, 16-18, 24, 27-31, 32, 37, 40]	• Complex protocol hardware • Bi-Phase Authentication scheme (BAS) • SUBASE, BAN and dynamic ID • Mutual authentication • HRV based biometric, unique random keys, NIST statistical test suite • (FSUAP) Flexible and Secured User Authentication Protocol • (URSC) Unique Random Sequence Code • Identity based cryptography • AVISPA and BAN-logic • Random oracle model • Rabin cryptosystem, Asymmetric cryptography	• Consume more energy and time, Improves battery life of a node, Low energy consumption • Reduced network traffic to protect against DOS, Brute Force attacks. • Design biometric authentication protocols. • Resists Session key, disclosure, smart card stolen, replay, Guessing, DOS, user impersonation attacks • Performance of the scheme/Protocols with parameters like frugal energy consumption, low computational cost, low communication cost and higher efficiency. • Create unique and random keys. • Retain provisioning of anonymity and enhance network performance. • Validate mutual authentication, verify man-in-middle and replay attack • Mutual authentication using BAN logic.
[5, 7, 14, 15]	• Hash function and user password • Phase for user-password change hashed value of plain text • Hash function • Biohash function	• Vulnerable to stolen-verifier, forge and replay attacks. • No Mutual authentication. • Lack of confidentiality. • Viable for devices with limited resources. • No complicated equipment for biometric encryption. • Robust and Security without time synchronization.
[10, 19-22, 25, 39]	• Biometrics without using password. • Face recognition • Fingerprint verification and El Gamal's cryptosystem	• Resists several kinds of DOS attacks. • Increase node life time, Enhanced security features, Reduction of overloaded communication. • Vulnerable to various spoofing attacks. • Sharing of secret key through the insecure channels can be avoided.

	• Cancelable Fingerprint • Symmetric session key. • protocol for Internet of Vehicles (IoV) • Biometric template, symmetric cryptosystem for WSN	• Analysis of protocol done using real-or-random (ROR) and Burrow-Abadi-Nadheem(BAN) • Secured communication and defend against various attacks
[6, 9, 12, 13, 23, 26]	• User password • Smart card	• Resist Impersonation, DOS attacks, Session Key, Disclosure, Smart card stolen replaying and Password guessing. • Vulnerable to session key compromise attack, smart card stolen attack, and offline password guessing attack • Proved secrecy of session key used during mutual authentication. • Complex hardware and faced difficulties with issues like message confidentiality, data integrity and node compromise.
[33]	• Session key exposure by GW node • User and Gateway mutual establishment of a session key • Multi factor user authentication	• No perfect forward secrecy • Biometric recognition error and no revocation phase • Resist node capture attack, gateway node by pass attack and user impersonation attack. • Cause of node capture attacks • Adversary's capabilities, attack targets and vulnerabilities were discussed
[34]	• Random oracle model	• Formal verification with ProVerif • Security properties to keep away from various security vulnerabilities
[35]	• Authenticated Key Agreement (AKA)	• Identify impersonation occurrence • XOR operation and hash function implemented
[36]	• Mutual authentication • Simulation tool ProVerif (2.0)	• Minimized storage and computational cost
[38]	• Secret Key Generation (SKG) protocol • NS2 Simulator	• Maximized the throughput and minimized the power consumption

Emerging Technologies:

- Voice biometry- Uses unique tone, pitch and frequency of voice to verify an individual. Online banking and customer care services are applications to adopt such technology
- Gait recognition and vein recognition are the next emerging biometric technologies as future applications tend to adopt continuous authentication process.

Trending technology is Continuous authentication, which can be accomplished by computing an "authentication score" in real time that replicates the possibility that user is who they say they are.

3. PROPOSED SYSTEM

Authentication verifies legitimate users to gain access to systems or services. Biometric traits such as iris, fingerprint, face, voice, keystroke, vein-scan etc. are used in devices like mobile phones, laptops, and company security systems. As per studies, researchers have compared and concluded that compared to all biometric traits. Fingerprint and iris features provide more accuracy, also these are more widely used for authentication.

In this section, a multimodal biometric based authentication system is proposed for securing a wireless sensor network. The system provides mutual consent between user and gateway for communication. The proposed mechanism considers user ID, iris and fingerprint biometric to authenticate the user. Gateway node registers all users ID's to provide communication service between the user and base station. Gateway node authenticates each user who is trying to access or communicate to the base station. Proposed architecture WSN-MAS is illustrated in Figure 3, provides a greater level of protection and functionality to enhance security towards access of information from WSN. Figure 4 represents the workflow model for WSN-MAS.

The phases of the proposed scheme are as follows:

- Registration: User registers through ID and biometric traits. An encryption key will be generated and saved in Gateway node. Fingerprint and iris features are extracted to generate a template and stored in the user's device.
- Authentication: Matching of ID and biometric traits for similarity. Gateway node receives the encrypted key information generated from biometric traits and checks for ID in the database.
- Access: User is granted access for sensory data through gateway node if the template is matched. Session key is shared among the user, gateway node and sensor node. If no matching is found, the request is rejected.

```
WSN-MAS Algorithm
Step 1: Registration - user registers his/her identity using ID, fingerprint and iris biometric features, stored in database.
Input: U ID, FP, Iris
UID generates nonce
BI: repository is populated
GWN obtains RCW
Output: GWN stores template in DB
Step 2: Authentication- accept or reject the user request through authentication
Input: GWN ←template
GWN authenticates user UID when sensory data of sensors is requested
UID passes input identity and biometrics for verification
Output: Template Ur
Step 3: Access -gateway node grants access and permits the user to communicate
While (GWN == Ur)
   if (template == UID)
user authenticated, grant access
   else
user not authenticated, access denied.
```

Some notations used in the proposed WSN-MAS algorithm is depicted in Table 2.

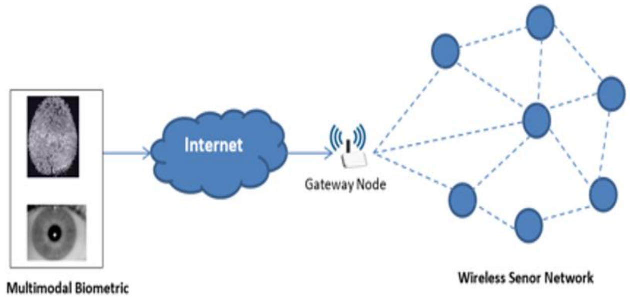

Figure 3. WSN-MAS architecture

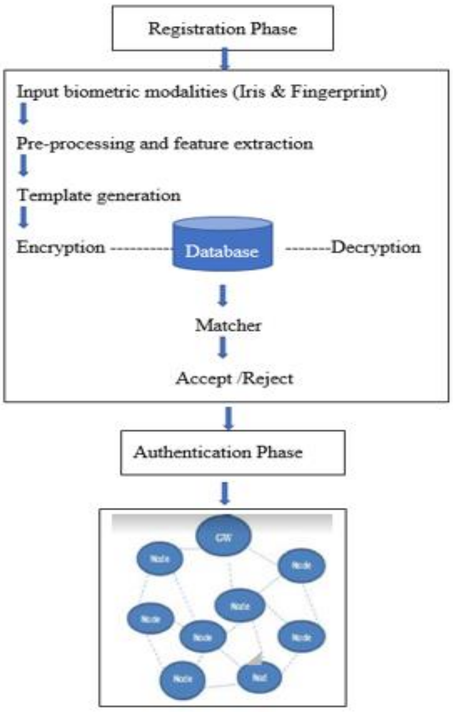

Figure 4. Workflow model for WSN-MAS

Table 2. Notation used in the WSN-MAS algorithm

Notation	Description
UID	User Name and Password
GWN	WSN Gateway Node
DB	Database
RCW	Random Code Word generated by GWN
Ur	User request
FP	Fingerprint

The proposed method uses fingerprint and iris biometric traits for authentication process. Fingerprint and iris images are pre-processed and features will be extracted using hybrid wavelet with 5 level of decomposition. KNN classifiers will be adopted for unimodal fingerprint recognition and multimodal instances of iris recognition. Fusion of both biometric traits are done at feature level and they apply machine learning algorithms to achieve better recognition rate. Wireless sensor network will be simulated to perform the registration and authentication process for users. Hashing mechanism with light and simple computations will be used to match the user request with stored templates. Gateway nodes stores the calculated hash values and validates the similarity checks. Templates of registered users are matched and authenticated.

4. CHALLENGES AND FUTURE DIRECTIONS

WSNs are deployed in unfavorable environments and encounter several challenges. Access to information and services must be secured by WSNs since Login takes place in uncertain networks, though registration is handled in secured channels. Sensor nodes with limited resources are targets for DOS attacks, hence justifying legitimate users is a concern. Identification and revocation of negotiated sensor nodes are a threat to WSN. An organized user authentication scheme should avoid malicious parties from fixing fake sensor nodes to the network. Isolation of sensor nodes from gateway nodes or networks with critical information should be provisioned to prove the legitimacy without being compromised to any other network. Securing channels for the authentication process should include lightweight and robust user authentication schemes for WSNs.

5. CONCLUSION

In this study, an attempt is made to present an insight of various biometric protocols, methodologies used to provide user security for wireless sensor networks. Characteristics, methodologies, requirements and limitations of such systems are discussed. Biometric authentication is relatively unique to an individual. User biometrics are used by various methods to improve existing security; a comprehension of various authentication schemes relating to defend against attacks, and some protocols discussed were proposed to enhance performances. The proposed WSN-MAS fulfills functional features to enhance security in WSN. The scheme is applicable to WSNs and smart environments such as smart healthcare, smart grid and intelligent transportation system. The proposed scheme can be enhanced to evaluate the computational efficiency and compared with the existing system.

REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4): 393-422. https://doi.org/10.1016/S1389-1286(01)00302-4

[2] Yick, J., Mukherjee, B., Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12): 2292-2330. https://doi.org/10.1016/j.comnet.2008.04.002

[3] Chong, C.Y., Kumar, S.P. (2003). Sensor networks: Evolution, opportunities, and challenges. Proceedings of the IEEE, 91(8): 1247-1256. https://doi.org/10.1109/JPROC.2003.814918

[4] Bhattacharyya, D., Ranjan, R., Alisherov, F., Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3): 13-28.

[5] Wong, K.H., Zheng, Y., Cao, J., Wang, S. (2006). A dynamic user authentication scheme for wireless sensor networks. In IEEE International Conference on Sensor

Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 1: 8. https://doi.org/10.1109/SUTC.2006.1636182

[6] Das, M.L. (2009). Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 8(3): 1086-1090. https://doi.org/10.1109/TWC.2008.080128

[7] Yuan, J., Jiang, C., Jiang, Z. (2010). A biometric-based user authentication for wireless sensor networks. Wuhan University Journal of Natural Sciences, 15(3): 272-276. https://doi.org/10.1007/s11859-010-0318-2

[8] Yoon, E.J., Yoo, K.Y. (2011). A new biometric-based user authentication scheme without using password for wireless sensor networks. In 2011 IEEE 20th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 279-284. https://doi.org/10.1109/WETICE.2011.47

[9] Khan, M.K., Alghathbar, K. (2010). Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors, 10(3): 2450-2459. https://doi.org/10.3390/s100302450

[10] He, D., Zhang, Y., Chen, J. (2012). Robust biometric-based user authentication scheme for wireless sensor networks. IACR Cryptol. ePrint Arch., 203.

[11] Kaul, S.D., Awasthi, A.K. (2016). Security enhancement of an improved remote user authentication scheme with key agreement. Wireless Personal Communications, 89(2): 621-637. https://doi.org/10.1007/s11277-016-3297-6

[12] Yu, S., Lee, J., Lee, K., Park, K., Park, Y. (2018). Secure authentication protocol for wireless sensor networks in vehicular communications. Sensors, 18(10): 3191. https://doi.org/10.3390/s18103191

[13] Althobaiti, O., Al-Rodhaan, M., Al-Dhelaan, A. (2013). An efficient biometric authentication protocol for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(5): 407971. https://doi.org/10.1155/2013/407971

[14] Kang, D., Jung, J., Kim, H., Lee, Y., Won, D. (2018). Efficient and secure biometric-based user authenticated key agreement scheme with anonymity. Security and Communication Networks, 2018: 9046064. https://doi.org/10.1155/2018/9046064

[15] Riaz, R., Chung, T.S., Rizvi, S.S., Yaqub, N. (2017). BAS: The biphase authentication scheme for wireless sensor networks. Security and Communication Networks, 2017: 7041381. https://doi.org/10.1155/2017/7041381

[16] Pagnin, E., Mitrokotsa, A. (2017). Privacy-preserving biometric authentication: Challenges and directions. Security and Communication Networks, 2017: 7129505. https://doi.org/10.1155/2017/7129505

[17] Riaz, R., Gillani, N.U.A., Rizvi, S., Shokat, S., Kwon, S.J. (2019). SUBBASE: An authentication scheme for wireless sensor networks based on user biometrics. Wireless Communications and Mobile Computing, 2019: 6370742. https://doi.org/10.1155/2019/6370742

[18] Razzak, M.I., Khan, M.K., Alghathbar, K. (2010). Contactless biometrics in wireless sensor network: A survey. In Security Technology, Disaster Recovery and Business Continuity, 122: 236-243. https://doi.org/10.1007/978-3-642-17610-4_27

[19] Lin, C.H., Lai, Y.Y. (2004). A flexible biometrics remote user authentication scheme. Computer Standards & Interfaces, 27(1): 19-23. https://doi.org/10.1016/j.csi.2004.03.003

[20] Sarkar, A., Singh, B.K. (2020). A novel session key generation and secure communication establishment protocol using fingerprint biometrics. In Handbook of Computer Networks and Cyber Security, 777-805. https://doi.org/10.1007/978-3-030-22277-2_31

[21] Banerjee, S., Chunka, C., Sen, S., Goswami, R.S. (2019). An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wireless Personal Communications, 107(1): 243-270. https://doi.org/10.1007/s11277-019-06252-x

[22] Yu, S., Kim, M., Park, Y. (2020). A secure biometric based user authentication protocol in wireless sensor networks. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0830-0834. https://doi.org/10.1109/CCWC47524.2020.9031136

[23] Sadri, M.J., Rajabzadeh Asaar, M. (2020). A lightweight anonymous two-factor authentication protocol for wireless sensor networks in Internet of Vehicles. International Journal of Communication Systems, 33(14): e4511. https://doi.org/10.1002/dac.4511

[24] Turkanović, M., Brumen, B., Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 20: 96-112. https://doi.org/10.1016/j.adhoc.2014.03.009

[25] Chen, C.T., Lee, C.C., Lin, I.C. (2020). Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. PloS One, 15(4): e0232277. https://doi.org/10.1371/journal.pone.0234631

[26] Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S.C., Islam, T. (2017). HRV-based biometric privacy-preserving and security mechanism for wireless body sensor networks. Wearable Sensors Applications, Design and Implementation, 12-1-12-27. https://doi.org/10.1088/978-0-7503-1505-0ch12

[27] Prabu, P., Senthilnathan, T. (2020). Secured and flexible user authentication protocol for wireless sensor network. International Journal of Intelligent Unmanned Systems. 8(4): 253-265. https://doi.org/10.1108/IJIUS-10-2019-0058

[28] Shin, K.C. (2013). A robust biometric-based user authentication protocol in wireless sensor network environment. Journal of Society for e-Business Studies, 18(3).

[29] Zhang, Q., Tang, C., Zhen, X., Rong, C. (2015). A secure user authentication protocol for sensor network in data capturing. Journal of Cloud Computing, 4(1): 1-12. https://doi.org/10.1186/s13677-015-0030-z

[30] Singh, D., Kumar, B., Singh, S., Chand, S., Singh, P.K. (2021). RCBE-AS: Rabin cryptosystem–based efficient authentication scheme for wireless sensor networks. Personal and Ubiquitous Computing, 1-22. https://doi.org/10.1007/s00779-021-01592-7

[31] Yoon, E.J., Kim, C. (2013). Advanced biometric-based user authentication scheme for wireless sensor networks. Sensor Letters, 11(9): 1836-1843. https://doi.org/10.1166/sl.2013.3014

[32] Wu, F., Xu, L., Kumari, S., Li, X. (2018). An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Networking and Applications, 11(1): 1-20. https://doi.org/10.1007/s12083-016-0485-9

[33] Yang, W., Hu, J., Wang, S., Wu, Q. (2018). Biometrics based privacy-preserving authentication and mobile template protection. Wireless Communications and Mobile Computing, 2018: 7107295. https://doi.org/10.1155/2018/7107295

[34] Banerjee, S., Chunka, C., Sen, S., Goswami, R.S. (2019). An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wireless Personal Communications, 107(1): 243-270. https://doi.org/10.1007/s11277-019-06252-x

[35] Suganthi, N., Vembu, S. (2014). Energy efficient key management scheme for wireless sensor networks. International Journal of Computers Communications & Control, 9(1): 71-78.

[36] Bashaa, M.H., Al-Alak, S.M., Idrees, A.K. (2019, April). Secret key generation in wireless sensor network using public key encryption. In Proceedings of the International Conference on Information and Communication Technology, pp. 106-112. https://doi.org/10.1145/3321289.3321320

[37] Alotaibi, M. (2018). An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access, 6: 70072-70087. https://doi.org/10.1109/ACCESS.2018.2880225

[38] Ryu, R., Yeom, S., Kim, S.H., Herbert, D. (2021). Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access, 9: 20380516. https://doi.org/10.1109/ACCESS.2021.3061589

[39] Kumari, S., Khan, M.K., Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. Ad Hoc Networks, 27: 159-194. https://doi.org/10.1016/j.adhoc.2014.11.018

[40] Wang, C., Wang, D., Tu, Y., Xu, G., Wang, H. (2020). Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2020.2974220

[41] Guan, J., Li, X., Zhang, Y. (2021). Design and implementation of continuous authentication mechanism based on multimodal fusion mechanism. Security and Communication Networks, 2021: 6669429. https://doi.org/10.1155/2021/6669429

[42] Zhang, X., Zhang, P., Hu, H. (2021). Multimodal continuous user authentication on mobile devices via interaction patterns. Wireless Communications and Mobile Computing, 2021: 5677978. https://doi.org/10.1155/2021/5677978

[43] Brown, R., Bendiab, G., Shiaeles, S., Ghita, B. (2020). A novel multimodal biometric authentication system using machine learning and blockchain. In International Networking Conference, 180: 31-46. https://doi.org/10.1007/978-3-030-64758-2_3

[44] Singh, L.K., Khanna, M., Thawkar, S., Gopal, J. (2021). Robustness for authentication of the human using face, ear, and gait multimodal biometric system. International Journal of Information System Modeling and Design (IJISMD), 12(1): 39-72. https://doi.org/0.4018/IJISMD.2021010103