Multimodal Biometric-Based Secured Access Mechanism for Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v18i09.30425

Preetha S(✉), Sheela S V
B.M.S. College of Engineering, VTU, Bengaluru, India
preetha.ise@bmsce.ac.in

Abstract—Wireless Sensors Network's (WSN) security is a critical concern owing to their unattended and intimidating distribution. Providing authentication to these networks with limited resources is a challenging task. Biometric based user authentication schemes with light computations and easy operations provide potential solutions. Several unimodal biometric techniques are proposed to secure WSN. Unimodal is susceptible to limited accuracy and spoofing. However, Multimodal biometric technology offers greater security. This paper proposes an algorithm combining fingerprint and iris biometric features for authentication. Registration and authentication processes using limited resources that are available at the WSN nodes are implemented. Experimentation results calculate computational overhead and are compared with existing methods.

Keywords—multimodal, iris, fingerprint, user biometric authentication, wireless sensor network

1 Introduction

Wireless sensor network (WSN) and wireless sensors have proved to be forefront technologies to highlight low-rate wireless personal area networks using limited resources and short communication ranges. Security and Privacy are very essential for data communication. Applications of WSN are vital in various domains like surveillance systems, agriculture, disaster management, environmental monitoring and healthcare [1]. Development of smart sensors in recent years has pulled progressions of such networks. It comprises micro-sensors which are proficient in observing environmental and physical aspects like vibrations, motions, temperature, and humidity. Sensor nodes are intelligent, small and inexpensive [2] due to the dire progress in Micro Electrical Mechanical Systems (MEMS) development. Several challenges like management of network and heterogeneous-node networks are faced as the scale of such networks expands. A WSN is formed with one or more base-station(s), 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. Earlier WSN was 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 environments and undergoes various challenges relating to malicious activities. Hence privacy of messages, integrity, and authentication are essential issues for transmission of data over these networks. Homogeneous and heterogeneous WSN is represented in Figure 1.

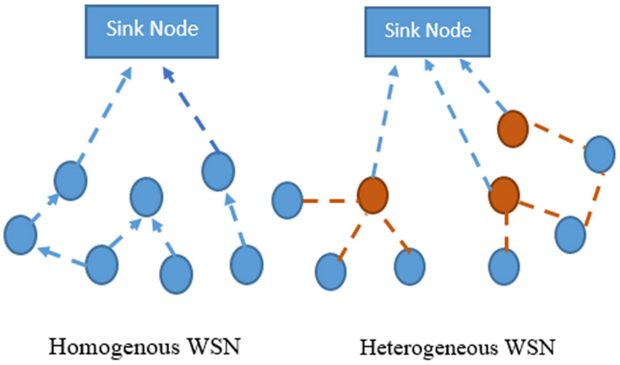

Fig. 1. Homogeneous and heterogeneous WSN

Data collection about an environment of an observed geographical area is the main reason for WSN existence. Users can observe or request for data when required or when an event has been triggered. Wireless Sensor Networks are simple to deploy and help in several kinds of implementations. Usually, a large number of implementations is managed at base station points or gateway nodes. Real time data collected by the sensors might be critical, valuable and confidential. Protection of such data from unauthorized user's accessibility is handled by security measures. Access control to the network is the solution for authorizing the data access. User authentication substantiates user identity or a device as a client to access the application or machine. Verification of account transactions of ATM machines, hand phone appliances and unfriendly entry to workplace networks are some of the user authentication examples [3].

In traditional authentication schemes, security was based on Passwords. Later Cryptographic Keys with Encryption algorithms were used. However, both these techniques failed due to their challenges. Biometric keys proved to be a better solution for claiming the user's identity and are established using behavioral and physiological characteristics of a person such as fingerprint, hand geometry, face, palm print, iris etc. User authentication using biometrics is integrally more trustworthy and safer than conventional user authentication techniques. Biometric keys cannot be predicted easily, misplaced or forgotten, they are hard to duplicate or share, and extremely difficult to forge or distribute.

In this paper, a proficient Multimodal User Authentication Scheme for WSN applications is proposed. The technique reduces authentication problems and enhances efficiency of WSNs. Recommended Multimodal User Biometric Authentication Scheme (MUBAS) provides

- Sustainable data integrity, Password verification and User anonymity
- Enhance message confidentiality and Session Key Security
- Defend against replay attack, thus improve performance and functionality of the network

Organization of the paper is as follows: Section 2 talks about existing WSN schemes with user authentication problems. Section 3, proposes a Multimodal biometric-authentication scheme. Section 4 analyses the performance of proposed method Section 5 concludes exploration of the proposed scheme.

2 Related work

User authentication system built on cryptographic hash functions and user password was proposed by Wong et al. [4]. Since a login node and gateway node maintain tables containing registered user information, users might be blocked from changing their password since user password may be visible by any sensor node. Hence this scheme remains susceptible to forge, stolen-verifier and replay attacks. A user authentication scheme for WSN based on user's password and smart cards proposed by Das et al. [5] overcomes the security shortfalls of Wong et al. schemes. But it doesn't overcome some security threats. Since there is no secure medium for data transmission, as an invader can effortlessly modify the data transmitted. Protocol in this scheme is not robust since it is influenced by a secret parameter 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 entities on a network. In this scheme, a negotiated node is vulnerable to several attacks like DOS attacks, password guessing, replaying and impersonation. Khan and Alghathbar [6] revealed that the system suggested by Das et al. does not offer mutual authentication and is vulnerable against privileged insider attack. The system proved that changing password is not easy in Das et al. scheme. Hence, they suggested a safety method that strives to deal with these security failings. Their protocol included a phase for user-password change to Das et al.'s scheme allowing users to modify their password easily. Any user wishes to change password, the old password is overwritten with new by smart cards. The approach built on hashed value of plain text eliminated the existing password problem. In Das's scheme, a network encounters several insider attacks as the gateway node receives a modest password depriving the practice of hash value. Thus, possibility of an insider attack in a network ID is declined by password's hash value.

Earlier user authentication security protocol established application of password to provide security. Password guessing attacks assisted to break short passwords. Also, passwords could be stolen and shared with other persons, 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 [7]. Compared to conventional password-based authentication, biometric authentication is more reliable and secure. Several kinds of security weaknesses of conventional user authentication protocols were highlighted by Alhobaiti et al. [8].

An effective user authentication scheme based on biometric was proposed for wireless sensor networks. This method is viable for resource controlled devices since it is built on hash function and doesn't need any complicated equipment for biometric encryption.

To a certain degree, Khan et al. suggested method deals with the security of a network by decreasing the weaknesses of Das's scheme; though, this suggested system also has some security defects. For instance, mutual authentication is not provided between user and sensor node as the session key has not been established among the two entities. Hence messages transmitted among participants undergo lack of confidentiality. A protocol based on user biometrics was suggested by Yuan et al. [9]. This approach uses a smart card and a password. Data transmitted were not encrypted, unauthorized users could view the messages easily if they succeeded in capturing any sensor nodes. Further, an invader can collect all available information and exchange messages between a user and sensor node as authorized person. Problems like data integrity and message confidentiality emerge since no provision of secured channel for data transmission.

Yoon et al. [10] suggested an improved scheme of Yuan et al.'s protocol built on biometrics without using passwords. 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 denial of service attacks. Privacy is still a concern since user response messages sent by the sensor node are not encrypted. Debiao [11] proposed a user's biometric protocol to overcome the weaknesses of Yoon et al.'s protocol. The protocol involves complex hardware and consumes more energy and time. Furthermore, their protocol remained exposed to several kinds of attacks, such as DOS, replay and guessing [12]. A scheme to authenticate users, based on user password and smart card was proposed by Kaul et al. [13] without considering security of user identity. This scheme was susceptible to smart card stolen attack, session key compromise attack and offline password guessing attack. SungJin et al. [14] 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.

Dongwoo et al. [15] eliminates weaknesses of Kaul et al. and recommends a key agreement method to secure user authentication. User biometric based on Bio-hash function was used to provide user authentication. Their study presented that their method is robust against all the attacks that Kaul et al. scheme was vulnerable to and furthermore it offered a high level of security without the requirements of time synchronization. A Bi-Phase Authentication scheme (BAS) for authentication in sensor networks was offered by Rabia et al. [16]. This scheme offered resistance against DOS attack by providing preliminary small scale authentication of the request message entering WSN. Although all of the above schemes and many other recent schemes [17, 18 and 19] ensure recommended security enhancements, weaknesses still remain related to their protocols and necessitate additional hardware and are exposed to different kinds of attacks.

Chen and Chang et al. [20, 21] described the enhancement of Das's protocol. The schemes provided a robust mutual two factor user authentication protocol to protect security in WSN environments. Security imperfections and lack of key agreement for WSN observed in Das's protocol. Vaidya et al. [22] proposed a robust protocol to resist various attacks and analyze performance by determining its efficiency. Security weaknesses of Vaidya et al. were addressed by Kim et al. [23]. Their scheme prevented several attacks, improved key agreement and mutual authentication, also proficient in computational cost and communication. Chang et al. [24] analyzed two factor authentication, key agreement and vulnerability of several attacks, and proposed a scheme to enhance the security requirements by minimizing computational cost. The method associates dynamic identity for users and removes constant parameters from user's request confirming that any two request messages are indistinguishable and independent. A study on current progresses in deep learning methodologies for feature extraction and retinal image segmentation was done by Kuryati et al. [25]. Image compression methods built on neural network was analyzed in [26]. End-to-end frames were studied to reveal interesting investigations of image coding frameworks. Re-enforced Deep Learning (RDL) model was proposed in [27] to verify personal identification using finger veins. This model involved multiple layers with a feedback to achieve better performance.

3 Proposed multimodal user biometric system for authentication for WSN

Our proposed system fulfils the shortcomings of existing techniques and enhances the security of user authentication in WSN. Fingerprint and iris features are remarkable when compared to other biometric traits. The proposed Multimodal User Biometric Authentication System (MUBAS) uses fingerprint and iris for authenticating a user while connecting a WSN. Figure 2 depicts the sequential steps for authentication using multimodal biometric. Fingerprint and iris authentication schemes do not require any supplement devices. Personal Computers or Personal Digital Assistant (PDA) are some of the devices used by users to provide biometric information. Within the range of query devices, users can send messages directly to sensor nodes to access information from the network. Sensor nodes are queried by the users using any personal devices such as PDA, mobile phone, notebook etc., thereby allowing multiple users to access wireless sensor networks. Secret information is preloaded to all sensor nodes prior deployment. Trusted nodes authenticate sensor nodes to entertain users' requests using this secret information.

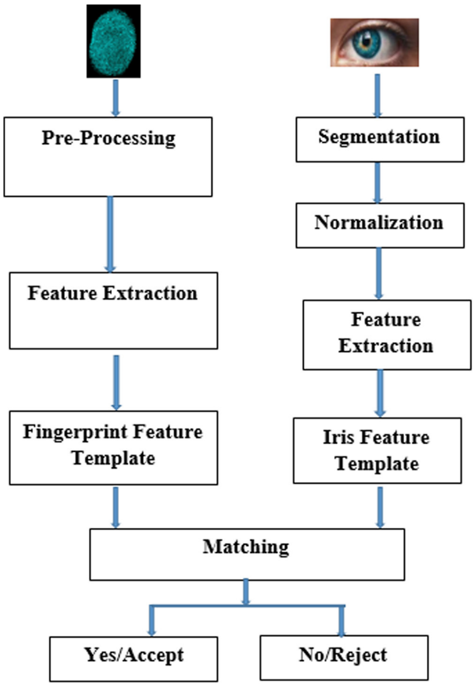

Fig. 2. Multimodal biometric steps for authentication

MUBAS considers a trusted WSN with base station and sensor nodes. Base station (BS), considered as Trusted Node (TN) acts as authenticator for both user and sensor nodes. TN is reliable and secured with overriding resources such as energy, memory and computation. Proposed framework for WSN is shown in Figure 3.

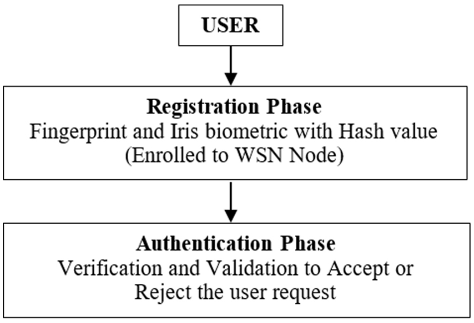

Fig. 3. Proposed framework for WSN

In WSN, nodes are randomly deployed to form clusters adopting unsupervised learning. Sensor nodes are grouped based on geographical area, range and affinity. Using K-means algorithm, one node from each cluster is elected as cluster head. Information collected by sensor nodes (primary nodes) are reported to Cluster head (secondary node), these cluster heads communicates with sink node (base station/trusted node).

3.1 Working of MUBAS algorithm

A. Registration Phase

(i) User’s signup with the WSN (trusted).

(ii) User’s biometric features (fingerprint and iris), calculate hash value and send it to WSN.

$$M_1 = [UID_u, v] \text{ where } v=H\text{ (biometric\_feature)} \tag{1}$$

(iii) Once signup from the user is done, WSN (trusted) calculates the response message resp, given by equation 2, sends to the user.

$$M_2 = [resp] \text{ where } resp = H(UID_u, ||x_0) \tag{2}$$

B. Authentication Phase

(i) User submits bio features (finger and iris) along with the H(bio). This is given in equation (3).

$$M_3 = [UID_u, resp', R_1, T_0] \tag{3}$$

where resp = H(bio_feature)
R_1 information requested
T_0 : timestamp

(ii) The WSN validates the message with a time stamp such that time stamp at which message received and time stamp at which requested should be within the threshold (delta T) otherwise rejected. If accepted then given for verification with UID at time T2. This is calculated according to the equation (4).

$$\begin{gathered} M_4 = [UID_u, resp1, T2] \text{ where} \\ Resp1 = H(UID_u||resp_1'||SN) \end{gathered} \tag{4}$$

(iii) Message at time T3 is validated and accepted if T3-T2>=T, then accepted or rejected.

$$Y_{resp} = H(UID_u||resp_2'||SN) \tag{5}$$

WSN validates if resp1!= resp2’ rejected or accepted and given message to UID with state [progress].

(iv) UID with status as [progress] then authentication process can occur, after successful authentication step, then WSN calculates according to equation (2) and sends the message.

Registration Phase: This phase registers users initially with a WSN which is trusted. User's biometric features (fusion of fingerprint and iris) is considered to calculate the hash value. Recorded hash value and biometric features are keyed into the WSN Node. Trusted node computes the response message and forwards it to the user. Trusted node applies the value of network information to extract the requested information.

Authentication Phase: Users submit requested information, biometric features (fingerprint and iris) and hash value of feature identity to the sensor node. The sensor node accepts a message and first examines the timestamp. Request is rejected if timestamp is greater than or equal to threshold value; otherwise, request is sent for user verification with its own identity to a trusted node at time stamp.

Here, assessed time interval and sensor node credentials are liable for managing user demands. Once messages are received, the trusted node verifies the validation of the message. If the new timestamp is greater than or equal to the threshold value, the request is rejected; otherwise, the trusted node checks the new value for response message. The trusted node compares hash values, if stored hash value is not equal to the new hash value, then trusted node rejects message to the sensor node. The sensor node forwards the message to the user. Otherwise, a trusted node sends the message to sensor nodes which are In-Progress. When a message with a state label In-Progress is sent to the user, it indicates that the user can proceed to the authentication process. If a successful match occurs, the trusted node calculates the new hash value and sends the message to the sensor node. Table 1 describes all notations and symbols used in the proposed algorithm.

Table 1. Symbols and notations

Abbreviation	Description
SN	Sensor Node
UID_u	User Identification
BS/TN	Base Station/Trusted Node
R_I	Information requested
T_0, T_1, T_2, T_3	Timestamps
resp1, resp2	Response messages
M1, M2, M3, M4	Messages
ΔT (delta T)	Threshold
H	Biometric Feature
||	Concatenation operator
Y_{resp}	Response message
v'	Hash value(Bio)

4 Performance analysis of proposed method

The performance of MUBAS is examined using a mathematical model compared with existing schemes. Analysis is done for security algorithms considering their hash functions and its computation time. With SHA-1, time for performing one-way hash function [TH] is 4.012 milliseconds, time for performing MAC function HMAC-SHA1 [TMAC] is 3.25 milliseconds and Time to encrypt/decrypt using RC5 [TRC5] is 0.27 milliseconds. Table 2 describes comparison of various Hash functions with respect to response time in milliseconds. Figure 4 depicts the comparison of various hash functions TH, TMAC and TRC5 relating to description and time in milliseconds.

Table 2. Comparison of hash functions

Name	Description	Time (ms)
TH	Time for achieving one-way hash function (SHA-1)	4.012
TMAC	Time for achieving MAC function (HMAC-SHA1)	3.25
TRC5	Time for encrypting/decrypting applying RC5	0.27

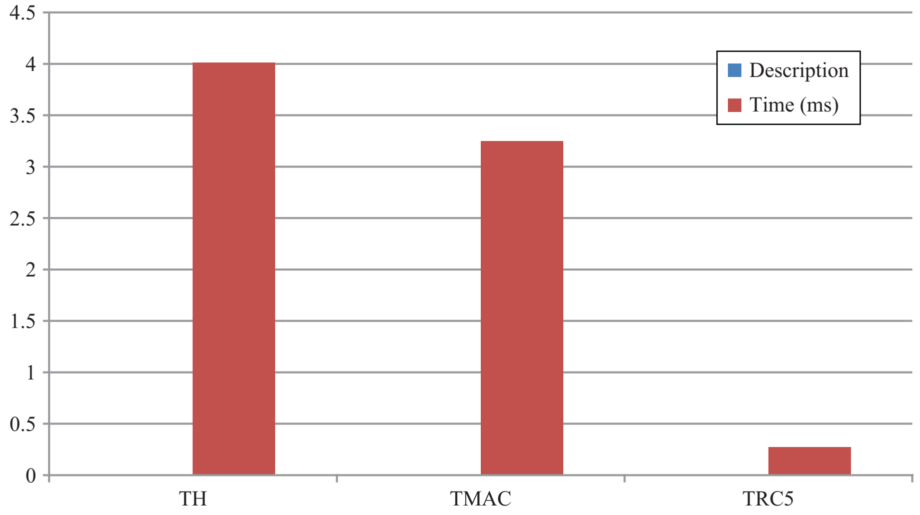

Fig. 4. Comparison of the various hash functions

With MUBAS, users register with WSN's trusted node with user ID and biometric traits. User's fingerprint and iris biometric features are extracted to calculate hash value that is sent to WSN. Hash operations are necessary during user registration phase and message time encryption/decryption. Trusted node computes a response message and sends it to the user. In the authentication phase, the user submits biometric features along with hash biometric. Later WSN validates the message within the threshold to accept or reject the request from the user. Upon acceptance, a message is sent for verification along with UID and time stamp. Message is validated by a trusted node and authenticates the user. Since sensor nodes have insufficient volume of energy, our protocol aims to minimize computational cost of the sensor node. Although a user and a trusted node have adequate resources to perform multiple tasks, our scheme also minimizes computational cost of a trusted node.

The proposed scheme is compared with three other schemes considering features namely user anonymity, mutual authentication, replay attack, password verification, session key security, message confidentiality and data integrity. Table 3 depicts the Features comparison of proposed approaches with existing methods.

Table 3. Comparison between MUBAS and existing methods

Features	Khan et al. [6]	Vaidya et al. [22]	Kim et al. [23]	Proposed MUBAS
User anonymity	X	X	1	1
Mutual authentication	X	1	1	
Replay attack	1	1	1	1
Password verification	1	1	1	1
Session key security	X	X	X	1
Message Confidentiality	1		X	1
Data Integrity	X	x	x	1

Simulation assesses the performance and strength of the proposed security method. Computational overhead for authentication increases as the number of users increases since more nodes are involved in the authentication process. Table 4 depicts assessment of other protocols with MUBAS.

Table 4. Comparison of users in MUBAS with existing schemes

Protocols	No. of Users
Yoon	580
Debiao	610
Kaul	630
MUBAS	620

Figure 5 shows comparison of Computational overhead with respect to number of users with proposed scheme. MUBAS computational overhead is minimal when compared to other schemes when multiple users accessing a network simultaneously.

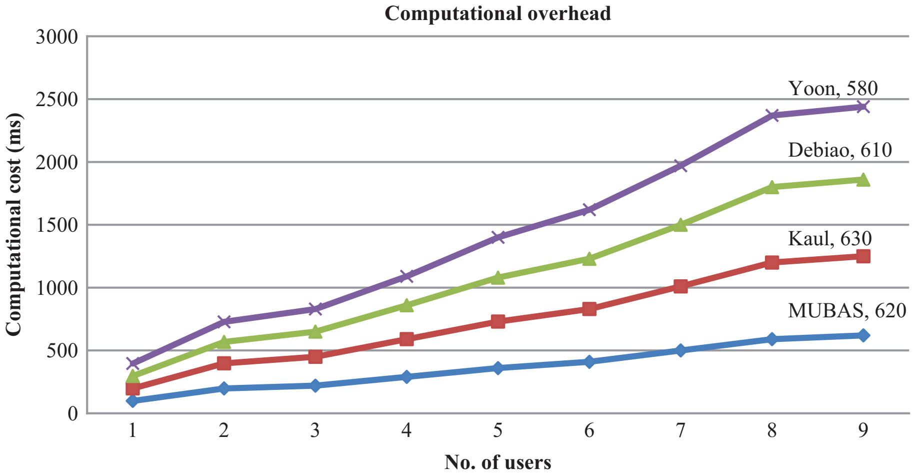

Fig. 5. Computational overhead with reference to number of users

Wireless sensor network simulation is established to illustrate the process of registration and authentication to provide end to end security. Sensor nodes are randomly deployed in a WSN environment. Clusters are formed using the K-means algorithm. Initially Cluster Head (CH) is elected based on various parameters such as battery life, authenticity, processing speed. Green colored nodes indicate members of clusters and red colored nodes indicate cluster head. CH is considered as a gateway (GW) node in our experiment. Registration and authentication is done to send data from WSN to cluster head and then to base station. We assume CH handles main computational load, since it will have sufficient computational resources. We consider this as sensible assumption, as the CH –node gathers enormous information from all sensor nodes in a form of request response. Figure 6 depicts the WSN Registration and Authentication process done during sending data with key to CH. Cluster head stores the calculated hash value and validates similarity checks. Registered users are authenticated by matching the templates of registered users.

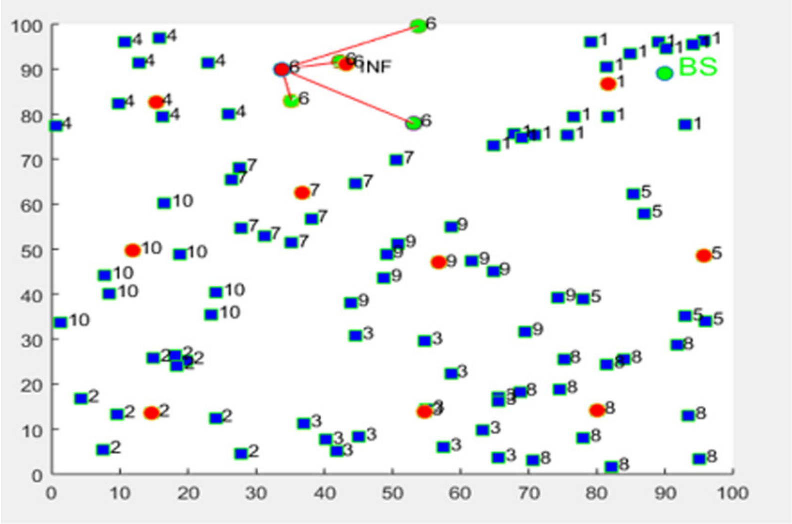

Fig. 6. WSN simulation of registration, authentication and sending data with key to cluster head (Green: Members of cluster, Red: indicates CH)

5 Conclusion & future work

A Multimodal user biometric authentication system named MUBAS is proposed to compute the efficiency of WSN. The approach uses multimodal biometric features of fingerprint and iris of the user for proving the identity. Light and simple computation but with a powerful hashing mechanism is used in the method. Mathematical analysis has been performed to demonstrate the security feature of the presented approach and the same is reported in the results section of this paper. In order to apply the biometric authentication approach performed at the WSN with limited resources, we presented a computationally simple but efficient algorithm for both registration and authentication process. MUBAS's computational overhead is reduced with respect to the number of users when compared with other schemes. In future MUBAS can be considered to design a Biometric Authentication framework to secure WSN.

6 Acknowledgment

The authors would like to thank B.M.S. College of Engineering for supporting in carrying out the research work.

7 References

[1] I. F. Akyildiz, W. Su, and Y. "Sankarasubramaniam, Sensor networks: a survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002. https://doi.org/10.1016/S1389-1286(01)00302-4

[2] J. Yick, B. Mukherjee, and D. Ghosal, ‘‘Wireless sensor network survey,’’ Comput. Netw., vol. 52, no. 12, pp. 2292–2330, Aug. 2008. https://doi.org/10.1016/j.comnet.2008.04.002

[3] Chee-Yee Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” Proceedings of the IEEE, vol. 91, no. 8, pp. 1247–1256, Aug. 2003. https://doi.org/10.1109/JPROC.2003.814918

[4] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, “A Dynamic User Authentication Scheme for Wireless Sensor Networks,” in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 1, pp. 244–251, IEEE, Taichung, Taiwan, June 2006.

[5] M. L. Das, “Two-factor user authentication in wireless sensor networks,” IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086–1090, 2009. https://doi.org/10.1109/TWC.2008.080128

[6] M. K. Khan and K. Alghathbar, “Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks’,” Sensors, vol. 10, no. 3, pp. 2450–2459, 2010. https://doi.org/10.3390/s100302450

[7] B. Debnath, R. Rahul, A. Farkhod, and C. Minkyu, “Biometric authentication: A review,” Science and Technology, vol. 2, no. 3, 2009. https://doi.org/10.1016/S0969-4765(09)70102-X

[8] O. Althobaiti, R. Mznah, and A. Abdullah, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 9, no. 5, 2013. https://doi.org/10.1155/2013/407971

[9] J. Yuan, C. Jiang, and Z. Jiang, “A biometric-based user authentication for wireless sensor networks,” Wuhan University Journal of Natural Sciences, vol. 15, no. 3, pp. 272–276, 2010. https://doi.org/10.1007/s11859-010-0318-2

[10] E.-J. Yoon and K.-Y. Yoo, “A new biometric-based user authentication scheme without using password for wireless sensor networks,” in Proceedings of the 2011 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2011, pp. 279–284, France, June 2011. https://doi.org/10.1109/WETICE.2011.47

[11] H. Debiao, “Robust biometric-based user authentication scheme for wireless sensor networks,” Cryptology ePrint Archive, vol. 203, pp. 1–15, 2012.

[12] G. Padmavathi and D. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of Computer Science and Information Security, vol. 4, no. 1, 2009.

[13] S. D. Kaul and A. K. Awasthi, “Security enhancement of an improved remote user authentication scheme with key agreement,” Wireless Personal Communications, pp. 1–17, 2016. https://doi.org/10.1007/s11277-016-3297-6

[14] R. Riaz, T.-S. Chung, S. S. Rizvi, and N. Yaqub, “BAS: the biphase authentication scheme for wireless sensor networks,” Security and Communication Networks, vol. 2017, Article ID 7041381, 10 pages, 2017. https://doi.org/10.1155/2017/7041381

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

[16] Riaz, Rabia, et al. “BAS: the biphase authentication scheme for wireless sensor networks,” Security and Communication Networks 2017 (2017). https://doi.org/10.1155/2017/7041381

[17] W. Yang, J. Hu, S. Wang, and Q. Wu, “Biometrics based privacy preserving authentication and mobile template protection,” Wireless Communications and Mobile Computing, Article ID 7107295, 17 pages, 2018. https://doi.org/10.1155/2018/7107295

[18] Z. Han, L. Yang, S. Wang, S. Mu, and Q. Liu, “Efficient multifactor two-server authenticated scheme under mobile cloud computing,” Wireless Communications and Mobile Computing, vol. 2018, 14 pages, 2018. https://doi.org/10.1155/2018/9149730

[19] E. Pagnin and A. Mitrokotsa, “Privacy-preserving biometric authentication: challenges and directions,” Security and Communication Networks, vol. 2017, Article ID 7129505, 9 pages, 2017. https://doi.org/10.1155/2017/7129505

[20] T. H. Chen and W. K. Shih, “A robust mutual authentication protocol for wireless sensor networks,” ETRI Journal, vol. 32, pp. 704–712, 2010. https://doi.org/10.4218/etrij.10.1510.0134

[21] I. P. Chang, T. F. Lee, T. H. Lin, and C. M. Liu, “Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks,” Sensors, vol. 15, pp. 29841–29854, 2015. https://doi.org/10.3390/s151229767

[22] B. Vaidya, D. Makrakis, and H. Mouftah, “Two-factor mutual authentication with key agreement in wireless sensor networks,” Secur. Commun. Netw. 2012, 9, 171–183. https://doi.org/10.1002/sec.517

[23] J. Kim, D. Lee, W. Jeon, Y. Lee, and D. Won, “Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks,” Sensors, vol. 14, pp. 6443–6462, 2014. https://doi.org/10.3390/s140406443

[24] Chang, I-Pin, et al. “Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks,” Sensors, vol. 15, no. 12, pp. 29841-29854, 2015. https://doi.org/10.3390/s151229767

[25] Hoque, Mohammed Enamul, and Kuryati Kipli. “Deep learning in retinal image segmentation and feature extraction: a review,” International Journal of Online & Biomedical Engineering, vol. 17, no. 14, pp. 103–118, 2021. https://doi.org/10.3991/ijoe.v17i14.24819

[26] Sadeeq, Haval T., et al. “Image compression using neural networks: a review,” International Journal of Online & Biomedical Engineering, vol. 17, no. 14, pp. 135–153, 2021. https://doi.org/10.3991/ijoe.v17i14.26059

[27] Najeeb, Shaima Miqdad Mohamed, Raid Rafi Omar Al-Nima, and Mohand Lokman Al-Dabag. “Reinforced deep learning for verifying finger veins,” International Journal of Online & Biomedical Engineering, vol. 17, no. 7, pp. 19–27, 2021. https://doi.org/10.3991/ijoe.v17i07.24655

8 Authors

Preetha S received Bachelor’s degree in Computer Science & Engineering from Visvesvaraya Technological, India, in 2007 and M.Tech degree in Computer Network Engineering in 2011. Currently, she is an Assistant Professor at the Department of Information Science & Engineering, B.M.S. College of Engineering. Her research interests include biometric Authentication, Social Area Networking, Wireless Sensor Networks, She can be contacted at email: preetha.ise@bmsce.ac.in; https://orcid.org/0000-0003-4160-8656

Sheela S.V holds a PhD in Biometrics from Visvesvaraya Technological University, India. She is currently Associate Professor in Department of Information Science & Engineering at B.M.S. College of Engineering. Her research interest are Biometrics, Human Computer Interaction. She has several publications to her credit. She is the member of IEEE. She can be contacted at email: ssv.ise@bmsce.ac.in; https://orcid.org/0000-0003-2749-6707

Article submitted 2022-02-25. Resubmitted 2022-04-05. Final acceptance 2022-04-07. Final version published as submitted by the authors.