

# An efficient authentication and key-distribution protocol for wireless multimedia sensor network

Basavaraj Patil<sup>1</sup>, Sangappa Ramachandra Biradar<sup>2</sup>

<sup>1</sup>Sri Dharmasthala Manjunatheshwara Institute of Technology, Affiliated to Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>Shri Dharmasthala Manjunatheshwara College of Engineering and Technology, Dharwad, India

## Article Info

### Article history:

Received Mar 24, 2022

Revised Apr 18, 2022

Accepted May 24, 2022

### Keywords:

Attack authentication

Key-exchange

Multimedia

Privacy

Wireless multimedia sensor network

## ABSTRACT

To provide security and privacy for multimedia data transmission, efficient techniques for authorizing and authenticating network users and nodes are required. These challenges have made it a vital and significant area of research in the present decade. Due to resource constraints, existing systems are unable to provide adequate protection against vulnerable behaviors and security assaults such as black-hole, Sybil, man-in-the-middle, and other similar attacks. In this paper, an effective enhanced engineered cementitious composites (ECC) and crypto-based authentication with a key exchange mechanism is proposed. The method boosts the effective authentication mechanism and reduces the number of vulnerable activities in the network. The simulation results demonstrate that the suggested technique is robust to malicious assaults and performs mutual authentication efficiently. A cost-benefit analysis validates that the processing, communication, and storage requirements are much reduced when compared to existing approaches. Furthermore, an informal security analysis demonstrates that the suggested protocol is secure and adaptable to real-time scenarios.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Basavaraj Patil

Sri Dharmasthala Manjunatheshwara Institute of Technology

Ujire 574240, Dakshina Kannada, Karnataka, India

Email: bbpatilcs@gmail.com

## 1. INTRODUCTION

Wireless multimedia sensor networks (WMSNs) are increasing its scope as a major sub-domain of wireless sensor networks that support multimedia data transmission, monitoring, and processing in the network. With the rapid growth of technology, the demand for multimedia data such as text, audio, images, and video has increased in terms of size, necessity, and flexibility of use. It is critical to safeguard the data transmitted over the network [1]–[3]. This issue has made it difficult for the research community to provide efficient solutions to the aforementioned issues. The WMSNs can store, and process in real time multimedia data transmission rising from heterogeneous sources. The reference architecture of WMSN is as shown in Figure 1.

Due to the system's reliance on wireless transmission, nearly all the information entering it is at risk of interception. Data confidentiality [4], Availability, Authentication [5], Authorization, Integrity, freshness, and non-repudiation are the major needs for providing the security [6], [7]. The wide range applications of WMSN are data collection, monitoring, and analysis in diverse domains like agriculture, health, and military applications [8], [9], as well as pollution and traffic monitoring. The authentication [10], [11] provides authorization of the users/node to perform the secured data transmission activities in network. Authentication is the one of the major cryptographic services involved in the authentic data processing. It can be carried out using digital signatures, using authentication codes between the communication nodes and key-agreement techniques.

The major elements required for authentication process are to verify the source identity from sender and validating the information veracity for safeguarding the message inventiveness. The preventive measures against the attacks can be employed. The process makes use of shared key in which sender and the receiver consider same key for verification and authorization. After the verification process, the respective private keys are employed to encrypt the information. The process of authorization of the nodes involving in the communication are to be verified and validated with some set of protocols in consideration of various parameters. The process should consider the identity of the nodes, key distribution time, energy consumption, and resource utilization.

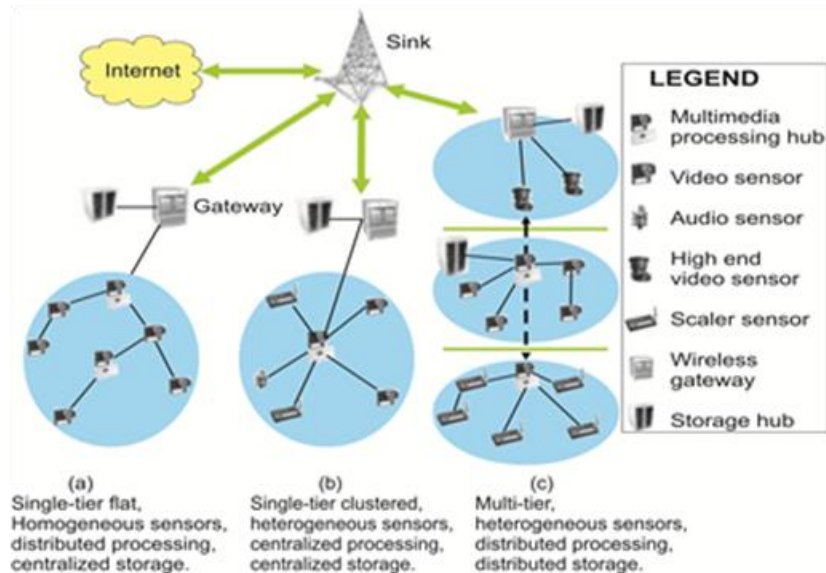


Figure 1. Typical design of WMSN [12]

The overview of previous studies on existing authentication protocols are discussed as below. Rajeswari and Seenivasagam proposed [10] lightweight authentication protocol (LAP) for smart dust. It utilizes lesser keys to guarantee the security for nodes prior to distribution and reduces the communication overhead. Their evaluation and the experimental results show that it has lesser computational and communication requirements with reduced overhead. Akyildiz *et al.* [12] overviewed the various applications and reviewed some commercial products available.

Chatterjee *et al.* [13] proposed authentication mechanism to resist for the various vulnerable attacks in sensor networks with light computational and communicational load. The issues with key management and access control are addressed in 4-phases- registration, node validation process by cluster heads, mutually authenticating themselves and sharing the generated secret keys. In each session, another key is produced and shared to prevent replay attacks. The proposed authentication protocol is designed based on engineered cementitious composites (ECC) that withstand the various attacks. The experimental results show that it has less energy consumption for efficient authentication. It also improved with traffic congestion and delay with higher security. Light-weight digital signature algorithm (LWDSA) [14] is an authentication system that uses MBLAKE2b and ECCDSA to interact directly or across many hops. Using MBLAKE2b and the elliptic curve digital signature technique, the proposed work seeks to construct a light-weight authentication system (ECDSA). For constrained WSN contexts, the authors claim that the framework increases longevity and reduces computing time. The Scyther protocol verification tool was used to verify and confirm the experimental testing.

Temirlan and Li [15] propose a redesigned user authentication strategy to address existing scheme limitations and improve security. The costs of elliptic curve random point scalar multiplication are replaced with cost-effective symmetric-key operations. They integrated ECDSA with medium access control (MAC) to improve the security of the authentication process and the reliability of key exchange.

EdDSA algorithm [16] is a dual structured lightweight authentication mechanism designed with dual-topology for multicast WSNs. The vulnerable nodes are optimally observed by a theoretical game model to avoid the illegitimate access (man-in-middle attack) with fast authenticity. The simulations conducted on NS2 validate that the performance is better, has reduced energy consumption 0.13% and time consumption 0.07% compared to existing methods.

For farm surveillance, Ali *et al.* [17] devised a remote user authentication technique based on WSN. Users are divided into four categories: farmer (user-node), BS, GW-Node, & SN. Sensors may collect ecological data such as temperature, moisture, wetness, pH, light intensity, CO<sub>2</sub>, and so on, and then send it to the gateway for monitoring. It is critical to prevent unwanted access, eavesdropping, and malicious behaviours on these ecological data in order to maximize productivity. The simulation results show that the protocol ensures that key exchange and authentication are both efficient. BAN logic is used to verify validity, while AVISPA software is used to ensure resilience to security threats.

Yasmin *et al.* [18] present an authentication framework for authenticating sensor nodes both inside and outside the network, based on an identity (ID)-based technique and an online/offline signature (OOS) mechanism. The simulation is built on TinyOS for MICA2 sensor nodes, and the session keys are only shared with outsiders after they have been authorized via the suggested process. The limitations of the existing work are overcome with the proposed method. The proposed key exchange and modified ECC based authentication mechanisms with digital hashing guarantees the effective authentication of the user in WMSN for secure transmission and resistance for the attacks.

**2. RESEARCH METHOD**

The working of the proposed key distribution and authentication protocol is shown in Figure 2. The contribution for the work is to design the reliable and enhanced authentication and key distribution protocol is implemented for the secured data transmission in WMSN. The formal security analysis is conducted to verify the resistance of the known attacks.

The proposed method provides authentication process with the combination of modified ECC and digital hashing. It focusses on achieving the integrity and confidentiality of the data. The sybil attack is considered in WMSN to provide an efficient authentication mechanism. The network topology is built, and attacks are launched in order to ensure efficient transmission of multimedia data. A novel modified ECC based authentication scheme for WMSN is proposed to overcome the limitations the problems of authentication in comparison with existing protocols like RSA, ECDSA [14], [19], [20], ECDH [13].

In topology, a sender and a receiver communicate with one another to exchange data. Each party generates their own private-public keys. These keys are obtained by generating an elliptic curve and the points on it. When a node wishes to communicate or send data to another node, the sender node generates a shared key using its own private key and the public key of the desired node. The shared key is applied to encrypt data sent between nodes. When a node gets data, it generates a shared key as well. This shared key is used at the receiver end to decrypt the data. On the other hand, the attacker receives both the sender and receiver nodes' public keys but is unable to generate the shared keys. The data transmission procedure is complete by the time the attacker attempts to decrypt the data using various keys. As a result, the data is secured using ECC-based key exchange. The phases involved in the establishing the connection, key exchange and authenticating between the user, gateway and sensor nodes.

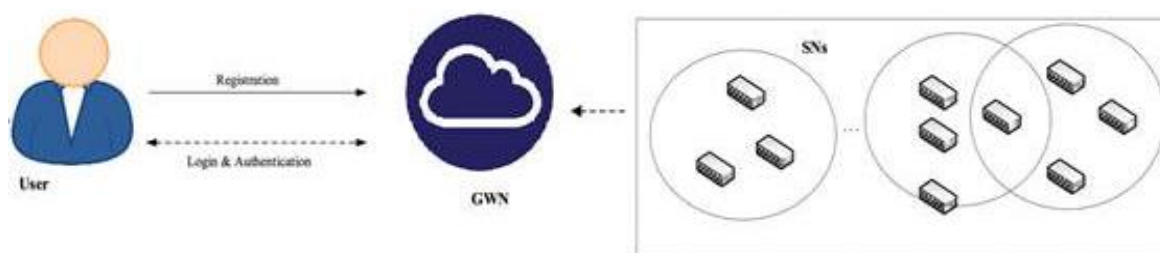


Figure 2. Working of proposed registration and login phases

**2.1. Registration phase**

In any communication channel, the process of data transmission starts with the registration. It is mandatory phase to verify authenticate users and allow them to participate in the network. The registration as in Figure 3 taken place between user-gateway and later between sensor node and gateway. The notations are listed in Table 1 and the registration steps are as follows:

- a) Registering user-node and gateway
  - The user U selects ID<sub>i</sub> and password PW<sub>i</sub>
  - Select the random integer n and calculate  $pw = h(Pw_i \oplus n) * P$
  - Generate pairs of signature keys and validation keys (Q<sub>i</sub>, q<sub>i</sub>) and send message {pw, ID<sub>i</sub>, Q<sub>i</sub>} to the GW

- GW contains value  $Q_i$ , sets crypto shared keys  $(Q_v, q_v)$
- GW calculates  $a=h(pw \parallel ID_i)*P$  and send the message  $\{a, q_v\}$  to  $U_i$
- When receives message stores values  $(a, q_v, n, P)$
- b) Registration of gateway with sensor node
  - $S_j$  selects  $ID_j, h(PW_j)$  and generates random number  $y$
  - $S_j$  calculate  $c= h(ID_j \parallel y), j= h(ID_j \parallel c \parallel h(PW_j) \parallel T_1)$  and send message  $\{j, ID_j, h(PW_j), c, T_1\}$  to the GW
  - GW verifies the  $T_1$  timestamp and compare value of  $j$  with new updated one.
  - GW calculates  $d=h(c \parallel ID_j)*P, g=d.x \oplus h(ID_j \parallel h(PW_j))$  and  $f=h(g \parallel T_2)$
  - GW sends message  $\{f, g, T_2\}$  to sensor node  $S_j$
  - Verify timestamp  $T_2$ , compare received value with new and stores it.

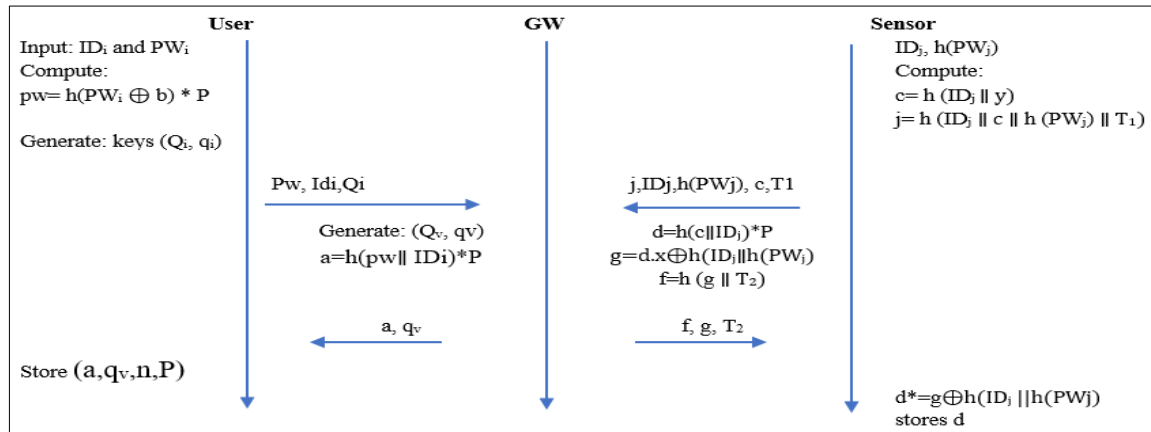


Figure 3. Registration phase

Table 1. Notations used

Notation	Description	Notation	Description	Notation	Description
$U_i$	User node	$S_j$	Sensor node	$Sig_u(m)$	Signing algorithm on ECC for $U_i$
$ID_i$	User identity	$ID_j$	Sensor node identity	$N_i, N_k$	Nonces
$PW_i$	User password	$pw_j$	Sensor node password	$HMAC(M, K)$	Crypto hash calculation
GW	gateway	$h()$	hash function	$M$	signed message
$q, p$	prime numbers ( $p=2q+1$ )	$P$	large order point chosen for EC (user)	$sk$	session key
$Q_i, q_i$	Public-private key of $U_i$	$Q_v, q_v$	Public-private key of $U_j$		

**2.2. Login and authenticate phase**

Once the user registers to the network, the next phase to provide access to the network is the login phase, where the user's ID and password are verified. After successful login, secret keys are exchanged between the User and GW, and then the User connects to the sender node through the gateway as shown in Figure 4.

- a) Login phase
  - $U_i$  inputs  $ID_i$  and  $PW_i$
  - Calculate new values of  $a*=h(pw \parallel ID_i) *P$  and compare
  - $U_i$  picks random nonce key  $k$  and  $N_i$ , where  $k$  is a HMAC key
  - $U_i$  calculates secret value  $R=a*q_v$  and cipher text  $w=(k \parallel N_i) \oplus R.x$
  - Create an ECC signature  $s=Sig_u(a \parallel w)$  and send the message  $\{s, a, w\}$  to the GW
- b) Authentication
  - GW receives message from  $U_i$  and restore secret value  $R=h(pw \parallel ID_i)*Q_v$
  - Obtain key value  $k$  from value  $w$
  - Select generated random value  $N_k$
  - Calculate session key  $sk= h(N_k \parallel k)$  and cipher text  $e=sk \oplus R.x$
  - GW initially sends message  $\{e, HMAC(e, k)\}$  to  $U_i$ , verify HMAC and calculates session key  $sk=e \oplus R.x$
  - GW calculate  $Z=R.x \oplus d.x$  pass on message  $\{pw, e, Z, w\}$  to sensor  $S_j$

- $S_j$  obtains  $R$  from  $Z=R.x \oplus d.x$  and calculate session key  $sk=e \oplus R.x$
- $S_j$  obtain  $k$  from  $w$  and send message  $E(pw.x \parallel N_i, Sk)$ ,  $HMAC(E(pw.x \parallel N_i, sk), k)$  to  $U_i$
- $U_i$  validates hash value, cipher text is encoded to verify acknowledged session key  $sk$ .

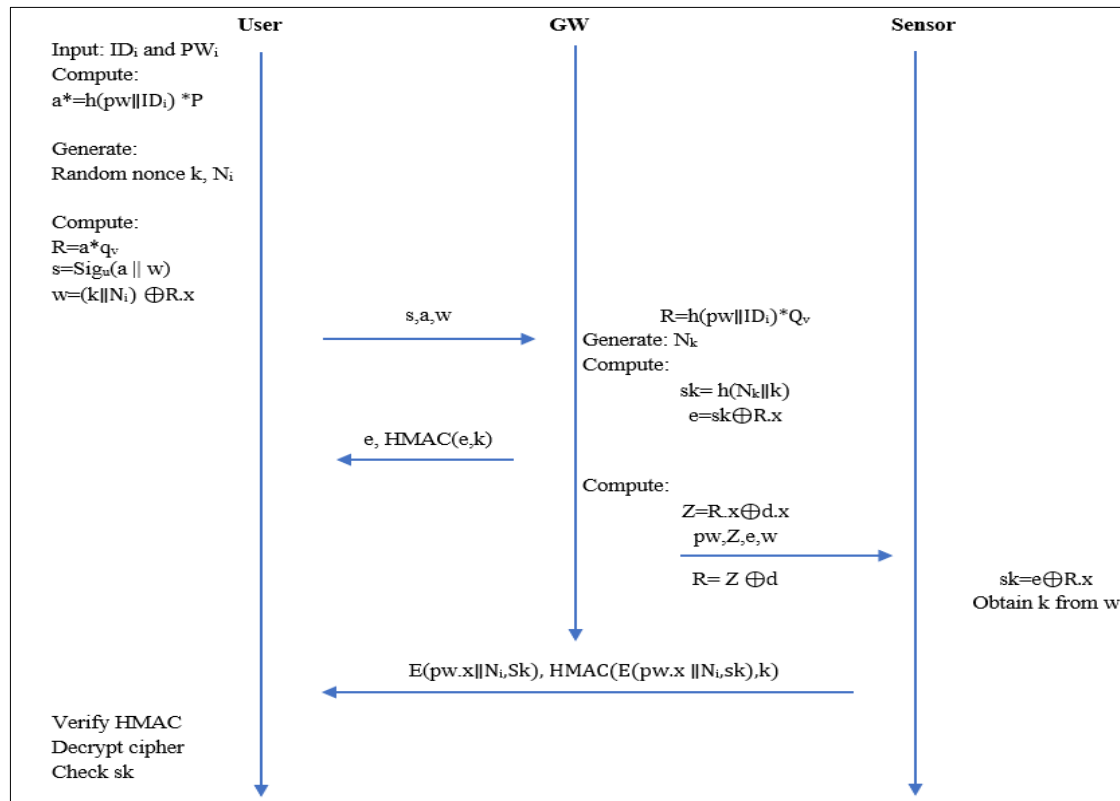


Figure 4. Login and authentication phase

### 3. RESULTS AND DISCUSSION

#### 3.1. Security analysis

To evaluate the proposed authentication mechanism, it is required to evaluate its performance. The various attacks like node replication, sybil, insider and Man-in-middle attacks are tested. The results justify that security analysis of the proposed method has stability to the security attacks and deliver secure authentication.

##### 3.1.1. Node replication attack

The proposed authentication process helps to reduce the replication attacks. The forged nodes are created by the attacker which matches with the genuine nodes and try to accumulate the information like node-id (ID), public and private keys ( $Q, q$ ). In this type of the attacks, the attacker collects the required information and imitate to duplicate the original sensor node ( $S_j$ ) with forged node [20]. The scheme also incorporates the reply message attack, hence the fresh nonce for each node is used. The reply is not sent to forged node, as it uses the retrieved old nonce value. Hence it is shown that the proposed scheme is protected against repetition attack.

##### 3.1.2. Sybil attack

The design is setup by introducing the sybil attack, where the malicious or unauthorized user try to pretend as the original node ( $S_j$ ) by obtaining the forged data. In the proposed scheme, the identity ( $U_i, U_j$ ) of each node participating in the network is verified by the signature generated. The exchange of the key ( $Q_i, q_i, Q_v, q_v$ ) happens only between the verified nodes only. The HMAC gives the additional security feature to guarantee the data transmission only between valid nodes ( $U_i, U_j$ ) and cannot pass through the gateway (GW). Hence the proposed scheme is resistant against the Sybil attack.

### 3.1.3. Insider attack

In this scheme, it's impossible to gather the user credentials as it consists of value of  $n$  and  $pw_i$ . The value of  $n$  is unpredictable to guess, hence even the insider of GW nodes is impossible obtain credentials. Therefore, the purported scheme is resistant to insider attack.

### 3.1.4. Man in-the middle attack

In this type of attack, the intruder tries to listen the conversation between two nodes. The exchange of the messages takes place only between the user  $U_i$ , GW and sensor node  $S_j$  only after verification of HMAC value. Hence the proposed scheme allows only the legal and legitimate users are allowed.

### 3.1.5. Mutual authentication

The process of verification of nodes is done at the initial stage of registration and login phase. The communication happens only between two-entities: User nodes-gateway or gateway-sensor nodes. The HMAC value provides the evidence of message integrity. The GW authenticates the participating nodes by verifying the hash key  $k$ . The messages sent back with verified crypto hash key.

## 3.2. Performance analysis

The proposed mechanism is much suitable for the low-powered sensor networks. It consumes lesser power and less space experimental results. NIST advised network parameters are consider for the implementation. The performance evaluation is conducted with security features, computational cost, and communication cost. The various features required to prove the better security of the proposed protocol the features shown in Table 2 are compared over [21]-[25] schemes.

Table 2. Comparison of security features

Security features	[21]	[22]	[23]	[24]	[25]	Proposed
Tolerant for password guessing attack	✗	✗	✗	✓	✗	✓
Delivers efficient login	✗	✓	✗	✓	✓	✓
Provide mutual-authentication	✓	✓	✓	✓	✓	✓
Session-key security	✓	✓	✓	✓	✓	✓
Tolerant for replay attack	✓	✗	✓	✗	✓	✓
Tolerant for GWN bypass attack	✓	✓	✓	✓	✓	✓
Tolerant to denial-of-service attack	✓	✓	✗	✗	✗	✓

### 3.2.1. Computation cost

The computation costs include registration, login phase, key generation, and authorization. The hash function needs very less computing time, including cryptographic acts and key encoding. The state-of-art outcomes with execution time  $t_h \approx 0.0004$  s, and encryption/decryption time  $t_{ed} \approx 0.0017$ s. The computation cost for the GW node is bit greater than a sensor node. In consideration of better security, bit high computational cost with all security features is desirable. The comparative analysis of proposed mechanism with existing schemes [21]-[23], [26] are as shown in Table 3 and Figure 5. It gives the time taken for the computation cost at different levels.

Table 3. Computation cost evaluation

Scheme	User	GW	Sensor Node	Overall Cost	Time(ms)
[21]	$3t_h$	$2t_h + 2t_{ed}$	$5t_h$	$10t_h + 2t_{ed}$	22.4
[26]	$8t_h$	$10t_h$	$5t_h$	$23t_h$	11.5
[22]	$8t_h + 2t_{ed}$	$6t_h + 1t_{ed}$	$7t_h + 1t_{ed}$	$21t_h + 4t_{ed}$	45.3
[23]	$6t_h$	$10t_h$	$7t_h$	$23t_h$	11.5
Proposed	$7t_h$	$6t_h$	$4t_h$	$18t_h$	7.2

The notation used for computation time are as follows,

$T_h \rightarrow$  hash computation time       $T_{ed} \rightarrow$  Symmetric encryption/decryption

### 3.2.2. Communication cost

The total bits transmitted in login-stage and authentication-stage is called as communication cost. For the fast data transmission and reduce traffic congestion, the communication cost should be less as much as possible. The comparative analysis of the cost for various protocols is as shown in Figure 5 and Table 4. The cost of [22] less compared to our protocol, but all the security features are not satisfied in it. The highest cost of [26] is 2432 bits ( $19 \times 128$ ) and hence our proposed protocol has less computational cost without compromising any security aspects (features).



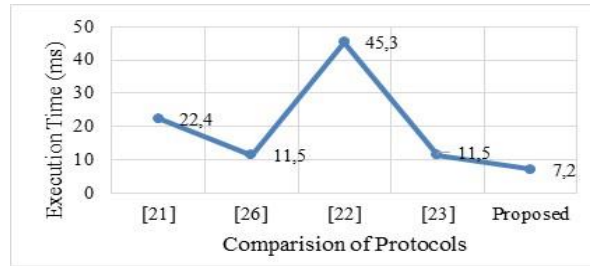


Figure 5. Computation cost of different schemes

Table 4. Communication overhead and storage cost

Schemes	Communication cost (bits)	Storage cost (bits)
[21]	1,792	672
[26]	2,432	640
[22]	1,024	896
[23]	1,920	640
Proposed	1,280	512

**3.2.3. Storage cost**

As the sensor nodes are available with lesser memory storage, the consumption of memory is also equally important to improve the performance. The total number of bits stored is referred as the storage cost. The Table 4 its evident that proposed scheme has a smaller amount of storage overhead than the existing methods as represented in Figure 6.

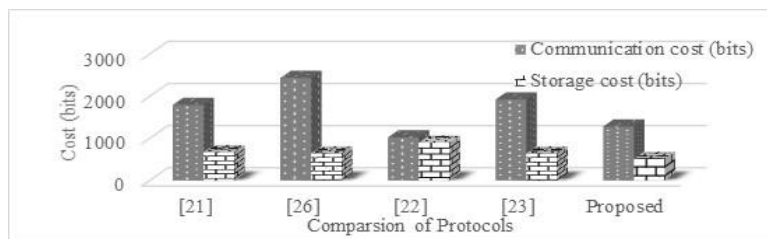


Figure 6. Communication and storage cost of different schemes

**4. CONCLUSION**

The challenging task in WMSN is to ensure reliable and secure data transfer. The proposed authentication and key distribution protocol improves the node authorization and effective key exchange mechanism for secure data transfer. Users must first register before being involved in the data transfer process. Later, users are authenticated using shared crypto keys. The security analysis proves that the proposed mechanism provides efficient mutual authentication and resilience to various security assaults. Furthermore, it provides security against vulnerabilities like password guessing resistance, replay resistance, effective login, session key security, gate-way bypass assault, and denial-of-service attack. The performance was evaluated and found to be better than other methods in terms of safety. In the future, the authentication process can be strengthened to withstand all forms of vulnerable activity, and key exchange can be improved using efficient cryptographic algorithms.




**REFERENCES**

- [1] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Networks*, vol. 51, no. 4, pp. 921–960, 2007, doi: 10.1016/j.comnet.2006.10.002.
- [2] M. O. Farooq and T. Kunz, "Wireless multimedia sensor networks testbeds and state-of-the-art hardware: A survey," *Commun. Comput. Inf. Sci.*, vol. 265 CCIS, no. PART 1, pp. 1–14, 2011, doi: 10.1007/978-3-642-27192-2\_1.
- [3] H. E. Zouka, "A secured wireless multimedia sensor network," *IJCSIS, J. Comput. Sci.*, vol. 14, no. 1, pp. 11–17, 2016.
- [4] Rekha and R. Gupta, "Elliptic curve cryptography based secure image transmission in clustered wireless sensor networks," *Int. J. Comput. Networks Appl.*, vol. 8, no. 1, pp. 67–78, 2021, doi: 10.22247/IJCN/2021/207983.
- [5] E. Barker, M. S. E. Barker, W. Barker, W. Burr, and W. Polk, "Recommendation for Key Management – Part 1 : General," *NIST Spec. Publ. 800-57 Part 1, Revis.*, no. May, pp. 1–142, 2007, [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>.




- [6] G. C. Kessler, "An overview of cryptography (Updated Version)," vol. 1998, no. January, pp. 1–65, 2019, [Online]. Available: <https://www.garykessler.net/library/crypto.html>.
- [7] S. K. Singh, M. P. Singh, and D. K. Singh, "Most cited survey article in computer science and engineering," *Guid. to Wirel. Sens. Networks*, vol. 2, no. 1, pp. 27–45, 2019, doi: 10.1007/978-1-84882-218-4.
- [8] U. Jain and M. Hussain, "Securing wireless sensors in military applications through resilient authentication mechanism," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 719–728, 2020, doi: 10.1016/j.procs.2020.04.078.
- [9] A. Msolli, A. Helali, and H. Maaref, "New security approach in real-time wireless multimedia sensor networks," *Comput. Electr. Eng.*, vol. 72, pp. 910–925, Nov. 2018, doi: 10.1016/j.compeleceng.2018.01.016.
- [10] S. R. Rajeswari and V. Seenivasagam, "Comparative study on various authentication protocols in wireless sensor networks," *Sci. World J.*, vol. 2016, no. iii, 2016, doi: 10.1155/2016/6854303.
- [11] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009, doi: 10.1109/TWC.2008.080128.
- [12] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "Wireless multimedia sensor networks: applications and testbeds," *Proc. IEEE*, vol. 96, no. 10, pp. 1588–1605, 2008, doi: 10.1109/JPROC.2008.928756.
- [13] K. Chatterjee, A. De, and D. Gupta, "A secure and efficient authentication protocol in wireless sensor network," *Wirel. Pers. Commun.*, vol. 81, no. 1, pp. 17–37, 2015, doi: 10.1007/s11277-014-2115-2.
- [14] M. Lavanya and V. Natarajan, "LWDSA: light-weight digital signature algorithm for wireless sensor networks," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 42, no. 10, pp. 1629–1643, 2017, doi: 10.1007/s12046-017-0718-5.
- [15] I. Temirlan and Y. Li, "ECC-based user authentication scheme for wireless sensor networks," *Int. J. Eng. Res. Sci.*, vol. 3, no. 6, pp. 21–28, 2017, doi: 10.25125/engineering-journal-ijoe-jun-2017-5.
- [16] N. Yuvaraj, R. A. Raja, T. Karthikeyan, and K. Praghsh, "Improved authentication in secured multicast wireless sensor network (MWSN) using opposition frog leaping algorithm to resist man-in-middle attack," *Wirel. Pers. Commun.*, vol. 123, no. 2, pp. 1715–1731, Oct. 2022, doi: 10.1007/s11277-021-09209-1.
- [17] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Futur. Gener. Comput. Syst.*, vol. 84, pp. 200–215, 2018, doi: 10.1016/j.future.2017.06.018.
- [18] R. Yasmin, E. Ritter, and G. Wan, "An authentication framework for wireless sensor networks using identity-based signatures: Implementation and evaluation," *IEICE Trans. Inf. Syst.*, vol. E-95-D, no. 1, pp. 126–133, 2012, doi: 10.1587/transinf.E95.D.126.
- [19] A. Corbellini, "Elliptic Curve Cryptography: ECDH and ECDSA," *Andrea Corbellini Blog*, pp. 1–12, 2015, [Online]. Available: [https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/#disqus\\_thread](https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/#disqus_thread).
- [20] A. Pandey and R. C. Tripathi, "A survey on wireless sensor network security," *Int. J. Comput. Appl.*, vol. 3, no. 2, pp. 43–49, 2010, doi: 10.5120/705-989.
- [21] S. D. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in IoT-based healthcare environment," *J. Reliab. Intell. Environ.*, vol. 6, no. 1, pp. 3–13, Mar. 2020, doi: 10.1007/s40860-019-00079-w.
- [22] J. L. Li, W. G. Zhang, S. Kumari, K. K. R. Choo, and D. Hogrefe, "Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 6, p. e3295, Jun. 2018, doi: 10.1002/ett.3295.
- [23] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci. (Ny)*, vol. 321, pp. 263–277, Nov. 2015, doi: 10.1016/j.ins.2015.02.010.
- [24] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors (Switzerland)*, vol. 14, no. 6, pp. 10081–10106, 2014, doi: 10.3390/s140610081.
- [25] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Futur. Gener. Comput. Syst.*, vol. 63, pp. 56–75, Oct. 2016, doi: 10.1016/j.future.2016.04.016.
- [26] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18295–18325, Jul. 2018, doi: 10.1007/s11042-017-5376-4.

## BIOGRAPHIES OF AUTHORS



**Basavaraj Patil**    is presently working as an Assistant Professor at the SDM Institute of Technology, Ujire, Karnataka. He is pursuing a Ph.D. in Computer Science and Engineering at Visvesvaraya Technological University, Belagavi. He obtained his M. Tech and B.E in Computer Science and Engineering from SDM College of Engineering and Technology, Dharwad, and Rural Engineering College, Hulkoti respectively. His research interests include computer networks, wireless sensor networks, and cryptography. He has published 8 papers in International Journals and Conferences. He is a life member of ISTE, member of IE(I) and IAENG. He can be contacted at email: [bbpatilcs@gmail.com](mailto:bbpatilcs@gmail.com).



**Dr. Sangappa Ramachandra Biradar**    is Professor in the Department of Information Science and Engineering at the SDM College of Engineering and Technology, Dharwad, Karnataka, India. He obtained his Bachelor of Engineering from BLDEA's College of Engineering & Technology, Bijapur. He obtained his Master of Technology from M.I.T., MAHE, Manipal. He received his Ph.D. from Jadavpur University, Kolkata, India. He is guiding six Ph.D. students at Visvesvaraya Technological University, Belagavi, Karnataka. He has published 20 papers in international journals and 32 at International and National Conferences. He is a life member of ISTE, ACM and IAENG. He can be contacted at email: [srbiradar@gmail.com](mailto:srbiradar@gmail.com).