EasyChair Preprint

№ 10512

Review Paper of Performance Analysis in Wireless Sensor Networks

Tiyas Sarkar, Ravi Kumar, Mellachervu Sathwik Kumar,
Sanchit Aggarwal, Achyuta Sandhya and Anand Mohan Shukla

July 8, 2023

Review Paper of Performance Analysis in Wireless Sensor Networks

Tiyas Sarkar[1], Ravi Kumar[2], Mellachervu Sathwik Kumar[3], Sanchit Aggarwal[4], Achyuta Sandhya[5], Anand Mohan Shukla[6]

Department of Computer Science Engineering, Lovely Professional University, Jalandhar - Delhi, Grand Trunk Rd, Phagwara, Punjab 144001

Email: [a)] tiyas.11901657@lpu.in [b)]ravik.cs.19@gmail.com
[c)]sathwikkumarmellachervu0712@gmail.com [d)]sanchitashpit2001@gmail.com
[e)]sandhyaroyal1125@gmail.com [f)]anandshukla8933@gmail.com

Abstract In recent times where everything works under the influence of technology, the wireless sensor networks mostly used where the communication happens in between the machines. As the wireless sensor networks are wireless in nature and it's accessible to network community and it has high chances of getting hacked, so we need to have a protection for the data in the network and to effectively protect the information, WSNs must always be authenticated, and shared keys must be created between deployed sensor nodes and their peers. Security researchers have attempted on numerous occasions to encrypt such data in this fashion. They are trying to discover solutions through multifactor authentication schemes. Regrettably, the bulk of their schemes are susceptible to potential security flaws, such as user impersonating assaults. To decrease computational and communication costs, a spatially unclonable characteristic safe authenticating & identifying method is suggested for biometric technology authentication and authorization. Furthermore, to preserve the anonymity of the session key, an indestructible session is established between the client, ground station, and nodes via an adaptive key exchange replace procedure. We exhibit a comparison to employing a detailed analysis.

Keywords Authentication, WSN, multifactor, Computation overheads, Secure session key, Sensor node, Hash Function, Fuzzy Logic.

INTRODUCTION

Wireless sensor network are assessing and evaluating that integrate tiny actuators and sensor components with general-purpose computer units. With the introduction of Mini micro-sensors and minimal power wireless transmission, the proposed application of sensor networks that are wireless is diversification. Remote sensor networks, in contrast to standard sensor networks, include numerous sensors that are tightly bound. To produce robust, resilient, and long-lasting networks, these sensor nodes execute extensive signal processing, computing, and network self-configuration. Sensor networks, in particular, do local processing to decrease communication and hence energy consumption. The cluster-based methodological approach is, in our opinion, the most efficacious and adaptable routing approach for WSN. Clustering is a crucial cost-cutting feature in cluster based sensor networks. The term "cost" in this context refers to the expense of establishing the business.

The above section provides a synopsis of security challenges of WSN. Let's start with WSN limits and security. These networks' requirements, as well as innovative management assaults and countermeasures of WSN. Next comes the wider context of the security issue at hand. Encryption methodology, key distribution, secure routing, secure data aggregating, intrusion detection, and authentication and authorization are the six areas into which these concerns are grouped. Many advantages as well as disadvantages Explain, compare, and assess security protocols & In each of these categories, there are additionally certain open research questions addressed.

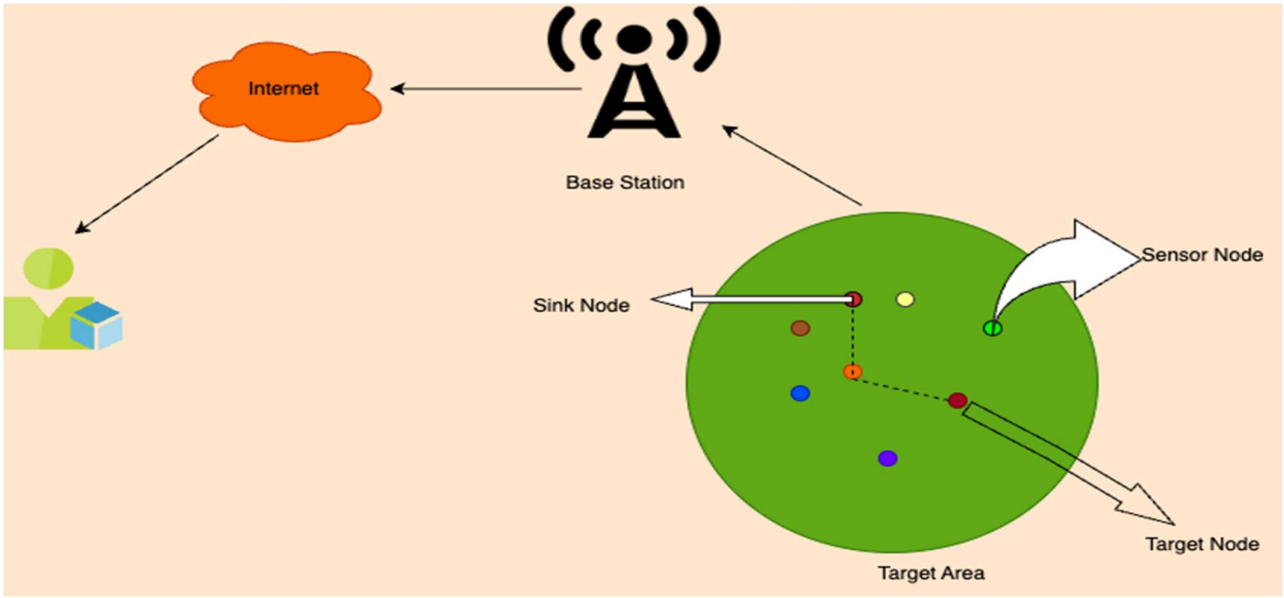

FIGURE 1. *Architecture of the Wireless Sensor Network.*

Authentication using multifactor: Multifactor authentication (MFA) is a security solution that validates user authentication using multiple methods. It is more secure than standard authentication methods. MFA requires something users know (like a password) and something they have (like a mobile phone or biometric information). Authentication using a certificate is more secure and reliable than password-based authentication. To sign in, the user presents their certificate and the server validates it. The server then uses cryptography to determine if the user's private key is connected to the certificate, actually It's like having a driving license or passport.

Authentication using Swarm Intelligence: A Swarm Intelligence security is built around identification and authentication. It is critical for a mass robot to understand if it is engaging with an authenticated robot. Various mass environment executions have different methods of authenticating robots inside the organization system. Some of them employ group IDs, while others use personal identities that must be given on a regular basis. Attacks can target an entity's authentication, confidentiality, integrity, and availability since identities can be faked or altered. As a result, robot identification in swarm intelligence environments is a problematic area of security challenges. Management is another critical part of security in swarm systems. Cryptographic keys must be controlled in this section. These keys specify which robot pairs can get security services & this key needs to be updated.

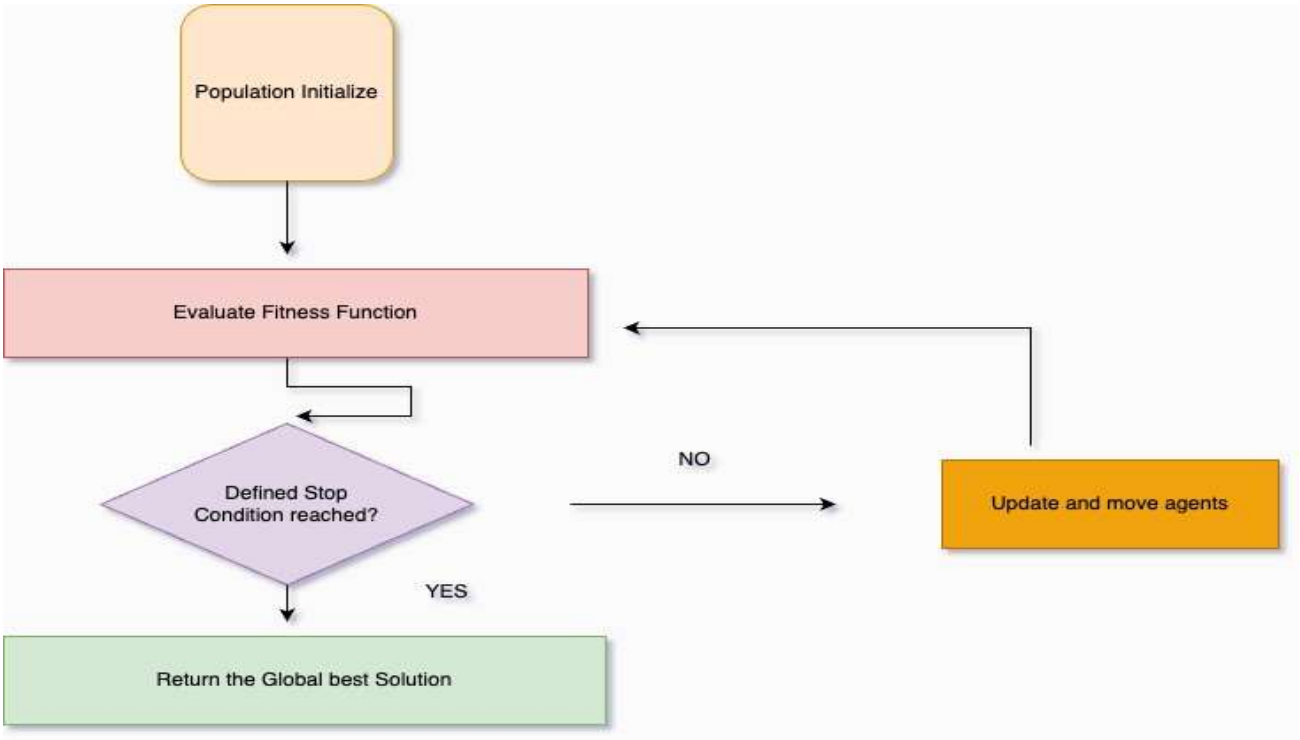

FIGURE 2. *Swarm Intelligence Algorithm.*

Message authentication code (MAC): Basically, MAC is used as an authentication scheme. We can observe these authentication features to the simple textual content collectively with the key and resulting in a fixed-length code recognized as MAC. The MAC is also known as message digest and acts as an authenticator. As a result, the sender or recipient must use this fixed-length code to authenticate (MAC) as shown in Fig. 1 We can apply MAC feature with a secret key on a simple message which produces a fixed-length MAC value. The reversibility from the MAC code to the unique message is now not possible.

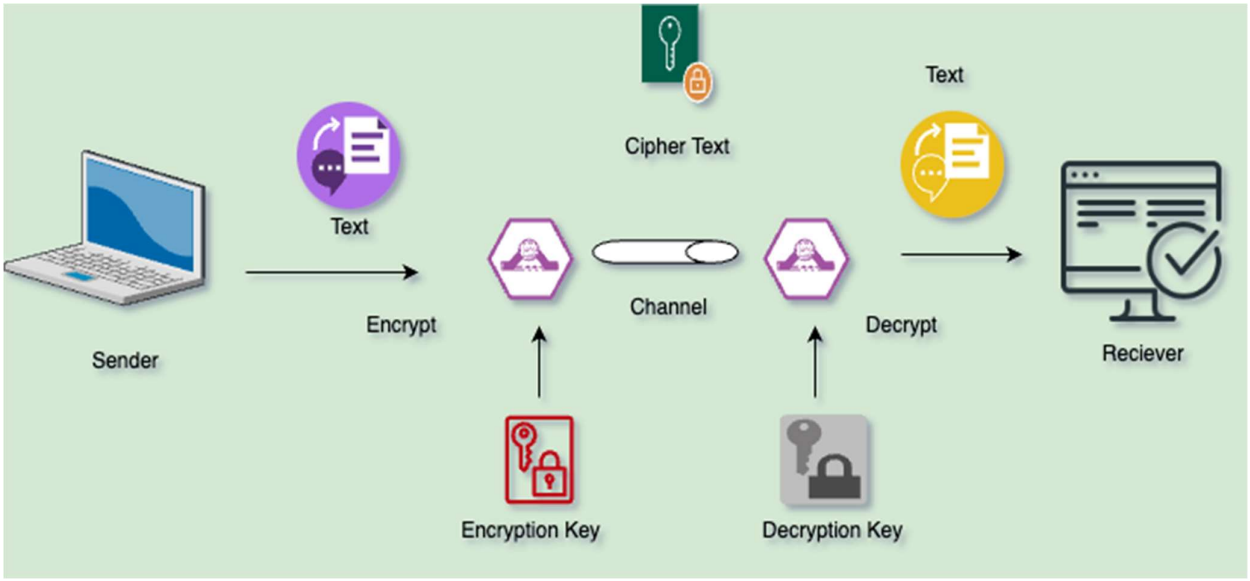

FIGURE 3. *Message Encryption and Decryption.*

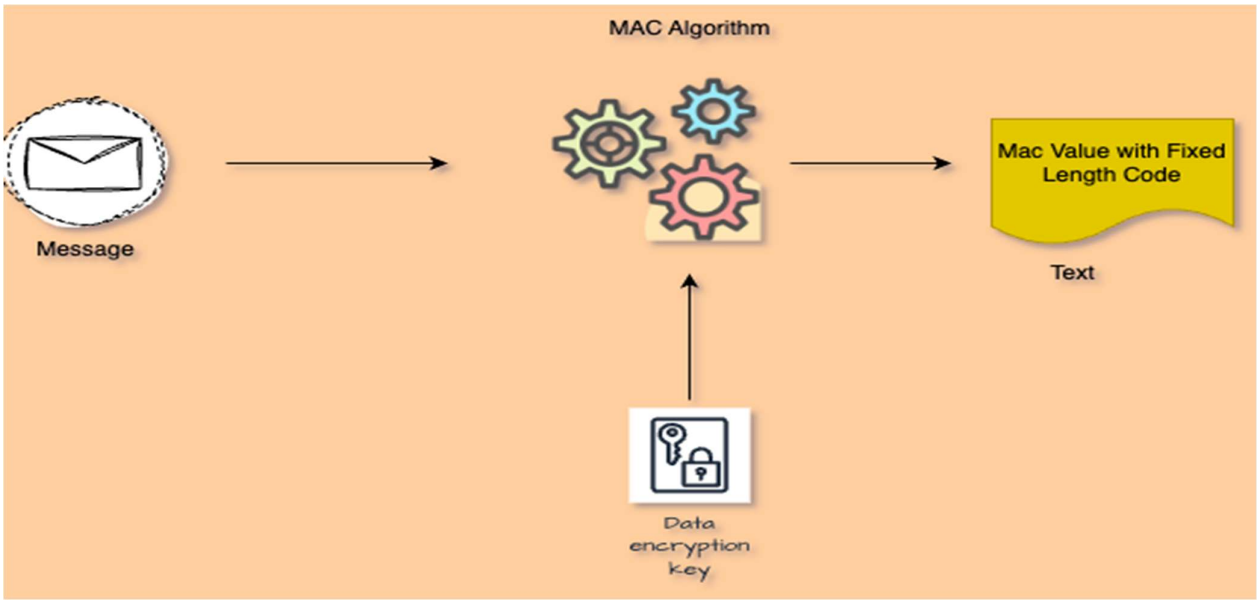

FIGURE 4. *MAC Function Process after Applying on Message.*

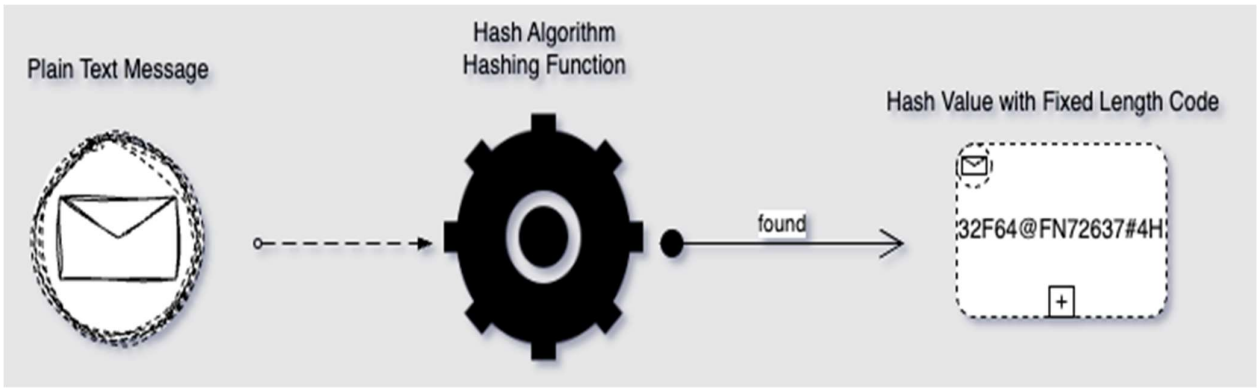

FIGURE 5. *Apply Hash Function on Message.*

Hash Functions: As opposed to MAC, this method uses the hash function to construct fixed-length code, often known as hash code, on plain text that is not dependent on the key (h). An example of a fixed-length code is in this instance, authenticator bode. So, this authentication code must be provided whether the sender wants to authenticate the recipient or the recipient wants to authenticate the sender, as shown in Fig. 3. The hash function will be applied to the plain message to obtain a fixed-length hash code (h). As this hash code is unidirectional, communication is more secure.

Authentication using Fuzzy Logic: First, the associated works pertaining to how to balance energy consumption and improve the lifespan of WSNs were specified. The absence of clustering techniques was then investigated. Based entirely on this study, a qualified sense based completely energy green Clustering method (FLEEC) was presented. The set of rules was examined using the simulation programmed NS2. The outcomes demonstrated that it's significantly more powerful than other clustering protocols such as LEACH and CHEF in terms of energy performance. WSN durability, however, remains an important research subject. According to the authors, future research will focus on themes such as how to collect moving intensity and figures concurrently for WSNs, as well as how to appropriately route several of the cluster heads.

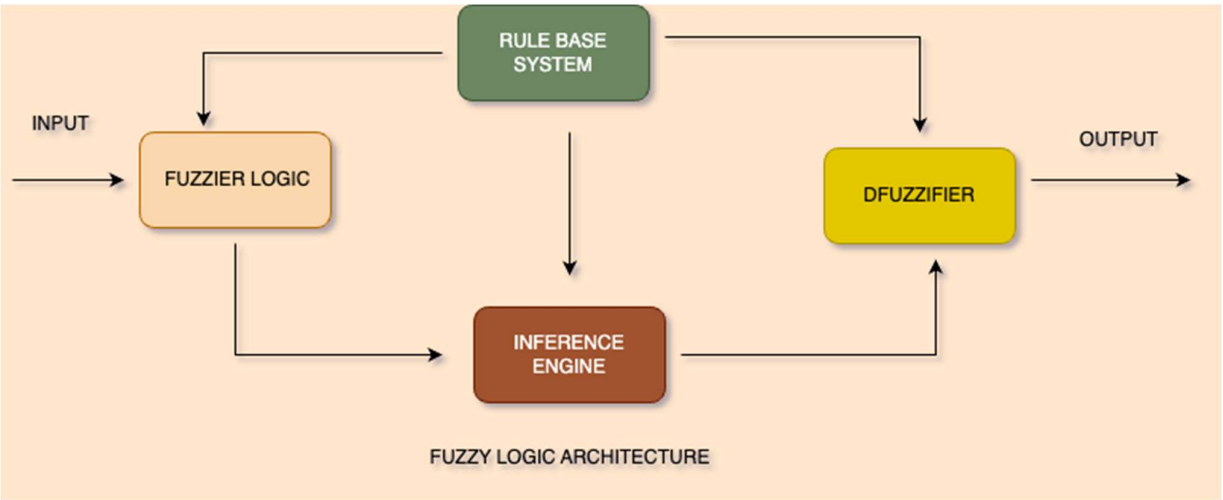

FIGURE 6. *Fuzzy Logic Architecture.*

CONTRIBUTION

This paper describes existing authentication on wireless sensor networks and also provides a comparative analysis considering different matrices. Therefore, comparative verification analysis for authentication is discussed. The essential contributions of this notes are reported as follows:

• By taking communicational and computational cost criteria into account, an examination of the existing authentication method and network security techniques is discussed. The authentication schemes also highlight future areas for research, which is helpful for academics working in this area.

• The remainder of the paper might examine the various WSN architectures and how they affect security. For example, due to their decreased communication and power consumption and evaluation of the efficacy of various Intrusion detection and prevention systems are examples of security methods. firewalls, and security-aware routing protocols, hierarchical WSN architectures may be more secure than flat architectures.

Therefore, the importance of protecting WSNs to ensure their continuous usage in diverse applications might be highlighted in this study on the contribution of WSNs to security. In order to create a user authentication strategy that is better than the current one, an analysis of the current user authentication system is presented.

LITERATURE REVIEW

During the last few years, there are so many authentication mechanisms for secure data sharing in WSNs which have been introduced before. The majority of authentication techniques focus on the communication parties generating Hash-based Message Authentication Code (HMAC). Abdul et al. [1] discuss a Hardware Implementation of Effective Framework using Hash Function. However the limitation of the schemes are Problem of poor security & Power consumption of sensor nodes. Elshamy et al. [2] discuss Secure Z-MAC Protocol where a Preferred answer for protection attack using elliptic-curve encode and IHOP. However limitation of the schemes are Improve data integrity & encryption. Dinesh et al. [3] discuss a Fuzzy based hybrid BAT and firefly algorithm for optimal path selection using hybrid BAT & Fuzzy Logic. The scheme for analyzing the security of wireless sensor networks through the utilizing of SIEM and a multi-agent approach has limitations in terms of its high throughput and low energy consumption. Although it utilizes security information and event management, its improvement in terms of slowly converging with big data analytics is progressing gradually[4]. Ravi et al. [5] discuss a Multifactor authentication scheme for Intelligent IOT enabled WSN using session key. However, the limitations of the scheme are denial of service, node compromise attacks, and 150 the problem of updating passwords is possible. Sudha et al. [6] Pulse detection of jamming attack by utilizing swarm intelligence. However, the limitations of the scheme are Identifying and mitigating the jamming attack Detection. Zhang et al. [7] describe objective to enhance the security and energy efficiency of Internet of Medical Things (IoMT) in healthcare, which will be achieved through the use of an energy-efficient routing protocol called ECC-EERP. However, the challenge is to ensure the optimization of communication networks for better effectiveness.

REFERENCE	SCHEME	SECURITY METRICS	METRICS	RESEARCH LIMITATION
2019 [14]	Biometrics as well as smart cards are part of a two-factor remote user authentication approach for sensor networks that are wireless.	Session key, mutual authe ntication protocols, perfect forward confidentiality, and user request.	Cryptographic keys, mutual authentication mechanism com plete forward confidentially, and user request.	Human impersonation attack and sensory node capture attacks are ineffective at providing mutual authentication and user anonymity.
2020 [11]	Security Assessment of Wireless Sensor Networks Using SIEM and a Multi-agent Methodologic al approach.	This same Security Information and Event Management (SIEM) strategy is utilized in combination with a multi-agent paradigm.	artificial immune system Agents that gather data, a coordinating agent (supervisor), and localized detection systems for intrusions (IDSS).	Increasingly converges with big data analytics. Ingesting data from the several sources (often through bespoke connectors) and responding with escalating storage requirements. Tools.
2021 [23]	Anonymous access authentication recommendation for big data wireless sensor networks.	Access authentication tactic for massive data sensor networks that are wireless. (AAA-WSN).	High level of efficiency in the forward secrecy. Scheme is resilient from the most recently known attack that Environments supporting real-time data.	Improving field of user anonymization andmutual authentication.
2022 [34]	Genetic Algorithm for WSN Network Security Situational Awareness.	The biometric key was generated using genetic algorithm extraction technology as well as the hash function.	Suitable for complexWSN environment for data privacy protection in WSN. Two-factor user authentication scheme.	Significantly improve the system for intrusion detection, such as low detection speed, excessive load, and too late to deal with huge datasets.
2022 [26]	Secure Z-MAC Protocol as a Recommended WSN Possible Attack Mitigation	Incorporate the Z-MAC protocol using IHOP and elliptic-curve encryption.	Flooding assaults, black hole attacks, and DDoS Attack on message manipulation	Improve dataintegrity and encryption.
2022 [39]	Hardware Implementationof Effective Framework between Security and QOS for WSN.	Intrusion detection unit. Hash-based Message Authentication Code (HMAC) and Advanced Encryption Standard (AES).	Remote communication, Hardware implementation, Hostility of the operating environment.	Problem of poor security. Power consumptionof sensor nodes

2023 [24]	Offer Energy and Security Enhancement for Healthcare 5.0 on the Internet of Medicinal Things for WSN.	Energy-efficient routing protocol built around elliptic curve cryptography (ECC-EERP)	System for healthcare 5.0 has a high degree of safety and therefore is energy efficient.	To enhance the effectiveness of communication networks.
2023 [20]	WSN optimal path selection using only a hybrid BAT and firefly algorithm utilizing fuzzy logic.	The path is selected to use fuzzy logic, and the selection is enhanced to use a hybrid BAT.	Focus on providing safe transmission of information among node for efficient and scalable data packet delivery to the destination.	Minimum delay, highthrough-put, low energy consumption, decreased overall processing time
2023 [39]	Efficient Encryption with Energy Optimization for Sensor Networks that are Wireless.	Random Possible combination ,Pseudo Algorithmic Cluster Mechanisms	Calculation metrics utilized Energy. Overheads, calculation costs, and time consumption are all factors to consider. GKA (Group Key Agreement) and MPKE (Multipath Key Establishment).	The possibility of many attacks, their intrinsic potency, and their contradiction For use in typical security solutions
2023 [27]	Swarm intelligence for WSN pulse jamming intrusion detection.	Swarm intelligence algorithm	Attacks on IEEE802.15.4 encompass jamming, denial of sleep, tampering, and cheating.	Acknowledging and countering the jamming assault, The detection accuracy is poor.
2023 [29]	Augmentation in performance and security using feature selectionAnd classification technique for WSN.	Fast Correlation based Feature Selection n (FCBFS) with XG-Boost.	NSL-KDD intrusion detection benchmark dataset.	Used it for training in addition to nature-inspired hybrid algorithms. Stack-based FS algorithms can enhance IDS models.
2023 [25]	Multifactor authenticationscheme for Intelligent IO enabled WSN.	Session key, Mutual Authentication Hash Function andFuzzy extractor.	Computational communication andcost and security. Sensor node's mutual authentication on Intelligent IOT enabled WSN.	Employed to Eliminate guessing of offline passwords and biometric keys. Acquire anonymity to Defend against base station impersonation attacks.

TABLE 1. Literature Review of Authentication Schemes in Wireless Sensor Network .

OPEN CHALLENGES

An evaluation of existing user authentication documentation on Wireless Sensor Network presents a number of challenges, stated as follows:

- To improve security, wireless sensors should be authenticated in a broadcast manner, this will also reduce computational and communication costs. However, it can be difficult to authenticate mobile sensor nodes due to their limited energy and computing power. Additionally, mobility protocols may not always work well with these nodes.

- Moreover, wireless connection makes it easy for an additional party to intercept sensor communications. A distributed denial of service attack, for example, is one of the most challenging security risks (DDoS attack). The goal of this exploit is to disrupt the sensor network's function and appearance.

Furthermore, we assume that one of the possibilities that researchers might explore in order to create adequate protection for WSNs is to use new technology in creating devices capable of offering excessive speed, low cost, low energy consumption, and adequate storage space. The authors stated that their sketch is sufficient to allow fast execution of several complex security algorithms including such the Advanced Encryption Standards (AES), Elliptic Curve Cryptography (ECC), local intrusion detection systems (IDSS), and Secure Hash Algorithm. Additionally, their schematic allows simultaneous sequence unfold spectrum and can provide robust wireless communication.

PERFORMANCE ANALYSIS OF USER AUTHENTICATION ALGORITHMS

Here we compared the performance analysis of existing schemes based on energy efficiency as shown in figure 7 where Zubin et al. providing the best energy efficiency cost result.

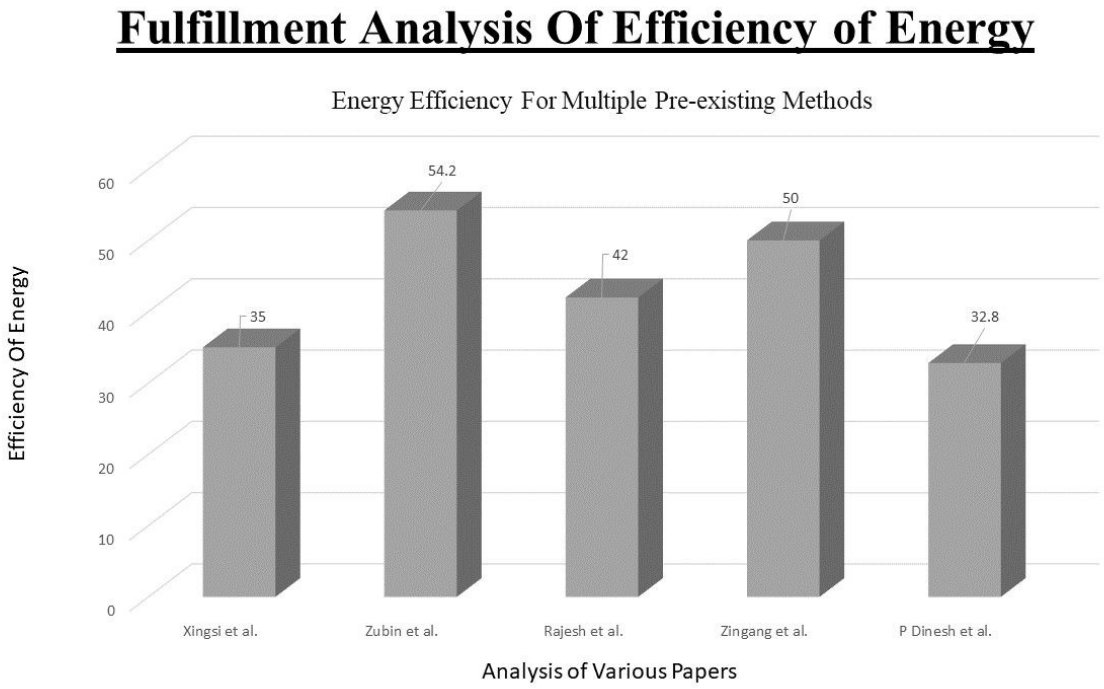

FIGURE 7. *Energy Efficiency Overhead for Various Existing Methods.*

PERFORMANCE ANALYSIS OF USER AUTHENTICATION ALGORITHMS

Here we compared the performance analysis of existing Computational Cost schemes as shown in figure 8 where Ravi et al. providing the best computational cost result.

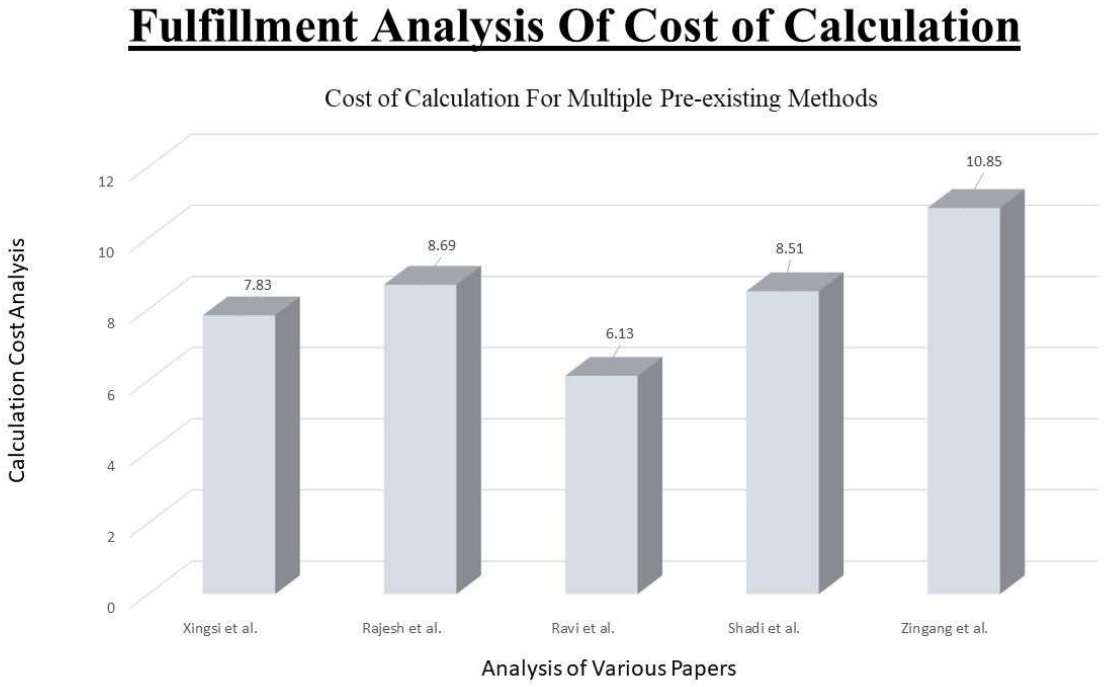

FIGURE 8. *Cost of Computational Overhead for the Various Existing Methods.*

CONCLUSION

An efficient and clean user authentication is constantly a big subject in WSN. Afterward, we developed enhanced key sharing - exchange and authentication protocol technique tailored to IoT WSNs. As we demonstrate in this paper, Xue, Xingsi, et al. and another scheme is susceptible to impersonation and spoofing attacks, text-alteration assaults, and DDoS attacks and is not able to provide adequate security protection and mutual authentication protocols. There is also a problem with their scheme in that it involves too many communication and computation costs. This paper offered an extensive person authentication scheme that retains all protection functionalities and incorporates extra security features for WSNs. The proposed scheme provides a realistic protection against an adversary attempting to breach security. Furthermore, our future investigations revealed that the suggested architecture is appropriate for real-time sensor networks with regard to of computing as well as communication costs. Ultimately, we have evaluated how well our approach measures up to other similar methodologies beside these proposed scheme attempts to keep computational costs down while maintaining security.

In this paper, we gathered all the information on WSN schemes and security methods with research limitations and studied the performance analysis of methodologies like secure schemes of WSN like Two-factor remote user authentication schemes using Biometric, Smart Card, swarm intelligence (SI) and Multifactor authentication schemes for Intelligent IOT-enabled WSN. The multi-factor authentication (MFA) is more secure because if a hacker wants to attack a normal network that does not have multi-factor authentication, then. Multi-factor authentication (MFA) is used to present users with two or more pieces of evidence or factors for authentication. The main goal of MFA is to add an additional authentication factor for added security. This has many benefits for organizations choosing to use MFA in their authentication approach. This could be an important area for future research directions in this area and is rarely applied in WSN.

REFERENCES

1. Abdul-Karim, M.S., Rahouma, K.H. and Nasr, K., 2022. Hardware Implementation of Effective Framework for the Trade-off between Security and QoS in Wireless Sensor Networks. Microprocessors and Microsystems, 93, p.104590.

2. Revanesh, M., Acken, J.M. and Sridhar, V., 2022. DAG block: Trust aware load balanced routing and lightweight authentication encryption in WSN. Future Generation Computer Systems.

3. Sudha, I., Mustafa, M.A., Suguna, R., Karupusamy, S., Ammisetty, V., Shavkatovich, S.N., Ramalingam, M. and Kanani, P., 2023. Pulse jamming attack detection using swarm intelligence in wireless sensor networks. Optik, 272, p.170251.

4. Kumar, R., Singh, S. and Singh, P.K., 2023. A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs. Computers and Electrical Engineering, 105, p.108495.4.

5. Nashwan, S., 2021. AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. Egyptian Informatics Journal, 22(1), pp.15-26.

6. Srinivasan, S., Ramesh, T.K., Paccapeli, R. and Fanucci, L., 2022. Industrial functional safety assessment for WSN using QoS metrics. Heliyon, 8(11), p.e11255.

7. Yadav, R., Sreedevi, I. and Gupta, D., 2023. Augmentation in performance and security of WSNs for IoT applications using feature selection and classification techniques. Alexandria Engineering Journal, 65, pp.461-473.

8. Cao, C., Tang, Y., Huang, D., Gan, W. and Zhang, C., 2021. IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021, pp.1-8.

9. Almansoori, M.N., Elshamy, A.A. and Mustafa, A.A.M., 2022. Secure Z-MAC Protocol as a Proposed Solution for Improving Security in WSNs. Information 2022, 13, 105.

10. Dinesh Kumar, P. and Valarmathi, K., 2022. Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network. Automatika, pp.1-12.

11. Natarajan, R., Lokesh, G.H., Flammini, F., Premkumar, A., Venkatesan, V.K. and Gupta, S.K., 2023. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. Infrastructures, 8(2), p.22.

12. Vasilyev, V. and Shamsutdinov, R., 2020, November. Security analysis of wireless sensor networks using SIEM and multi-agent approach. In 2020 Global Smart Industry Conference (GloSIC) (pp. 291-296). IEEE.

13. Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O.I., Selvaraj, D. and Abdulsahib, G.M., 2023. A Hybrid Cross Layer with Harris-Hawk-Optimization-Based Efficient Routing for Wireless Sensor Networks. Symmetry, 15(2), p.438.

14. Zhang, G. and Ning, Z., 2023. Personal Health and Illness Management and the Future Vision of Biomedical Clothing Based on WSN. International Journal of Data Warehousing and Mining (IJDWM), 19(1), pp.1-21.

15. Cao, C., Tang, Y., Huang, D., Gan, W. and Zhang, C., 2021. IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021, pp.1-8.

16. Roman, R. and Lopez, J., 2009. Integrating wireless sensor networks and the internet: a security analysis. Internet Research.

17. Sharma, K., Ghose, M.K., Kumar, D., Singh, R.K. and Pandey, V.K., 2010. A comparative study of various security approaches used in wireless sensor networks. International Journal of Advanced Science and Technology (IJAST), 17, pp.31-44..

18. Singh, S.K., Singh, M.P. and Singh, D.K., 2011. A survey on network security and attack defense mechanism for wireless sensor networks. International Journal of Computer Trends and Technology, 1(2), pp.9-17.

19. Muhajjar, R.A., Flayh, N.A. and Al-Zubaidie, M., 2023. A Perfect Security Key Management Method for Hierarchical Wireless Sensor Networks in Medical Environments. Electronics, 12(4), p.1011.