Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 2, June 2025, pp. 387~395
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i2.6216

Mitigating Wormhole Attacks' Risks within Wearable Body Network

Mohammed Abdessamad Goumidi[1], Ehlem Zigh[2], Adda Belkacem Ali-Pacha[3]
[1,2,3]Coding and Information Security Laboratory (LACOSI), Electronic Department, Electrical Engineering Faculty, Sciences and Technology University of ORAN- Mohamed Boudiaf (USTO-MB), Oran, Algeria.

Article Info

Article history:

Received Jan 5, 2025
Revised May 15, 2025
Accepted Jun 1, 2025

Keywords:

Mitigating
Risks
Wormhole attacks
Trusted secure routing protocol
Wearable body network

ABSTRACT

In this research, we sought to develop a trust and secure routing protocol based on the Ad-hoc On-Demand Distance Vector (AODV) routing to combat wormhole attacks in Wearable Body Networks (WBNs), which integrates a routing strategy that leverages the path-checking method to detect and isolate paths affected by wormhole attacks effectively, it employs a routing technique that prioritizes nodes with the most heightened remaining energy during data transmission, along with a mixed cryptographic algorithm that combines the modified One Pad Time with the modified Affine ciphers to ensure safe transmission against malicious biosensor threats. Experimental findings indicate that our proposed protocol transcends the classic AODV routing protocol across all evaluation parameters, including packet delivery ratio, throughput, and energy consumption. Its primary advantage lies in considering multiple factors, like detecting unauthorized biomedical biosensors, efficient energy utilization in the network, and secure data transmission—differentiating it from other safe routing protocols. Moreover, the mixed encryption algorithm enhances efficacy and bolsters sensitive data security compared to classic cipher methods like the One Pad Time and Affine ciphers.

Corresponding Author:

Mohammed Abdessamad Goumidi
Coding and Information Security Laboratory (LACOSI)
Electronics Department, Electrical Engineering Faculty
Sciences and Technology University of ORAN- Mohamed Boudiaf (USTO-MB)
El Mnaouar, BP 1505, Bir El Djir 31000, Oran, Algeria
Email: mohammedabdessamad.goumidi@univ-usto.dz

1. INTRODUCTION

Wearable Body Networks represent a specialized category of Mobile Ad Hoc Networks composed of numerous medical sensors positioned around, on, or in the person's body to monitor physiological signs. These physiological signs will be transmitted to a medical server through an access point using wireless technology [1,2,3], enabling physicians to gain valuable insights into human health [4,5].

However, The distributed architecture and network mobility [6,7,8] make it susceptible to various denial-of-service attacks, including wormhole attacks, which can jeopardize the sensors within the system [9]. This study aims to address this challenge. A wormhole attack is a passive attack that establishes an unauthorized connection between two communicating nodes, causing legitimate nodes to route their data through this link. This act can result in data interception and compromise the integrity of the affected nodes [10,11,12,13,14,15,16,17].

Many scientific researchers used trust routing protocols to reduce the wormhole attack risk in the network. For example, Asha Mansore and Surbhi Koushik [18] proposed a wormhole prevention and detection technique within MANET (Wban by example) based on hope count analysis of all available paths from the source to the destination, which is then compared to a threshold value. The suggested technique is incorporated into the AODV routing protocol and demonstrates a network performance improvement in throughput, Delivery packet ratio, and energy consumption. Similarly, Zulfiqar Ali Zardari et al. [19] presented a

lightweight method to detect and prevent wormhole attacks in MANET (WBAN example). The suggested method is incorporated into the AODV routing protocol, in which the source biosensor computes the means sequence digit of the Route REPly (RREP) packets. If the corresponding biosensor sequence digit exceeds the calculated means value, all traffic will dumped, and the sensor will labeled as malevolent. The suggested approach is less complicated, power-efficient, and improves network lifetime.

Current protocols designed to mitigate the risks associated with wormholes and enhance network security and performance face certain limitations. For example, they often select routing paths without considering the residual energy levels of the participating nodes, which can lead to the overutilization of already weakened sensors and result in their premature failure. Additionally, these approaches typically lack acknowledgment mechanisms to verify the integrity of the transmission path, making it difficult to detect issues such as packet loss, route failure, or wormhole attacks. Furthermore, data is frequently transmitted in plaintext without encryption or protection against injection and eavesdropping, exposing the system to security threats such as data interception, manipulation, and forgery. Such limitations severely compromise network security, reliability, and energy efficiency.

To overcome these limitations, we proposed a trust-safe routing protocol to mitigate wormhole attacks within Wireless Body Area Networks (WBANs). We hypothesized that our Trust-Safe AODV (TSAODV) routing protocol will significantly improve the detection and mitigation of wormhole attacks in Wireless Body Area Networks (WBANs) by combining a path verification strategy, energy-aware routing decisions, and a robust cryptographic approach that utilizes a modified One-Time Pad and a modified Affine cipher. Our TSAODV aims to achieve a higher wormhole attack detection rate than the standard AODV protocol, leveraging path verification and mechanisms for detecting illegitimate sensors. The secure path validation and message acknowledgment (through the Message Receipt Packet - MRP) incorporated in our TSAODV is expected to enhance throughput, increase packet delivery ratios, and reduce packet losses, even under wormhole attacks.

Additionally, the protocol will distribute energy consumption more efficiently among nodes by prioritizing those with the highest remaining energy, thereby extending the overall lifespan of the network. To validate these hypotheses, we will conduct simulations in NS2, utilizing a WBAN environment consisting of 16 sensor nodes. The scenarios will include wormhole attacks simulated by colluding nodes. We will collect and compare metrics such as Packet Delivery Ratio (PDR), Energy Consumption, Throughput, and wormhole detection accuracy against standard AODV and other Trusted protocols.

The expected outcome is that TSAODV will demonstrate superior performance in secure, energy-efficient, and reliable data transmission, confirming its suitability for WBANs. However, scalability to larger, more generalized networks may require adaptation due to the overhead introduced by cryptographic and acknowledgment mechanisms.

2. RESEARCH METHOD

To fulfill our research objectives, we complete the following tasks:

i. Set up a WBN with the classic AODV routing protocol under wormhole attacks using the NS2.35 simulator.

ii. Propose a trust-safe AODV routing protocol that incorporates a cipher algorithm, then examine the performance of this trust-secure routing protocol (TSAODV) and compare it to the classic AODV protocol.

2.1. WBAN Simulation Task

The primary objective of this task is to create and simulate an EEG network that accurately reflects a real-world EEG setup utilizing Network Simulator 2.35. This wearable network includes multiple EEG biosensors strategically positioned on the person's head in a star structure with a central sink. We consider that the transmission between the portable biosensors and the sink isn't secure and may be susceptible to wormhole attacks. Such attacks exploit vulnerabilities in the AODV routing protocol, potentially jeopardizing biosensors' integrity within the network.

2.2. Trusted secure routing protocol implementation Task

The second task focuses on developing a trust-secure routing protocol to counter wormhole attacks in Wearable Body Networks. The TSAODV, an improved version of the AODV protocol, is designed to enhance communication security within WBANs. It facilitates unicast and multicast packet transmissions, even in scenarios with dynamic sensor movement. A key strength of TSAODV lies in its holistic approach to detecting

malicious sensors, improving energy usage, and assuring secured data transmission. The protocol achieves reliable packet delivery through two distinct operational phases:
− Route Request and Reply Phases.
− Data Transmission Phase.

2.2.1 Route Request and Reply phases

During the Route REQuest and REPly phases, a source sensor initiates communication. It begins by sending RREQ packets and waits to receive RREP packets from different biosensors. Then, it stores the received RREP packets with their corresponding sequence digits. The source biosensor then computes the sequence digits average of all RREP packets as outlined in eq. 1.

$$Average = \sum_{i=1}^{k} SN_i /k \quad (1)$$

Where: SN_i is the sequence number of the route reply packets and k is the the total reply (RREP) count.
Next, it compares the sequence digit incorporated in the route reply packet of each sensor in a specific available path with the average value obtained in Equation 1. If the sequence digit surpasses the mean value, the source sensor concludes that wormhole attacks exist in the considered path. Upon identifying harmful routes, the associated next hop entry is removed to prevent the suspected neighbor from being utilized for routing. Finally, different routes are analyzed using the same method to determine the reliable path, which contains sensors with the highest remaining energy for delivering the data to the final recipient sensor. The source sensor computes the remaining energy of each trust path as in eq. 2:

$$RE_{PATH} = \frac{\sum_{i=1}^{S} RE_i}{Hope\_Count} \quad (2)$$

Where: RE_i is the remaining energy of each sensor in the same path, and S is the total sensor in the path.

2.2.2 Data Transmission phase

In this phase, the source sensor exchanges ciphered message packets with the destination sensor by utilizing a mixed encryption method that integrates the modified One Pad Time with the modified Affine ciphers. During the data transmission phase, the source sensor proceeds as follows:
− It ciphers the original information using the modified One Pad Time cipher as in eq. 3:

$$C_{MOPT}(i) = (Original\_Information_i + Key_i)\ mod\ 38 \quad (3)$$

− It selects two positive digits m, n different to zero with $\gcd(m, S_A)$, and $S_A$the alphabet size. Then it ciphers the ciphered information with the modified One Pad Time cipher using the modified Affine cipher as in eq. 4:

$$C_{MA} = (m.C_{MOPT}(i) + n)\ mod\ 38 \quad (4)$$

− Finally, it transmits the ciphered data with the modified One Pad Time cipher to the receiving sensor via a trust route with the highest remaining energy.

Upon reception of the ciphered information. The recipient initially deciphers the ciphered data with the modified One Pad Time cipher using the modified Affine cipher as in eq. 5:

$$D_{MA} = m^{-1}(C_{MA} - n)\ mod\ 38 \quad (5)$$

Then, it deciphers the deciphered data with the modified Affine cipher utilizing the modified One Pad Time cipher as in eq. 6:

$$D_{MOPT} = (D_{MA}(i) - n)\ mod\ 38 \quad (6)$$

The suggested cryptosystem enhances the traditional One Pad Time and Affine ciphers by increasing the alphabet size from 26 to 38, unlike classic ciphers [20, 21, 22, 23, 24]. Table 1 [25] shows the modified alphabet table of our cryptosystem, which contains letters with specific characters and associates their numeric values. This increase in alphabet size raises the key number of the traditional affine and One Pad Time ciphers. Moreover, in One Pad Time, the secret key is randomly generated and utilized only once to cipher a message, which is then deciphered again with the duplicate key. This feature makes it invulnerable to force-brute attacks. Furthermore, the combination of both ciphers increases the complexity of our cryptosystem.

Table 1. Alphabet table of modified One Pad Time-modified Affine cipher.

Symbols with their positions															
a	b	#	c	d	*	e	f	+	g	h	-	i	j	$	k
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
l	?	m	n	!	o	p	@	q	r	%	s	t	>	u	v
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<	w	x	^	y	z										
32	33	34	35	36	37										

This protocol ensures high reliability by enabling acknowledgment transmission upon successfully delivering packets from the transmitter to the receiver. Once the recipient biosensor has obtained all packets, it sends a Message Receipt Packet (MRP) back to the transmitter biosensor. When receipting the MRP, the source biosensor validates the total path as trustworthy. This mechanism guarantees the successful data packet delivery and acknowledgment through the MRP.

The TSAODV routing protocol significantly improves network safety by addressing key aspects like detecting unlawful biomedical biosensors, efficient energy utilization, and secured communication. However, the classic AODV routing protocol lacks integrated network safety measurements.

3. RESULTS AND DISCUSSION

We conducted the proposed Trust-Safe Routing Protocol (TSAODV) simulation using the NS-2.35 network simulator to evaluate its effectiveness in mitigating wormhole attacks within a Wireless Body Area Network (WBAN). The network topology comprises sixteen EEG biosensors organized in a star configuration, with a central sink node responsible for data collection. To simulate a hostile environment, two biosensors were configured as malicious nodes, colluding to create a wormhole tunnel and disrupt the routing process. The simulation environment reflects the real-world constraints of WBANs, including limited node mobility and energy. We utilized Key performance metrics such as packet delivery ratio, energy consumption, and wormhole detection rate to assess the protocol's reliability, security, and efficiency. The proposed TSAODV protocol integrates a path verification mechanism and trust-based routing that prioritizes nodes with higher residual energy, along with a Message Receipt Packet (MRP) scheme for secure acknowledgment, making the simulation scenario both realistic and comprehensive for testing the protocol under attack conditions. Table 2 presents the various metrics utilized for the network simulation.

Table 2. Simulation Set-up.

Metrics	Specifics
Software	NSv2.35
Total biosensor	16
Physical link	Wireless
Routing Protocols	AODV/TSAODV
Wormhole attack sensors	2
The initial energy of the biosensors	150J
Simulation time	14s

To validate the effectiveness of the proposed Trust-Safe AODV (TSAODV) protocol, we conducted a series of quantitative experiments using the NS2.35 simulator. The simulation setup involves a Wireless Body Area Network (WBAN) comprising 16 biosensor nodes deployed in a star topology, with two nodes acting as malicious wormhole collaborators. The metrics used to assess performance include Packet Delivery Ratio (PDR), throughput, energy consumption, and wormhole detection rate, as shown in Table 3.

Quantitative results demonstrate that TSAODV significantly outperforms standard AODV and other convolutional protocols under the same conditions. For instance, our TSAODVRPBOC protocol achieves an impressive PDR of approximately 99.77%, with a data rate of 21.88 Kbit/s, energy consumption of 12J, and detection rate of 100%. In contrast, the AODV protocol records a PDR of around 99.21%, a data rate of 21.77 Kbit/s, and an energy consumption of 15J, with no wormhole attack detection. The TSAODV routing protocol yields several significant improvements compared to the AODV protocol. Notably, there is a slight enhancement in the Packet Delivery Ratio (PDR) of 0.56%, attributed to the rapid and efficient packet delivery to their terminus biosensors. It can detect and isolate wormhole attacks earlier in the communication process, effectively preventing disruptions in packet delivery, unlike the AODV protocol, which suffers from a significant packet loss rate due to these wormhole nodes. Then, we noticed a marginal increase in the throughput of 0.11 Kbit/s compared to AODV. This improvement arises from TSAODV's ability to route data through trust medium biosensors, which are determined based on their high residual energy, ensuring safe packet delivery inversely to the AODV protocol, which suffers from packet loss caused by malicious nodes

with low energy, which disrupts the communication process. There is a little decline and improvement in energy consumption of 1.39J when comparing the TSAODV routing protocol to AODV. This decrease is because TSAODV selects the path with the fewest middle sensors and the heightened remaining energy, ensuring efficient use of delimited resources, particularly energy. However, the AODV protocol is vulnerable to wormhole attacks, where a tunnel is created between the sender and final recipient biosensors, allowing unauthorized access to secret data. Furthermore, TSAODV exhibited a wormhole detection rate of 100%, unlike the AODV protocol, which lacks path verification or acknowledgment mechanisms. Such attacks can use the behavior of nodes and facilitate further unauthorized intrusions. Additionally, they establish two long-distance tunnels between nodes, leading to interference that involves normal nodes, ultimately resulting in transmission loss and increased power drain. These quantitative findings confirm that TSAODV is a reliable and efficient routing protocol tailored for WBANs capable of mitigating wormhole threats while preserving energy and ensuring timely data transmission.

Table 3. Routing protocols performance analysis.

Routing protocol kind	Data rate (Kbit/s)	PDF (%)	Energy consumption (J)	Detection rate (%)
AODV in [25]	21.770	99.21	28.3034	No Available
TSAODV (2025)	21.880	99.77	26.9176	100

Table 4 presents a comparison of the performance of the mixed cipher technique, which combines the modified One Pad Time cipher used in the TSAODV with the modified Affine cipher against traditional methods such as the One Pad Time and Affine ciphers. As outlined in the third section, the proposed cipher technique exhibits greater complexity than the classical One Pad Time and Affine cipher algorithms. The heightened complexity significantly reduces the network's vulnerability to attacks from malicious nodes. Consequently, eavesdroppers would encounter considerable challenges in decrypting the ciphertext or utilizing brute-force methods to compromise the cryptosystem, owing to the enhanced intricacy of the ciphertext generated by this novel approach. The mixed encryption technique enhances the security and effectiveness of text message encryption.

Table 4. Cryptosystems features analysis.

Cryptography cipher algorithm kind	Characteristics	Specifications
Our modified One Pad Time- modified Affine ciphers (2024)	Structure	Symetric
	Alphabet size	38
	Keys update	Yes
	Comlexity	High
Traditional One Pad Time cipher	Structure	Symetric
	Alphabet size	26
	Keys update	No
	Comlexity	Low
Traditional Affine Cipher	Structure	Symetric
	Alphabet size	26
	Keys update	No
	Comlexity	Low
Traditional One Pad Time-Affine ciphers [24] (2019)	Structure	Symetric
	Alphabet size	26
	Keys update	No
	Comlexity	Medium

Table 5 presents a performance analysis of our TSAODV routing protocol in comparison to other routing protocols, including the classic AODV as discussed in [25] by V. Rohit et al., as well as similar trusted routing protocols proposed by A. Mansore et al. and Z. Zardari et al. [17-18]. The analysis reveals that the performance of our TSAODV protocol surpasses that of protocols such as the classic AODV as TAODV mentioned in [26], [18], and [19]. The suggested TSAODV protocol establishes a trusted routing path by effectively detecting and isolating wormhole attacks, a capability not present in the traditional AODV protocol. Additionally, it reduces energy consumption during packet routing by selecting the shortest path, characterized by the fewest intermediate biosensors and the highest residual energy. This optimization is lacking in other routing protocols. Furthermore, our TSAODV protocol enhances network security through robust data encryption. Its hybrid encryption method, which combines a modified One Pad Time cipher with a modified Affine cipher, offers improved resistance to brute-force attacks, distinguishing it from other routing protocols.

Table 5. Routing Protocols features analysis.

Features	AODV [26] (2021)	TAODV [18] (2015)	TAODV [19] (2018)	TSAODV (2025)
Trust path	✗	✓	✓	✓
Transmission safety	✗	✗	✗	✓
Energy efficient routing	✗	✗	✗	✓

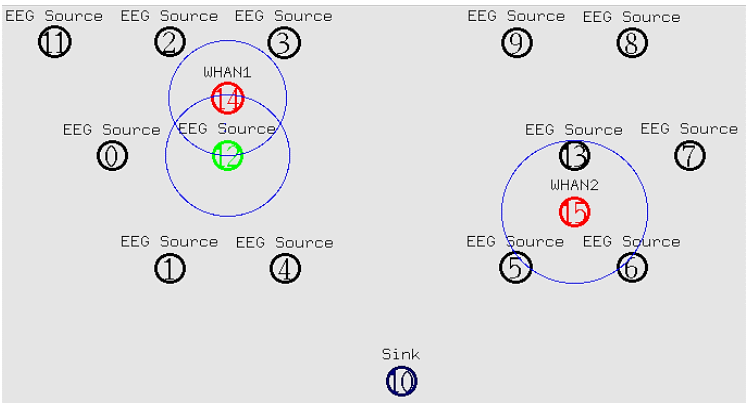

Figure 1. Wormhole attacks under AODV routing protocol.

Figure 1 displays our network simulation screenshot demonstrating wormhole attacks using the AODV protocol at the time (t). We observed that the malevolent sensor with ID digit 14 failed to relay any packets from the EEG source sensor(ID digit 12) to the sink (ID digit 10). Instead, it sent the packets to another unauthorized biosensor with ID digit 15 because wormhole attacks use vulnerabilities in the path discovery procedure of routing protocols. These attacks manipulate the path discovery procedure by positioning themselves strategically with the assistance of two or more colluding sensors. In this scenario, the assailant sensor with ID digit 14 has a higher sequence digit than the legitimate nodes and the shortest route to the final recipient. Consequently, the Route Request (RREQ) generated by the source node with ID digit 12 achieves its destination sooner through the wormhole link between sensors with ID digits 14 and 15, while the Route Reply (RREP) message follows the same route back to the source. In AODV, forward and backward paths are symmetrical, allowing the wormhole biosensor nearest the source with ID digit 14 to capture data packets. It can then relay these packets to the other colluding node with ID digit 15, which might replay, broadcast, or discard them. Furthermore, the two colluding sensors may create loops with packets, ultimately leading to their loss.

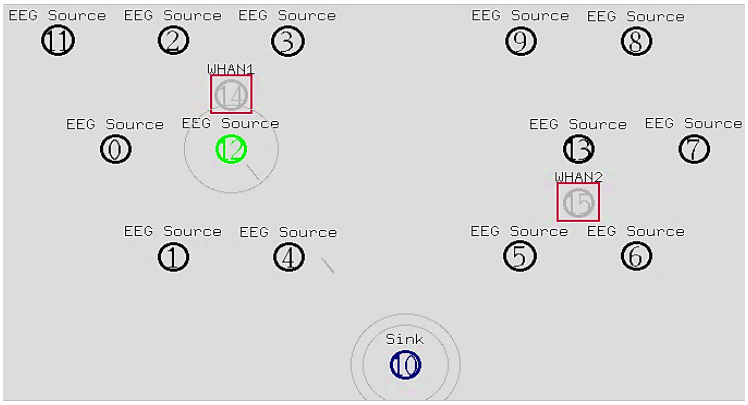

Figure 2. Wormhole attacks under TSAODV routing protocol

Figure 2 displays our network simulation screenshot illustrating wormhole attacks while employing the TSAODV protocol at the time (t). We marked the safe transmission establishment between the transmitting biosensor with ID 12 and the receiving biosensor with ID 10 via an alternative trust path characterized by the most elevated remaining energy selected by the source sensor with ID 12. In the simulation, the transmitting

sensor with ID 12 sends RREQ packets and subsequently begins to receive RREP packets from various biosensors within the network. It retains all RREQ packets along with their respective sequence digits. After calculating the average of these sequence digits, the transmitter compares each route reply packet's sequence digit from the sensors in the available path connecting nodes with ID 12-14-3-9-15-10 to the average value. It identified that the node's sequence digits with ID 14 and 15 exceeded the mean value, leading the source sensor with ID 12 to conclude that wormhole attacks were present along the investigated path. Upon detecting a malicious route, the corresponding next hop entry will deleted, preventing the suspected neighbor from being used for routing. Ultimately, the source sensor with ID 12 verifies the trustworthiness of an alternative path using the same procedure and selects a reliable route that connects directly to the destination biosensor with ID 10. Following the detection and isolation of the malicious path, the origin sender and final recipient sensors securely exchange data, which is encrypted utilizing a modified One Pad Time cipher combined with a modified Affine cipher.

4. CONCLUSION

Despite the numerous applications and advantages of wearable body networks (WBNs), they remain susceptible to various security threats, particularly wormhole attacks. To address these vulnerabilities, we developed a trust-safe AODV routing protocol. This enhanced protocol incorporates several key elements, including trust path analysis, energy availability during routing, and secure data encryption for transmission. The proposed protocol effectively detects and isolates wormhole attacks by utilizing a path verification technique to identify malicious routes. It also takes into consideration the battery life of the medium sensors along the chosen path, thereby ensuring energy efficiency.

. Additionally, secure communication is achieved through information encryption, employing a hybrid encryption method that combines a modified One Pad Time cipher with a modified Affine cipher. Experimental evaluations demonstrate a 0.56% improvement in Packet Delivery Ratio (PDR), an increase of 0.11 Kbit/s in throughput, a decrease of 1.39J in energy consumption, and a wormhole attack detection rate of 100% when using the TSAODV compared to classic AODV and Trust AODV routing protocols. The TSAODV establishes reliable routes by selecting trusted biosensors with the highest remaining energy, thereby enhancing network security through its hybrid encryption method. Additionally, our findings indicate that the hybrid cipher technique used in our proposed protocol exhibits greater resilience against brute-force attacks than traditional single-cipher algorithms, such as standalone modified One Pad Time or Affine ciphers. Moving forward, we aim to expand our approach to address multiple simultaneous attack types targeting WBANs, further strengthening their security and reliability.

REFERENCES

[1] D. S. Bhatti et al., “A Survey on Wireless Wearable Body Area Networks: A Perspective of Technology and Economy,” Sensors, vol. 22, no. 20, p. 7722, Oct. 2022, doi: 10.3390/s22207722.

[2] E. El-Adawi, E. Essa, M. Handosa, and S. Elmougy, “Wireless body area sensor networks based human activity recognition using deep learning,” Sci Rep, vol. 14, no. 1, p. 2702, Feb. 2024, doi: 10.1038/s41598-024-53069-1.

[3] S. B, P. B, A. S, and N. J, “Wireless Body Area Networks: Survey of recent research trends on energy efficient routing protocols and guidelines,” Jul. 22, 2021. doi: 10.21203/rs.3.rs-385025/v1.

[4] M. A. Goumidi, N. Hadj-Said, A. B. Ali-Pacha and E. Zigh, "Detection of Malicious Nodes in WBAN using a Feed Forward Back Propagation Neural Network," 2022 International Conference of Advanced Technology in Electronic and Electrical Engineering (ICATEEE), M'sila, Algeria, 2022, pp. 1-6, doi: 10.1109/ICATEEE57445.2022.10093101.

[5] Q. Liu, K. G. Mkongwa, and C. Zhang, “Performance issues in wireless body area networks for the healthcare application: a survey and future prospects,” SN Appl. Sci., vol. 3, no. 2, p. 155, Feb. 2021, doi: 10.1007/s42452-020-04058-2.

[6] W. I. Khedr, A. Salama, M. M. Khashaba, and O. M. Elkomy, “Security Analysis of Wireless Body Area Network Protocols: A Survey,” 2023.

[7] Laboratory of Coding and Security of Information (LACOSI), Department of Electronic, Faculty of Electrical Engineering, University of Sciences and Technology of ORAN- Mohamed Boudiaf (USTO-MB), Algeria, M. A. Goumidi, E. Zigh, N. Hadj-Said, and A. B. Ali-Pacha, “A Hybrid Intrusion Detection System to Mitigate Biomedical Malicious Nodes,” IJCNIS, vol. 16, no. 2, pp. 117–133, Apr. 2024, doi: 10.5815/ijcnis.2024.02.10.

[8] G. M. Abdessamad, Z. Ehlem, and A.-P. Adda Belkacem, “Mitigating blackhole attacks in wireless body area network,” IJEECS, vol. 36, no. 3, p. 1555, Dec. 2024, doi: 10.11591/ijeecs.v36.i3.pp1555-1563.

[9] M. Hanif et al., “AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks,” Electronics, vol. 11, no. 15, p. 2324, Jul. 2022, doi: 10.3390/electronics11152324.

[10] K. Jae-Dong, “A Comprehensive Analysis of Routing Vulnerabilities and Defense Strategies in IoT Networks,” Oct. 17, 2024, arXiv: arXiv:2410.13214. doi: 10.48550/arXiv.2410.13214.

[11] M. Yaghoubi, K. Ahmed, and Y. Miao, "Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges," JSAN, vol. 11, no. 4, p. 67, Oct. 2022, doi: 10.3390/jsan11040067.
[12] D. S. Bhatti, S. Saleem, A. Imran, H. J. Kim, K.-I. Kim, and K.-C. Lee, "Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions," Sci Rep, vol. 14, no. 1, p. 3428, Feb. 2024, doi: 10.1038/s41598-024-53938-9.
[13] QUEST Nawabshah, Pakistan et al., "Analysis and Countermeasures of Wormhole and Sinkhole Attacks in WBAN," JISR-C, vol. 20, no. 1, Jun. 2022, doi: 10.31645/JISRC.22.20.1.3.
[14] Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore (Tamil Nadu), India. and Parvathy. K, "Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT): A Review," IJRTE, vol. 10, no. 1, pp. 199–203, May 2021, doi: 10.35940/ijrte.A5873.0510121.
[15] U. Ghugar and J. Pradhan, "Survey of wormhole attack in wireless sensor networks," Comput. Sci. Inf. Technol., vol. 2, no. 1, pp. 33–42, Mar. 2021, doi: 10.11591/csit.v2i1.p33-42.
[16] A. S. Rajasekaran, L. Sowmiya, A. Maria, and R. Kannadasan, "A survey on exploring the challenges and applications of wireless body area networks (WBANs)," Cyber Security and Applications, vol. 2, p. 100047, 2024, doi: 10.1016/j.csa.2024.100047.
[17] M. A. Goumidi, E. Zigh, and A. B. Ali-Pacha, "Analytic Hierarchy Process for the Evaluation Of Attacks' Severity Level within WBANs".
[18] A. Mansore and S. Koushik, "Detection and Prevention of Wormholl Attack Using AODV Protocol," IJARCCE, vol. 4, no. 12, p. 330-331, Dec. 2015, doi:DOI 10.17148/IJARCCE.2015.41276.
[19] Z. Zardari, K. Memon, R. Shah, S. Dehraj, and I. Ahmed, "A lightweight technique for detection and prevention of wormhole attack in MANET," ICST Transactions on Scalable Information Systems, p. 165515, Jul. 2018, doi: 10.4108/eai.13-7-2018.165515.
[20] A. M. J, Hassan A., S. San, and A. Y., "A combined technique of an affine cipher and transposition cipher," Quest Journals, vol. 7, no. 10, 2021.
[21] O. Laia, E. M. Zamzami, Sutarman, F. G. N. Larosa, and A. Gea, "Application of Linear Congruent Generator in Affine Cipher Algorithm to Produce Dynamic Encryption," J. Phys.: Conf. Ser., vol. 1361, no. 1, p. 012001, Nov. 2019, doi: 10.1088/1742-6596/1361/1/012001.
[22] R. P. Ritonga, M. Zarlis, and E. B. Nababan, "Modification Affine Cipher Transform Digraph to Squared the value of 'n' in Text Security," in 2020 4rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), Medan, Indonesia: IEEE, Sep. 2020, pp. 124–128. doi: 10.1109/ELTICOM50775.2020.9230503.
[23] H. Mawengkang, I. L. Sitepu, and S. Efendi, "Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm," IOP Conf. Ser.: Mater. Sci. Eng., vol. 420, p. 012129, Oct. 2018, doi: 10.1088/1757-899X/420/1/012129.
[24] A. Ridho, A. M. Dewi, R. Siregar, M. Zarlis, and D. Hartama, "Analysis of Possibility of the Combination of Affine Cipher Algorithm with One Time Pad Cipher Using the Three-Pass Protocol Method in Text Security," J. Phys.: Conf. Ser., vol. 1255, no. 1, p. 012028, Aug. 2019, doi: 10.1088/1742-6596/1255/1/012028.
[25] A. Hassan , "A MODIFIED CEASER CIPHER," JMSCM, vol. 5, no. 3, 2024, doi: 10.15864/jmscm.5304.
[26] V. Rohit, D. S. Rohit, U. N. Varma, R. Venkatesh, and K. S. Vivek, "An Overview of AODV Routing Protocol," vol. 08, no. 04, 2021.

BIOGRAPHY OF AUTHORS

Mohammed Abdessamad Goumidi (http://orcid.org/0009-0002-2854-6665 is a PhD student attached to the Coding and Security of Information Laboratory (LACOSI), Electronic Department, Electrical Engineering Faculty, Sciences and Technology University of ORAN Mohamed Boudiaf (USTO-MB), Oran, Algeria. His research interests include wireless networks, cryptography, and cybersecurity. For more details, he can reached at mohammedabdessamad.goumidi@univ-usto.dz.

Ehlem Zigh (http://orcid.org/0000-0002-4161-8582) is a full professor attached to the Coding and Security of Information Laboratory (LACOSI), Electronic Department, Electrical Engineering Faculty, Sciences and Technology University of ORAN Mohamed Boudiaf (USTO-MB), Oran, Algeria. Her research interests include the Internet of Things. For further inquiries, she can reached at ehlem.zigh@univ-usto.dz.

Adda Belkacem Ali-Pacha (http://orcid.org/0000-0003-1828-9562) is a full Professor attached to the Coding and Security of Information Laboratory (LACOSI), Electronic Department, Electrical Engineering Faculty, Sciences and Technology University of ORAN Mohamed Boudiaf (USTO-MB), Oran, Algeria. His research focuses on cryptography. He can contacted at email: adda.alipacha@univ-usto.dz.