

Mitigating blackhole attacks in wireless body area network

Goumidi Mohammed Abdessamad, Zigh Ehlem, Ali-Pacha Adda Belkacem

Coding and Security of Information Laboratory (LACOSI), Department of Electronic, Faculty of Electrical Engineering, Sciences and Technology University of ORAN-Mohamed Boudiaf (USTO-MB), Oran, Algeria

Article Info

Article history:

Received Apr 11, 2024

Revised Aug 13, 2024

Accepted Aug 26, 2024

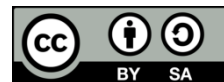
Keywords:

Blackhole attacks
Modified Affine-RSA cipher
Residual energy-based technique
Trust value-based strategy
Trusted secure routing protocol
Wireless body area network

ABSTRACT

In this paper, we aimed to develop a trusted secured routing Ad-hoc on-demand distance vector (AODV) protocol to fight against blackhole attacks within the wireless body area network (WBAN). The trusted secure routing protocol incorporates a routing strategy based on trust value to detect malicious nodes based on their trust value, a routing technique based on node residual energy to select the node with the highest residual energy during the communication process, and a hybrid cryptography algorithm that merges the Affine cipher with the modified RSA cipher algorithm to secure communication against malevolent biomedical sensor attacks. Simulation outcomes demonstrate that the suggested protocol outperforms the traditional AODV routing protocol in all evaluation metrics, including data rate, energy consumption, and packet delivery ratio. Its main strength is that it considers several factors, like illegitimate medical sensor detection, efficient network energy use, and secure data transmission, unlike similar secured routing protocols. Furthermore, the hybrid cipher algorithm improves the effectiveness and increases the security level of sensitive data compared to traditional cipher algorithms such as the Affine cipher and the RSA cipher.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Goumidi Mohammed Abdessamad

Coding and Security of Information Laboratory (LACOSI), Department of Electronic, Faculty of Electrical Engineering, Sciences and Technology University of ORAN-Mohamed Boudiaf (USTO-MB)

Oran, Algeria

Email: mohammedabdessamad.goumidi@univ-usto.dz

1. INTRODUCTION

A wireless body area network (WBAN) is a sub kind of mobile Ad hoc network designed to collect vital medical data using several sensors placed on, in, or around the human body [1], [2]. The medical data gathered is then wirelessly transmitted to a sink sensor, relaying to a medical server via an access point [3], [4]. The decentralized infrastructure of the network [5], [6] exposes it to various DoS attacks [7], including black hole attacks [8], [9]. This paper aims to address this issue. A black hole attack disrupts the communication between legitimate medical sensors and the sink [10], [11]. It occurs when an attacker seizes all network data without forwarding it to the destination. The malevolent biosensor falsely advertises itself as having the shortest path, luring other sensors in the network and then discarding all control and data packets routed through it. Consequently, all packets passing through the malicious node will suffer complete data loss, potentially endangering patients' lives [12].

Previous studies have used secure routing protocols to mitigate blackhole attacks in the network. For example, Sri and Rao [13] have proposed a secure Ad hoc on-demand distance vector (SAODV) protocol as a potential solution to minimize the negative effect of gray hole and blackhole attacks on network performance. The effectiveness of this protocol has been evaluated based on various metrics like overhead,

delay, throughput, and packet delivery ratio and compared with the basic ad-hoc on-demand distance vector (AODV) protocol version. Based on simulation outcomes analysis, the contributors found that the suggested protocol is more efficient than the AODV protocol. It improves network performance and increases network security. Anil and Kumar [14] created a secure AODV routing protocol, analyzed its performance, and compared it to the AODV protocol under black hole attacks. They measured the latency, throughput, and packet delivery ratio. Based on the simulation outcomes, contributors found that the secure AODV protocol has a higher Packet Delivery Ratio than the AODV protocol. Moreover, the data bit rate of the Secure AODV protocol is better than the AODV protocol. However, including end-to-end delay, the impact on Secure AODV by the illegitimate sensor is similar to that on AODV.

The existing secure protocols improve network security and performance. However, they consume significant amounts of time and energy and use a single line of defense based on their security mechanism, which weakens their security level. Furthermore, their security mechanisms are vulnerable to force-brute attacks. These are their primary limitations.

Our research concentrated on suggesting a trusted secure routing protocol to combat blackhole attacks in the WBAN. The proposed trusted secure routing protocol incorporates the routing strategy based on the trusted value used to find the alternative trusted path to avoid attacks, the routing technique based on sensor residual energy to select the sensor with the high residual energy during the communication process, and the hybrid cryptography algorithm combining the Affine cipher with the modified RSA cipher algorithms to secure the communication between sensors. Its main strength is that it considers several factors like illegitimate sensor detection, efficient network energy use, and secure data transmission.

The suggested trusted secure routing protocol combats the previous routing protocol drawbacks by using two defense lines (the routing strategy as the first defense line with the hybrid cryptography algorithm as the second defense line) to fight against force-brute attacks. It increases the network security level by employing the hybrid cryptography algorithm. Furthermore, based on experimental analysis, our routing protocol improves the network performances concerning packet delivery ratio, data rate, energy consumption, and delay compared to previous methods and traditional AODV protocol.

2. METHOD

To achieve our objective in this paper, we have to accomplish two main tasks as follows:

- a) Simulate a WBAN using the AODV routing protocol under a blackhole attack.
- b) Suggest a trusted secure AODV routing protocol based on a cryptographic algorithm and compare the trusted secure routing protocol based on cryptographic algorithm (TSAODVRPBOC) protocol performance with the traditional AODV protocol.

The first task involves designing and simulating an EEG network similar to a real EEG network using network simulator 2.35. The network comprises several biomedical EEG sensors set in the human head distributed according to a star topology with the sink. We assume that the communication between the wearable biomedical sensors and the sink is not secured and can be targeted by blackhole attacks, which take advantage of the AODV routing protocol weakness and compromise the devices within the network.

The second task is to suggest a new trusted secure routing protocol to combat black hole attacks in the WBAN. The TSAODVRPBOC is a refined and improved AODV protocol' version. It is designed to secure communication transmission within WBANs and allows unicast and multicast packet transmission even when sensors move dynamically. Its main strength is its consideration of multiple factors like malicious sensor detection, efficient network energy use, and secure data transmission. It operates in three phases for reliable packet transmissions. The three phases of the TSAODVRPBOC protocol are as follows:

- Route request phase.
- Route reply phase.
- Data transmission phase.

In the route request phase, the source sensor initiates the initial route revelation process by broadcasting a spurious route request packet containing a fake destination sequence number and destination address. When a malicious sensor responds with a false route reply packet claiming that it has an optimal route to the destination, the source sensor can identify the malicious sensor by recognizing the invalid RREPs received. Subsequently, the source sensor disseminates this information to all other sensors, effectively preventing the malicious sensor from participating in forwarding packets and disconnecting it from the network. This process allows the detection and elimination of illegitimate sensors caused by blackhole attacks in the communication network in an earlier stage. Also, during the route request phase, any malicious sensors resulting from low battery power are identified and removed by calculating the trust value of the sensors.

The trust value of a sensor S is determined using the following (1):

$$TV(S) = T_p(S_i, S_j) + D_p(S_i, S_j) + U_f(S_i, S_j) = ((T_p + R_p) + (D_p) + 3) / (T_p + R_p + D_p + 3) \tag{1}$$

Where:

$T_p(S_i, S_j)$: Represents the successful transmission and reception packets from sensor S_i to sensor S_j .

$D_p(S_i, S_j)$: Indicates the dropped packets from sensor S_i to sensor S_j .

$U_f(S_i, S_j)$: Represents an uncertainty factor initially set to 1. A value of 1 for the uncertainty factor indicates that the sensor is uncertain about the trustworthiness of the sensor S_j .

The trust value is updated depending on subsequent successful or failed packet transmissions from sensor S_i to sensor S_j , U_f will be updated.

$TV(S)$: Represents an average of three parameters that vary from 0 to 1.

For a sensor to be trusted, its trust value should be greater than or equal to 0.5. Every sensor in the network periodically shares the trust values of its neighboring sensors with all other sensors. Only trusted sensors are involved in information exchange, while all sensors with a trust value less than 0.5 will be deemed malevolent and removed from the network. The trust value of a sensor is updated based on the number of packets forwarded or discarded by it on behalf of other sensors.

Upon identifying and isolating the malicious sensors caused by blackhole attacks, the source sensor sends out a new route request (RREQ) packet with the accurate destination sequence number to all its trusted neighbors via a trusted route for the second time, thus initiating the route request phase. When an intermediate sensor receives a route request packet from a neighbors, it follows these steps:

- a) It verifies whether it has reached the intended destination by comparing its address with the destination address. If it has reached the destination, it replies to the source using the reverse route. If not, it proceeds to the subsequent steps.
- b) It verifies if the time to live (TTL) is zero. If it is, it tosses the received packet. Otherwise, it decrements the TTL field and increments the hop_count field.
- c) It maintains the transmitter address in its routing table and adds it to the route request packet.
- d) It sends a destination request to the next sensor in the routing table and waits for a destination reply.
- e) It verifies if the Trust value of the next neighbors sensor in the routing table is less than 0.5. If it is, it marks the neighbors sensor as malicious, sends an alert message to all other sensors to exclude the malicious sensor from forwarding packets, disconnects the malicious sensor from the network, and looks for another trusted neighbors to transmit the request. If the Trust value is not less than 0.5, it proceeds to the last step of the route request phase.
- f) It sends the route request packet to the neighbors.

The route request packet is sent until it reaches the destination in a secure way. When the destination receives a route request packet, it waits for a specific time before receiving other route request packets.

After the route request phase, the destination sensor prepares to exchange encrypted data packets with the source sensor using a hybrid cipher technique that merges the Affine cipher with the modified RSA cipher. So, during the route replay phase, the destination sensors perform the following steps:

- It computes the public key of the modified RSA algorithms in (2) by selecting six prime numbers, unlike in the traditional RSA, where the public key is calculated based on two prime numbers [15]-[18].

$$N = f . g . h . o . k . m \tag{2}$$

- It calculates the Euler's Phi $\phi(N)$ function based on the six prime numbers previously computed as in (3), unlike in the traditional RSA, where the Euler's Phi function is calculated based on two prime numbers [15]-[18]:

$$\phi(N) = (f - 1)(g - 1)(h - 1)(o - 1)(k - 1)(m - 1) \tag{3}$$

- It selects an integer e, which represents the public key, with $\text{gcd}(N, e) = 1$ and $1 < e < N$
- It calculates an integer d, which represents the secret key of the modified RSA algorithm using the following (4):

$$d = e^{-1} \text{mod } \phi(N) \tag{4}$$

- It computes each discovered path the cost as in (5):

$$Cost = RE / Hope\ Count \quad (5)$$

- It chooses the route with the highest cost value by selecting the path with the highest residual energy (RE) and the fewest intermediate sensors (shortest path).
- It sends the public keys (N, e) to the source sensor via a route reply packet.

The route reply packet is sent via the reverse path until it reaches the source biosensor.

Upon receiving the route reply packet, the source encrypts the data using the Affine cipher combined with modified RSA algorithms. The source sensor follows these steps:

- It selects two secret keys, i and j, with $i \neq 0$, $j \neq 0$, $\gcd(i, A) = 1$, and A being the size of the alphabet [19]-[23].
- It encrypts the data packets using the Affine Cipher as in (6):

$$E = ix + j \text{ mod}(A) \quad (6)$$

- It encrypts the encrypted data packets with the Affine Cipher using the modified RSA cipher:

$$CT = (E)^e \text{ mod } N \quad (7)$$

- It sends encrypted data packets with the secret keys through the reverse route until they reach the destination biosensor.

Upon receiving the encrypted data, the destination biosensor performs the following steps:

- It decrypts the encrypted message with the modified RSA cipher:

$$D_{rsa} = (CT)^d \text{ mod } N \quad (8)$$

- It decrypts the decrypted message with the modified RSA cipher using the Affine cipher:

$$D_{af} = i^{-1}(D_{rsa} - j) \text{ mod}(A) \quad (9)$$

- It sends an acknowledgment packet to the source sensor via the reverse path until it reaches the source biosensor.

This protocol is highly reliable as it supports the acknowledgment transmission following successful packet delivery from the source to the destination. Once the destination sensor has received all packets from the source sensor, it sends a data received packet (DRP) to the source sensor. Upon receiving the DRP from the destination sensor, the source sensor validates the entire route as trusted. This ensures the successful transmission of data packets and reception of the DRP.

Sensors determine if the route is trusted or not by calculating the trust value as in (10) and consider it a trusted route when the trust route value ≥ 0.5 :

$$TR = \frac{\text{successful packet transmissions}}{\text{total packets transmitted}} \quad (10)$$

the TSAODVRPBOC routing protocol enhances network security by considering factors such as detecting illegitimate medical sensors, efficient network energy use, and secure data transmission. In contrast, the AODV routing protocol does not consider network security measures.

3. RESULTS AND DISCUSSION

We have developed a trusted secure routing protocol to protect data from blackhole attacks in the WBAN. To simulate the network, we utilized the network simulator tool NS 2.35 and applied various metrics listed in Table 1. The network simulation involves a variation of one hundred medical sensors and a range of twenty-five illegitimate sensors. In our assessment, we considered the performance of the TSAODVRPBOC and AODV protocols under conditions with illegitimate sensors, focusing on parameters such as data bit rate, transmission delay, energy consumption, and packet delivery ratio.

Table 2 displays the differences in data rate, packet delivery rate (PDR), delay, and energy consumption under blackhole attacks using the AODV and TSAODVRPBOC. According to the table, the values recorded under 100 sensors are approximately 98.12% for PDR, 0.78 Mbit/s for data rate, 7.13J for energy consumption, and 1.62 ms for the delay using the TSAODVBOC while the values recorded under 100

sensors are approximately 90,44% for PDR, 0.73 Mbit/s for data rate, 7.41J for energy consumption, and 1.52 ms for the delay using the AODV.

Following the TSAODVRPBOC routing protocol implementation, there is a slight increase and enhancement in PDR of 7.68% compared to the AODV routing protocol due to the efficient and speedy delivery of packets to the destination sensor using the TSAODVRPBOC, which detects and isolates blackhole nodes in the earlier stage of the network communication before package delivery, unlike in AODV protocol where blackhole nodes drop the packets. Another slight increase and enhancement in data rate of 0.05 Mbit/s compared to the AODV routing protocol because the data passed via trusted intermediate nodes selected based on its trust value and achieved its destination when using the TSAODVRPBOC, which detects and isolates malicious nodes that arise due to the low energy, unlike in AODV protocol where this malicious nodes loss the packets. However, there is a slight decrease and enhancement in Energy consumption of 0.3J compared to the AODV routing protocol because the route with the smallest number of intermediate biosensors and the highest residual energy (shortest path) for the communication process is selected when using the TSAODVRPBOC, which ensures efficient use of the limited resources, in particular the energy consumption, unlike in AODV protocol where the blackhole attacks which disrupt legitimate nodes' communication by transmitting inaccurate requests or insistence that the path via the attacker sensor was the right or quickest route. Furthermore, we noticed an increase in delay of 0.1J compared to the AODV routing protocol because the sensor consumes more time encrypting and decrypting data when using the TSAODVRPBOC, which incorporated the mixed cipher technique. We observed a high delay when using the AODV due to the drop-down of a data packet during the communication process.

Table 1. Simulation setup

Various metrics	Values
Software	NSv2.35
Routing protocols	AODV/TSAODVRPBOC
Medical sensors count	100 biosensors
Square simulation area	1200 m*1200 m
Illegitimate medical sensors count	25 biosensors
The initial energy of medical sensors	150 Joule
Count of transmitted packets by each medical sensor	250 packets

Table 2. Network performance using AODV and TSAODVRPBOC routing protocols under blackhole

Protocols	Packet delivery ratio (%)	Delay (ms)	Throughput (bit/s)	Energy consumption (J)
AODV	90.4406	1.519017	731484.241	7.43081
TSAODVRPBOC	98.1159	1.6171	775931.232	7.13354

Table 3 shows the performance comparison between the mixed cipher technique, which merges the Affine cipher incorporated in the TSAODVRPBOC with the modified RSA algorithms and other traditional methods like the Affine cipher and the RSA cipher algorithms. We anticipated that the suggested cipher technique described in section 2 would be more complex than the classical RSA cryptosystem and Affine cipher algorithm. It is less vulnerable to malicious node attacks, as eavesdroppers will have difficulty deciphering the ciphertext or using brute force to break the system because of the increased complexity of the ciphertext resulting from the suggested cipher method compared to the classical Affine cipher or RSA algorithm. Combining the RSA method and Affine cipher could potentially enhance the effectiveness and security of text messages.

Table 4 displays the performance comparison between AODV and TSAODVRPBOC routing protocols by evaluating several characteristics such as trusted Route, communication security, and energy-efficient routing. We found that the tested TSAODVRPBOC routing protocol outperforms other protocols like traditional AODV and SAODV routing protocols proposed in [13], [14]. It offers a trusted path to route packets by selecting nodes with a trust value of more than 0.5, unlike other routing protocols, which don't integrate this characteristic. The suggested protocol ensures low energy consumption in the packet routing process by selecting the path with the smallest number of intermediate biosensors and the highest residual energy (shortest path), unlike other routing protocols that don't integrate this characteristic. Furthermore, it guarantees a secure network by encrypting the data within the network, unlike in traditional AODV routing protocol, where the cipher technique used is more robust against force brute attacks by merging the Affine cipher with the modified RSA algorithms unlike in other secured protocols that use a simple cipher technique.

Table 3. The affine-modified RSA cipher performance analysis

Cryptography algorithms	Features	Specifications
Our Affine- modified RSA cipher algorithm	Prime numbers Architecture Complexity level Key strength Key update Alphabet size	7 prime numbers monoalphabetic substitution and Asymmetric High strength Yes 26
Traditional RSA cipher algorithm [16], [24] (2023,2018)	Prime numbers Architecture Complexity level Key strength Key update	2 prime numbers Asymmetric medium Medium strength No
Traditional Affine cipher algorithm	Prime numbers Architecture Complexity level Key strength Key update Alphabet size	1 prime numbers monoalphabetic substitution Low Less strength No 26
Affine-RSA protocol [19] (2019)	Prime numbers Architecture Complexity level Key strength Key update Alphabet size	3 prime numbers monoalphabetic substitution and Asymmetric Medium strength No 26

Figure 1 shows a screenshot of our network simulation under blackhole attacks with AODV protocol at the time (t). We noticed that the unauthorized biosensor with ID number 6 did not forward any packets from the sink with ID number 0 to the destination sensor with ID number 24. Instead, it discarded the packets sent to it because the blackhole attacks exploit weaknesses in the routing protocols' route discovery process by sending false routes to the receivers. When the attacker biosensor receives a route request packet (RREQ), it sends a fake route reply packet (RREP) with a higher sequence number to the sender biosensor, claiming to have the most recent and shortest route to the receiver. Once the sender biosensor selects this route (which includes malicious biosensors), the malicious biosensor disregards all packets instead of forwarding them to the intended receiver, causing link failures.

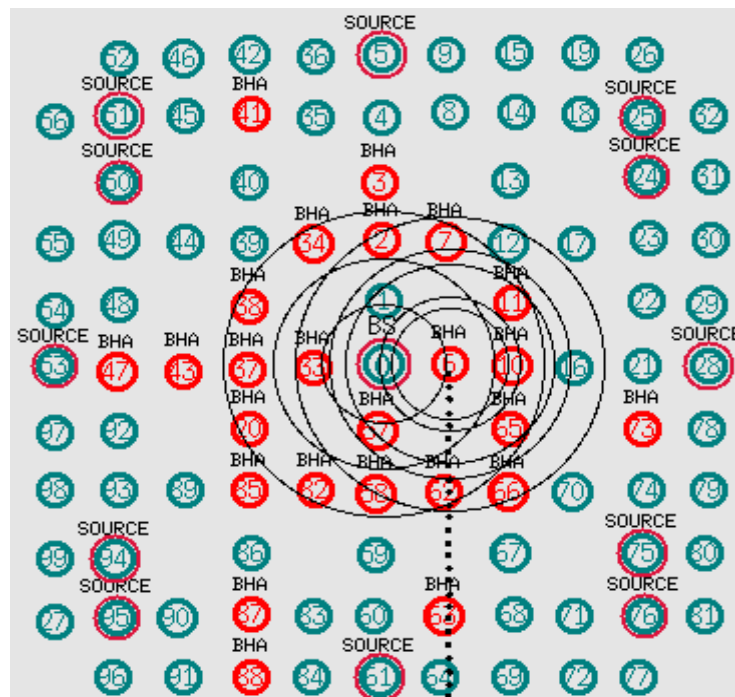


Figure 1. Network simulation under attacks using AODV routing protocol

Table 4. Comparative analysis between AODV and TSAODVRPBOC routing protocols

Characteristics	AODV [25] (2021)	SAODV [13] (2018)	SAODV [14] (2015)	TSAODVRPBOC (2024)
Trusted route	X	X	X	✓
Communication security	X	✓	✓	✓
Energy efficient routing	X	X	X	✓

Figure 2 shows a screenshot of our network simulation under blackhole attacks with TSAODVRPBOC protocol at the time (t). We observed the establishment of secure communication between the transmitter sensor with ID 0 and the receiver sensor with ID 24 via a trusted path. The successful communication establishment is because the source node detects blackhole attacks by sending fake route request packets with a false destination address and destination sequence number. When a malicious node responds with a false route reply packet claiming that it has an optimal route to the destination, the source biosensor can identify the illegitimate biosensor by recognizing the invalid RREPs received. In such cases, the legitimate sensors send alerts to inform their neighboring legitimate sensors. Each biosensor in the network is responsible for maintaining a trusted routing table containing the identification numbers of legitimate neighboring biosensors. This setup creates a complete network in which all the biosensors can securely communicate with each other. Additionally, malicious nodes that arise due to the lack of energy will be detected and isolated from the network during the communication if their trust value is less than 0.5. After detecting and isolating illegitimate sensors, the source and destination sensors exchange secure information encrypted with the Affine cipher with the modified RSA algorithm.

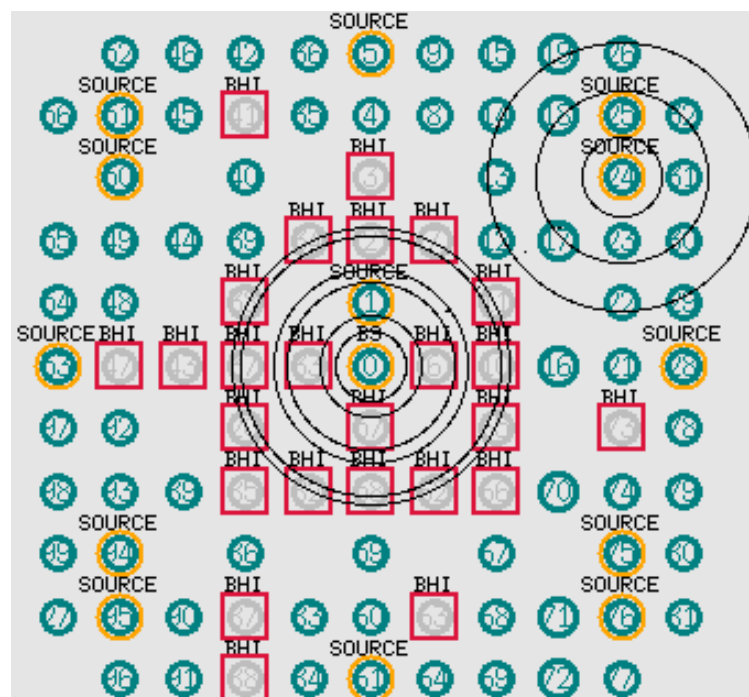


Figure 2. Network simulation under attacks using TSAODVRPBOC routing protocol

4. CONCLUSION




Despite the potential uses and advantages of wireless body area networks (WBAN), they are susceptible to attacks, particularly Blackhole attacks. In response, we have developed a trusted and secure AODV routing protocol to address these vulnerabilities within WBAN. Our proposed protocol considers multifactors such as node trust values, available battery power during the routing process, and secure data encryption during communication. It effectively detects and isolates blackhole attacks using fake route request packets and identifies malicious nodes resulting from low energy by evaluating node trust values. Furthermore, it accounts for the battery life of intermediate nodes along the selected route. Additionally, it ensures secure communication through data encryption using a combined cipher technique that integrates the Affine cipher with modified RSA cipher algorithms.

The experimental results demonstrate a 7.68% improvement in PDR, a 0.05 Mbit/s increase in data rate, and a 0.3J reduction in energy consumption when utilizing the TSAODVRPBOC compared to traditional AODV and SAODV routing protocols. Our routing protocol effectively ensures a reliable route, selects trusted sensors with the highest residual energy, and enhances network security by employing a hybrid cipher technique that combines the Affine cipher with modified RSA algorithms, unlike traditional AODV and SAODV routing protocols. Additional results show that the security mechanism in the suggested routing protocol is more robust and less susceptible to brute force attacks when using the hybrid cipher technique, unlike traditional single-cipher algorithms such as the Affine cipher and the RSA cipher algorithms. In the future, we aim to address other attacks targeting the WBAN.




REFERENCES

- [1] M. A. Panhwar, S. Jatoti, K. A. Memon, and S. Saddar, "Wireless body area networks: architecture, standards, challenges, and applications," *International Journal of Computer Science and Network Security*, vol. 19, no. 12, pp. 173–178, 2019.
- [2] S. J. Al-Sofi, S. M. S. Atroshey, and I. A. Ali, "Review of wireless body area networks: protocols, technologies, and applications," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 6, pp. 3677–3689, Dec. 2023, doi: 10.11591/eei.v12i6.5543.
- [3] M. A. Goumidi, E. Zigh, N. Hadj-Said, and A. B. Ali-Pacha, "A hybrid intrusion detection system to mitigate biomedical malicious nodes," *International Journal of Computer Network and Information Security*, vol. 16, pp. 117–133, 2024, doi: 10.5815/ijcnis.2024.02.10.
- [4] D. M. G. Preethichandra, L. Piyathilaka, U. Izhar, R. Samarasinghe, and L. C. De Silva, "Wireless body area networks and their applications—a review," *IEEE Access*, vol. 11, pp. 9202–9220, 2023, doi: 10.1109/access.2023.3239008.
- [5] M. Yaghoubi, K. Ahmed, and Y. Miao, "Wireless body area network (WBAN): a survey on architecture, technologies, energy consumption, and security challenges," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, p. 67, Oct. 2022, doi: 10.3390/jsan11040067.
- [6] M. Asam *et al.*, "Challenges in wireless body area network," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 11, 2019, doi: 10.14569/ijacsa.2019.0101147.
- [7] A. Rashid *et al.*, "Authentication healthcare scheme in WBAN," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 19, no. 2, pp. 118–127, Jul. 2023, doi: 10.37917/ijeee.19.2.14.
- [8] P. Rani, Kavita, S. Verma, and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, pp. 121755–121764, 2020, doi: 10.1109/access.2020.3004692.
- [9] B. U. I. Khan *et al.*, "Exploring manet security aspects: analysis of attacks and node misbehaviour issues," *Malaysian Journal of Computer Science*, vol. 35, no. 4, pp. 307–338, Oct. 2022, doi: 10.22452/mjcs.vol35no4.2.
- [10] A. Kanwal, P. Kumar, P. Kumar, and R. Asif, "Analysis and countermeasures of wormhole and sinkhole attacks in WBAN," *Journal of Independent Studies and Research Computing*, vol. 20, no. 1, Jun. 2022, doi: 10.31645/jisrc.22.20.1.3.
- [11] 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," in *2022 International Conference of Advanced Technology in Electronic and Electrical Engineering (ICATEEE)*, Nov. 2022, vol. 41, pp. 1–6, doi: 10.1109/icateee57445.2022.10093101.
- [12] R. Sivaranjani, D. R. Shankar, and D. S. Duraisamy, "Manet swamping and blackhole attack moderation using machine learning and a protection-based AODV protocol," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 12, no. 4, 2024.
- [13] M. S. Sri and K. S. Rao, "Prime product number and armstrong number based malicious node detection scheme in SAODV," *International Journal of Emerging Technologies and Innovative Research*, vol. 5, no. 11, pp. 570–578, 2018.
- [14] D. Anil and S. Kumar, "Implementation and comparison of enhance SAODV protocol against blackhole attacks in MANET using network simulator," *International Journal of Science and Research (IJSR)*, vol. 5, no. 11, 2015.
- [15] C. Gupta and N. V. Subba Reddy, "Enhancement of security of diffie-hellman key exchange protocol using RSA cryptography.," *Journal of Physics: Conference Series*, vol. 2161, no. 1, p. 12014, Jan. 2022, doi: 10.1088/1742-6596/2161/1/012014.
- [16] N. M. Chatheka and S. Glorindal, "Secure and efficient data transfer in AODV routing protocol using RSA encryption," *i-manager's Journal on Digital Forensics & Cyber Security*, vol. 1, no. 1, p. 1, 2023, doi: 10.26634/jdf.1.1.19389.
- [17] S. Shin, K. Won, and S. Shin, "Size efficient preprocessed symmetric rsa for wireless body area network," *ACM SIGAPP Applied Computing Review*, vol. 20, no. 1, pp. 15–23, Apr. 2020, doi: 10.1145/3392350.3392352.
- [18] U. Gulen, A. Alkhodary, and S. Baktir, "Implementing RSA for wireless sensor nodes," *Sensors*, vol. 19, no. 13, p. 2864, Jun. 2019, doi: 10.3390/s19132864.
- [19] M. Jannah, B. Surarso, and Sutimin, "A combination of rivest shamir adleman (RSA) and affine cipher method on improvement of the effectiveness and security of text message," *Journal of Physics: Conference Series*, vol. 1217, no. 1, p. 12073, May 2019, doi: 10.1088/1742-6596/1217/1/012073.
- [20] R. G. SINAMBELA and A. Fauzi, "Development of hybrid encryption method using affine cipher, vigenere cipher, and elgamal algorithm to secure text messages in data communication system," *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, vol. 2, no. 2, pp. 30–40, Feb. 2023, doi: 10.59934/jaiea.v2i2.154.
- [21] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wireless Networks*, vol. 27, no. 3, pp. 2119–2130, Feb. 2021, doi: 10.1007/s11276-021-02560-y.
- [22] 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," *Journal of Physics: Conference Series*, vol. 1255, no. 1, p. 12028, Aug. 2019, doi: 10.1088/1742-6596/1255/1/012028.
- [23] 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.
- [24] A. Sabo and A. Lawan, "An enhance approach for detecting and preventing single and collaborative attacks in mobile ad-hoc networks," *Fudma Journal of Sciences*, vol. 2, no. 1, 2021.
- [25] P. K. Maurya, G. Sharma, V. Sahu, A. Roberts, M. Srivastava, and M. T. Scholar, "An overview of AODV routing protocol," *International Journal of Modern Engineering Research (IJMER)*, vol. 2, no. 3, pp. 728–732, 2012.




BIOGRAPHIES OF AUTHORS

Goumidi Mohammad Abdessamad    is pursuing a Ph.D. in Cryptography and Data Security at the Sciences and Technology University of Oran, Mohamed Boudiaf (USTO-MB), Algeria. He is associated with the Coding and Information Security Laboratory (LACOSI) within the Department of Electronic and the Electrical Engineering Faculty. His research interests encompass artificial intelligence, cybersecurity, wireless networks, and cryptography. For further information. He can contact at: mohammedabdessamad.goumidi@univ-usto.dz.



Zigh Ehlem    is a full professor at the Sciences and Technology University of Oran, Mohamed Boudiaf (USTO-MB), Algeria. She is attached to the Coding and Information Security Laboratory (LACOSI) within the Department of Electronic and the Electrical Engineering Faculty. Her research interests encompass artificial intelligence, soft computing techniques, e-learning, image processing, and the internet of things. For further inquiries, she can contact at email: ehlem.zigh@univ-usto.dz.



Ali-Pacha Adda Belkacem    is a full Professor at the Sciences and Technology University of Oran, Mohamed Boudiaf (USTO-MB), Algeria. He is attached to the Coding and Security of Information Laboratory (LACOSI) in the Department of Electronic and Electrical Engineering Faculty. His research focuses on cryptography and digital communications. He can contact at email: adda.alipacha@univ-usto.dz.