I. J. Computer Network and Information Security, **2024, 2, 117-133**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.02.10

A Hybrid Intrusion Detection System to Mitigate Biomedical Malicious Nodes

Mohammed Abdessamad Goumidi*
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
E-mail: mohammedabdessamad.goumidi@univ-usto.dz
ORCID iD: https://orcid.org/0009-0002-2854-6665
*Corresponding Author

Ehlem Zigh
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
E-mail: ehlem.zigh@univ-usto.dz
ORCID iD: https://orcid.org/0000-0002-4161-8582

Naima Hadj-Said
Laboratory of Coding and Security of Information (LACOSI), Department of Computer Science, Faculty of Mathematics and Computer Science, University of Sciences and Technology of ORAN- Mohamed Boudiaf (USTO-MB), Algeria
E-mail: naima.hadjsaid@univ-usto.dz
ORCID iD: https://orcid.org/0000-0003-2561-0481

Adda Belkacem Ali-Pacha
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
E-mail: adda.alipacha@univ-usto.dz
ORCID iD: https://orcid.org/0000-0003-1828-9562

Received: 21 September 2023; Revised: 12 November 2023; Accepted: 21 December 2023; Published: 08 April 2024

Abstract: This paper proposes an intrusion detection system to prevent malicious node attacks that may result in failure links in wireless body area networks. The system utilizes a combination of Optimized Convolutional Neural Networks and Support Vector Machine techniques to classify nodes as malicious or not, and links as failure or not. In case of detection, the system employs a trust-based routing strategy to isolate malicious nodes or failure links and ensure a secure path. Furthermore, sensitive data is encrypted using a modified RSA encryption algorithm. The experimental results demonstrate the improved network performance in terms of data rate, delay, packet delivery ratio, energy consumption, and network security, by providing effective protection against malicious node attacks and failure links. The proposed system achieves the highest classification rate and sensitivity, surpassing similar methods in all evaluation metrics.

Index Terms: Wireless Body Area Network, Malicious Nodes, Failure Links, Security, Trust Value, Modified RSA Cipher, Optimized Convolutional Neural Network-support Vector Machine.

1. Introduction and Related Work

In recent years, the wireless body area network has become one of the fastest-growing areas due to its use in a wide range of applications such as sports, social networking, gaming, military, and telemedicine. The network comprises portable biosensors that attach to different parts of the body to collect vital signs. This data is wirelessly transmitted to a clinical help service where physicians analyze it periodically to prescribe suitable treatment.

The global wireless body area network has a three-tier architecture. The first tier involves sensitive data collected by a set of biosensors, which is stored in the sink biosensor. In the second tier, the biomedical data is wirelessly forwarded to the remote base station by the sink biosensor. Finally, in the third tier, the biomedical data is securely stored on a hospital server, and only authorized personnel can access it. The architecture of the global wireless body area network is illustrated in Fig. 1.

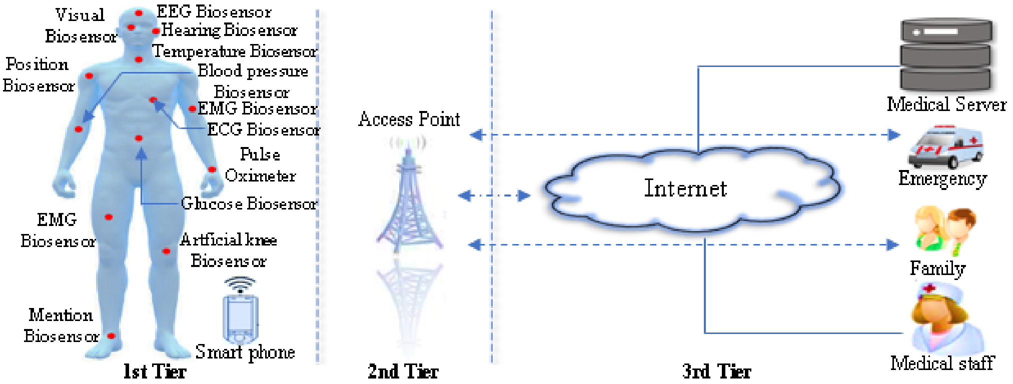


Fig.1. A global architecture of WBAN

The distributed architecture of the network can be vulnerable to different types of attacks that can disrupt communication tiers. This study specifically examines Blackhole attacks that target the first communication tier through biosensors. These attacks take advantage of weaknesses in routing protocols' route discovery process by sending false routes to the receivers. When receiving a route request packet (RREQ), the attacker biosensor sends a fake route replay packet (RREP) with a higher sequence number to the sender biosensor, indicating that it has the most recent and shortest route to the receiver. Once the sender biosensor selects this route (which includes a malicious biosensor), the malicious biosensors disregard all packets instead of forwarding them to the intended receiver [1], as seen in Fig. 2.

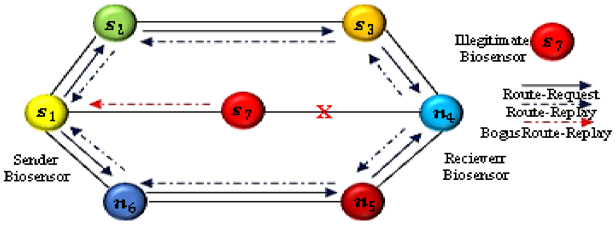


Fig.2. Blackhole attack

Intrusion Detection Systems (IDS) are a common security measure for detecting and isolating network intrusions. Typically, an IDS is composed of six blocks, each with a specific functionality. The monitoring block observes neighboring biomedical sensor nodes, while the analysis block stores records of normal and suspicious biosensor activity. The detection block uses a modeling algorithm to analyze network behavior and determine the legitimacy of actions.

The remaining three blocks of an IDS offer different procedures, including logging, alarming, and prevention. The logging block records every packet in a log file for later analysis by the security administrator. The alarm block generates an immediate response in the event of intrusion detection, potentially alerting authorities to suspicious biosensor activity. The prevention block is an advanced feature that can remove unauthorized biosensors from the network once they are detected [2].

The Fig. 3 describes the Intrusion Detection System:

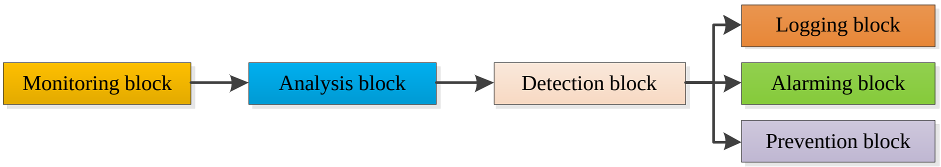


Fig.3. An intrusion detection system component

Previous studies have delved into utilizing Artificial Intelligence methods based on machine and deep learning techniques in creating intrusion detection systems for classifying illegitimate medical biosensors and damaged links within wireless networks, routing algorithms to avoid them, or cryptographic algorithms to secure the communication between medical sensors. Nevertheless, these systems often offer only a singular solution and carry out only one task to fight against illegitimate sensors and damaged wireless links. Furthermore, the convolutional techniques utilized by intrusion detection systems frequently consume a considerable amount of time and yield suboptimal accuracy, which are the primary limitations.

Our research is centered on preventing malicious node attacks in wireless body area networks that can lead to link failures. To accomplish this, we've developed a hybrid intrusion detection system that combines Optimized Convolutional Neural Networks with a non-linear SVM classifier. The CNN extracts node and link characteristics from a vast database created using data collected from sensors, as well as link traffic patterns simulated by Network Simulator software. The SVM algorithm functions as a binary classifier by classifying nodes as malevolent or trusted and links as damaged or normal wireless links. If an attack is detected, a trust-based routing strategy is employed to isolate malicious nodes or failure links and ensure a trusted path. Moreover, sensitive data is encrypted using a modified RSA encryption algorithm to secure communications between nodes.

Our proposed system provides three solutions to combat malicious nodes and failure links while addressing the shortcomings of previous conventional algorithms. Experimental results demonstrate that our system delivers effective protection against malicious node attacks and failure links by achieving the highest classification rate and sensitivity. Additionally, the network performance, concerning data rate, delay, packet delivery ratio, energy consumption, and network security, is improved compared to previous methods.

2. Review of Previous Studies

Rajesh Kumar D et al. [3], employed a Simulated Annealing Black-hole attack Detection-based Enhanced Gravitational Search Algorithm to identify and isolate illegitimate biosensors in WBANs. The performances of the suggested algorithm are evaluated in terms of the detection probability rate of illegitimate biosensors attack, consumed energy, illegitimate biosensors attack detection time, and Packet delivery ratio. Experimental results demonstrate that the EGSA-SABD reduces energy consumption by 21% and outperforms the detection probability rate of illegitimate biosensor attacks by 13%. Dinesh Kumar Anguraj et al. [4] have proposed a confidence-based intrusion detection model designed to identify unauthorized biosensors within WBANs (Wireless Body Area Networks). They have introduced a set of trust parameters, including energy, data, and communication trusts. When detecting illegitimate biosensors, the remaining biosensors within the network are gathered to form clusters. Each cluster is led by a cluster head (CH), selected through the multi-objective firefly algorithm. The primary goal of this system is to reduce transmission delays, increase broadcast energy, and enhance the data bit rate. Multiple biosensors are responsible for collecting physiological data, which are then transmitted to the CH. The CH subsequently forwards the gathered biomedical data to a sink and relays it to the system via a base station. To secure the data, a hybrid encryption algorithm is utilized, ciphering the information before it is transmitted to the medical server. The decryption process occurs on the server side to extract the original data. This proposed technique is implemented using an NS-2 simulator. Simulation results demonstrate that the suggested system outperforms the actual system in terms of data bit rate, transmission delay, packet delivery ratio, recall, and precision. Ali Raza Bhangwar et al. [5], suggested a trust and thermal-aware routing protocol for WBANs that takes trust and temperature of biosensors into account for isolating malicious biosensors. This innovative routing approach aims to identify and isolate malicious biosensors by factoring in trustworthiness and thermal conditions. By employing this multifaceted routing technique, the network can establish a secure and well-balanced environment, minimizing the inclusion of untrustworthy sensors within trusted paths. Simulation results indicate that this protocol exhibits superior performance in terms of temperature management, data transmission rates, packet latency, and packet drop rates, even when subjected to varying traffic conditions. Sangeetha Ramaswamy et al. [6], suggested a confidence system for secure communication in WBAN based on biosensor confidence and data confidence. Sensor confidence is computed utilizing direct confidence calculation and sensor comportments. Data confidence is computed utilizing data aging and consistent data success. The performance is evaluated using an existing protocol such as Body Area Network (BAN)-Trust and Trust Evaluation (TE)-WBAN which isn’t a cryptographic strategy. The protocol is lightweight and has low overhead. The performance is rated best in terms of minimum delay, packet delivery ratio, and data bit rate. Through extensive simulation selfishness attacks, data suppression attacks, on-off attacks, and sleeper attacks were precluded. Damanpreet Kaur et al. [7] have introduced a security technique for safeguarding patient data within WBANs, utilizing Elliptic Curve Cryptography (ECC). In this method, a Trusted Third Party (TTP) leverages the K-anonymity parameter along with K-1 dummy query users to ensure both data confidentiality and user location privacy. The results of their study highlight ECC as an encryption approach with a compact key size, delivering rapid encryption, and providing higher security compared to RSA. ECC effectively maintains user location privacy in real-time and demonstrates greater scalability, making it a more suitable choice for wearable devices equipped with enhanced storage and computing capabilities than RSA. Their experimental findings encompassing encryption and decryption times, message sizes, and their variation with respect to the K-anonymity metric value underscore the performance advantages of this proposed scenario. Sangwon Shin et al. [8] have introduced a WBAN system designed for space applications, incorporating message authentication through pre-processed symmetric RSA encryption. This system enables biosensors to achieve reliable data authentication through RSA while minimizing the impact on processing time. By allowing user-controlled pre-processing, it generates a wider array of potential combinations of RSA-encrypted authentication data. pre-processed symmetric RSA may be predicted to result in the minimization of a key size, up to 256 bits, while producing more total combinations compared to 1024-bit RSA with the non-effect on speed. A. Basnet et al. [9] have proposed a system that incorporates a hybrid approach combining the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) within WBANs. This system offers a straightforward, swift, and highly robust cryptographic solution for data security. In this scheme, ECC is employed to secure AES encryption keys, while the AES algorithm is used for the encryption and decryption of text. The choice of encryption method is determined based on the energy availability, particularly in a scenario where biosensors continuously harness solar power as their energy source. The results of this study demonstrate that the suggested EEHEE algorithm significantly enhances data file encryption. Furthermore, the EEHEE system encrypts data files rapidly while reducing energy consumption. The primary focus of this system is to minimize energy consumption within WBANs while simultaneously increasing cryptographic strength through the use of a hybrid symmetric and asymmetric encryption algorithm. As a result, this research offers an efficient scheme for enhancing security in real-time data transmission within telemedicine applications. Gurbeer Kaur et al. [10] have introduced an Enhanced Cost-effective, Energy-efficient, and Secure Routing (CESR) protocol for WBANs. This protocol is an enhancement of the reliable Adhoc On-demand Distance Vector (AODV) protocol found in the literature. One of the key improvements is the incorporation of RSA encryption for data encryption, enhancing overall security. To enhance energy efficiency, a cost function is developed to select the sender sensor with the lowest cost value, thus optimizing energy consumption. The performance of the CESR protocol is rigorously assessed using MATLAB, and the results demonstrate a notable increase in both reliability and security as a result of these enhancement techniques. Mohammed Ramadan et al. [11] have proposed an effective and secure identity-based encryption scheme based on the RSA assumption, which includes an equality test feature. They conducted a comprehensive security analysis of their scheme, demonstrating its resilience against chosen-identity and chosen-ciphertext attacks within the framework of the random oracle model. The experimental results demonstrate the scheme's effectiveness, due to its ability to provide a relatively low computational burden and seamless compatibility with WBAN applications. K. Kalaiselvi et al. [12] have designed a system to identify unauthorized biomedical nodes within a WBAN environment and to detect link failures caused by suspicious biomedical nodes. The approach involves two distinct subsystems: Suspicious Sensor Classification Sub-System: This system employs a coactive adaptive neuro-fuzzy inference algorithm based on machine learning techniques to classify suspicious sensors. The proposed illegitimate biomedical sensor classification system in WBAN achieved a packet delivery ratio (PDR) of 99.80% for a single unauthorized biomedical sensor and a PDR of 95.60% for 10 unauthorized biomedical sensors. It accomplished this with a detection latency of 0.50. 10^{-3} seconds for a single suspicious biosensor and 1.89. 10^{-3} seconds for the detection of unauthorized biomedical sensor nodes. Link Failure Classification Sub-System: For detecting link failures in the WBAN, a convolutional neural network algorithm based on deep learning techniques is employed. This system consumed 1.60. 10^{-3} seconds to detect a single link failure and achieved a PDR of 91.70%. When detecting 10 link failures in the WBAN, it consumed 2.20. 10^{-3} seconds.

3. Proposed Methods

Our objective in this study is to simulate an EEG network similar to a real EEG network. We aim to guarantee its dependability by applying an IDS that classifies the nodes as malicious or not and links as failure or not, then detects and isolates unauthorized biosensors as well as failure links caused by unauthorized biosensors in the network by establishing a trusted path. After, it encrypts the communication between biosensors. To achieve this purpose, we placed several biomedical EEG sensors in the human brain. Fig. 4 illustrates the distribution of biomedical EEG sensors in the human brain, according to a star topology where the sink is located in the center of the brain.

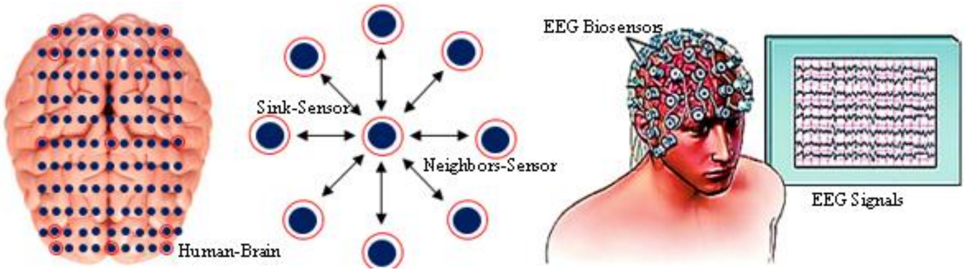


Fig.4. Distribution of EEG sensors

3.1. The Intrusion Detection System

We developed a hybrid intrusion detection system comprising three distinct blocks. The initial block effectively categorizes nodes and links within WBAN (Wireless Body Area Network) by utilizing a combination of an Optimized Convolutional Neural Network and a Support Vector Machine. It classifies nodes as malicious or not and links as damaged or not. The second block expertly detects and isolates malicious nodes and failure links in WBAN by employing a trust-based routing strategy, calculating the confidence value and hop counts to guarantee an optimal path while avoiding malicious nodes and failure links. The final block is responsible for ensuring the privacy of communication between nodes by providing data encryption through a modified RSA encryption algorithm.

Fig. 5 displays the flowchart of the suggested IDS example.

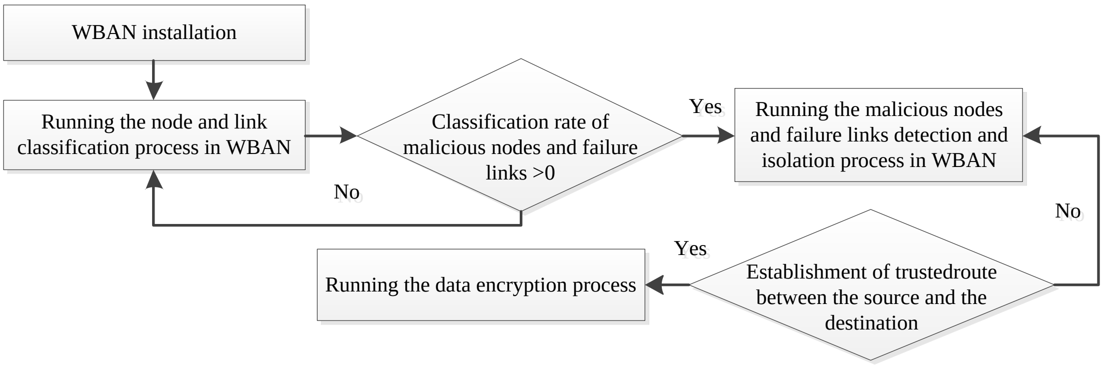

WBAN installation
Running the node and link classification process in WBAN
Classification rate of malicious nodes and failure links >0
Yes
No
Running the malicious nodes and failure links detection and isolation process in WBAN
No
Establishment of trustedroute between the source and the destination
Yes
Running the data encryption process

Fig.5. Flowchart of the suggested intrusion detection system

A. Nodes and Links Classification Process

The WBAN node and link classification process utilizes a hybrid approach that blends an optimized convolutional neural network with a support vector machine. By combining the best features of SVM and Optimized CNN classifiers, this hybrid model can accurately classify nodes and links. The optimized convolutional neural network automatically extracts features, while the support vector machine functions as a binary classifier. Fig. 6 illustrates the diagram of the detection system.

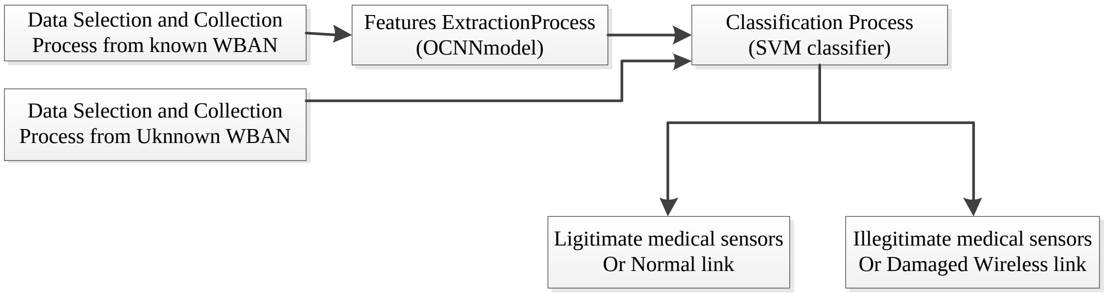

Data Selection and Collection Process from known WBAN
Features ExtractionProcess (OCNNmodel)
Classification Process (SVM classifier)
Data Selection and Collection Process from Uknnown WBAN
Ligitimate medical sensors Or Normal link
Illegitimate medical sensors Or Damaged Wireless link

Fig.6. Block of classification of nodes and links in WBAN

In the process of feature extraction, an optimized Convolutional Neural Network (CNN) model was utilized. The key benefit of using an optimized CNN is its ability to automatically detect important features without requiring human intervention. It functions similarly to humans and can learn local invariant features very well, extracting the most distinctive information from sensor nodes.

The optimized CNN architecture used in the proposed detection system is a modified version of the VGG16 model. It is composed of two blocks placed horizontally in parallel and five blocks placed vertically in series. The first two parallel blocks have four layers each, including one Convolutional Layer with 64 filters, a kernel size of 3 and padding equal to the same, one Max-Pooling layer with a pooling size of 3, stride of 2, and padding equal to the same, and two Batch-Normalization layers. The second two parallel blocks have the same architecture but with one Convolutional Layer with 128 filters. The third and fourth parallel blocks have one Convolutional Layer with 256 filters, and the last two parallel blocks have three Convolutional Layers with 512 filters and six Batch-Normalization layers.

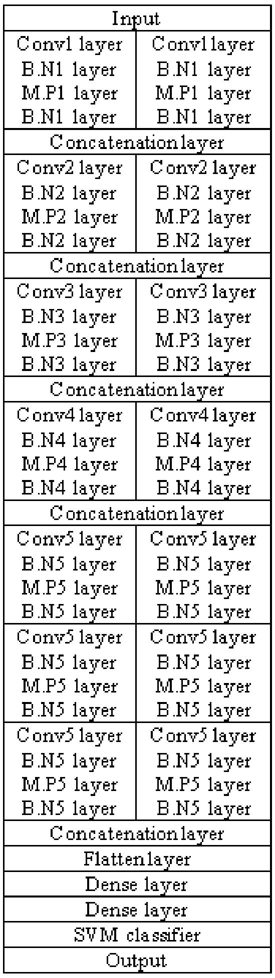
Every two blocks are concatenated with a concatenation layer. This suggested optimized CNN architecture uses a set of convolutional layers with a determined count of filters for map extraction, a set of Max-Pooling layers to minimize the dimensionality of the network by taking the highest value in a particular filter area, and a set of Batch-Normalization layers that are placed after each layer of the optimized CNN architecture to make the training of deep learning faster and more stable. After the last concatenation layer, three fully connected layers with 4096 neurons are placed and utilized to aggregate data from the final feature map and generate the final classification.

The first layer's input is a flattened version of the previous layer's output. Except for the final layer, all layers employ the rectified linear unit (ReLU) activation function. The input is processed by the first convolutional layers of the first two blocks with a set of filters that extracts superior-level characteristics of dimensionally minimized feature maps.

For the classification process, we employed the SVM classifier, which is a linear technique that can handle non-linear problems by projecting the data to a higher dimensional space. SVM works well for binary classification. In the optimized CNN-SVM algorithm, we replaced the last layer of the optimized CNN network, which uses the sigmoid activation function for final classification, with an SVM classifier. The CNN classifier's sigmoid layer is substituted with a nonlinear SVM for binary classification.

In simpler terms, we suggest using the hybrid optimized CNN-SVM classifier to classify illegitimate biosensors and failure links in the EEG network. The optimized CNN uses self-learning for feature map extraction, which is sent to the SVM for binary classification. We built the model over 1000 epochs with 1000 batch sizes, using the binary "cross entropy" function to determine the model's loss in binary classification.

The proposed architecture of the hybrid CNN-SVM model is shown in the fig. 7.



Input	
Conv1 layer B.N1 layer M.P1 layer B.N1 layer	Conv1 layer B.N1 layer M.P1 layer B.N1 layer
Concatenation layer	
Conv2 layer B.N2 layer M.P2 layer B.N2 layer	Conv2 layer B.N2 layer M.P2 layer B.N2 layer
Concatenation layer	
Conv3 layer B.N3 layer M.P3 layer B.N3 layer	Conv3 layer B.N3 layer M.P3 layer B.N3 layer
Concatenation layer	
Conv4 layer B.N4 layer M.P4 layer B.N4 layer	Conv4 layer B.N4 layer M.P4 layer B.N4 layer
Concatenation layer	
Conv5 layer B.N5 layer M.P5 layer B.N5 layer	Conv5 layer B.N5 layer M.P5 layer B.N5 layer
Conv5 layer B.N5 layer M.P5 layer B.N5 layer	Conv5 layer B.N5 layer M.P5 layer B.N5 layer
Conv5 layer B.N5 layer M.P5 layer B.N5 layer	Conv5 layer B.N5 layer M.P5 layer B.N5 layer
Concatenation layer	
Flatten layer	
Dense layer	
Dense layer	
SVM classifier	
Output	

Fig.7. Optimized CNN-SVM architecture of a modified VGG16-SVM version

B. Process for Detecting and Isolating Malicious Nodes and Failure Links in WBAN

The process of detecting and isolating malicious nodes and failure links in a WBAN involves a trust-based routing strategy, as shown in Figure 8. The network was originally designed to function autonomously with a standard routing protocol, allowing for a baseline observation of normal network behavior. This knowledge enables us to distinguish between normal and abnormal network activity. In the event of a Blackhole attack, where malicious nodes drop packets to prevent them from reaching their destination biosensor and wireless failure links occur, IDS is deployed on each network biosensor. At runtime, each IDS biosensor monitors the confidence levels of its closest neighbors using three metrics to compute confidence metrics:

- The Positive Conviction factor quantifies a node's confidence in the normalcy of its neighbor, calculated by analyzing successful packets sent and received during communication. The formula for this factor is as follows:

$$PC = (SP_s + SP_r)/(P_d + SP_s + SP_r + 3) \tag{1}$$

- The Negative Conviction factor measures a node's belief that its neighbor is abnormal, determined by examining dropped packets during communication. The formula for computing this factor is:

$$NC = P_d/(SP_s + SP_r + P_d + 3) \tag{2}$$

- The Uncertainty factor reflects a node's level of uncertainty regarding its neighbor's status (normal or abnormal). This factor starts at one when a biosensor first detects its neighbors before any communication occurs. To calculate the Uncertainty factor, the following formula is used:

$$U = 3/(SP_s + SP_r + P_d + 3) \tag{3}$$

As a result, these three factors are always considered in the following manner:

$$U + PC + NC = 1 \tag{4}$$

Where:
$\boldsymbol{PC}$: *Positive Conviction factor*
$\boldsymbol{NC}$: *Negative Conviction factor*
$\boldsymbol{SP_s}$: *Successful Packets sent*
$\boldsymbol{SP_r}$: *Successful Packets received*
$\boldsymbol{P_d}$: *Packets dropped (unsuccessful packets transmitted or received)*
$\boldsymbol{U}$: *Uncertainty factor*

Before transmitting data, a biosensor's conviction values are both 0, and its neighbor's uncertainty value is 1. During transmission, these values are updated based on packet sending, receiving, and dropping. The confidence value is regularly computed, and if the negative conviction surpasses a threshold, a system abnormality is detected.

At this point, identification rules are applied to recognize attacks like the Black Hole Attack, while considering network congestion. If a node is identified as an attacker, it is treated as malignant and not allowed in the network.

The threshold value is established by computing the mean packet delivery ratio under normal circumstances without malicious nodes. These measurements serve as a threshold to detect abnormal activity.

Trust values are regularly updated to detect an intrusion like the Black Hole Attack. If an illegitimate biosensor is identified, it is isolated and not allowed to participate in routing. The biosensor looks for another trusted route to reach its destination after removing the malicious node.

In other words, since every biosensor will be executing IDS, every biosensor can track the behaviors of its close neighbor. Every biosensor monitors the positive conviction, negative conviction, and uncertainty factors of its neighbor biosensors. If the negative conviction factor of some neighbor sensor exceeds the computed threshold value, the following acts are required:

- Identification of the attack and attacker to distinguish between a routing attack and network congestion, it is crucial to identify both the attack and the attacker. To determine if a black hole attack is occurring, a specific formula is used:

$$PTR = P_r(S)/P_r(SS) \tag{5}$$

Where:
$\boldsymbol{PTR}$: *Packet Transmission Rate*
$\boldsymbol{P_r(S)}$: *Number of received packets by a sensor S*
$\boldsymbol{P_r(SS)}$: *Number of sent packets by S's neighbors that aren't destined for S*

The malicious sensor (S) is detected and identified as an attacker, If (S) continues falling packets for a sufficient period. Specifically, if the Packet Transmission Rate is equal to one and the denominator is not equal to zero, then the sensor is considered to be the attacker.

- Isolation of the illegitimate biosensors from WBAN: once the malicious node has been identified, the sensor that detected it will isolate it from the WBAN.

Each biosensor in the WBAN is responsible for maintaining a trusted routing table that contains the identification numbers of legitimate neighboring biosensors. This creates a complete network in which all the biosensors can communicate with each other, while the illegitimate ones are isolated.

C. Data Encryption Process Using Modified RSA Cipher-based Algorithm

The RSA public-key cryptosystem is the most extensively utilized algorithm for public-key cryptography [13]. It was the pioneering algorithm of its type and continues to be a popular choice today. The technique of encrypting data involves a modified version of the classic RSA cipher algorithm. The following equations can be used to represent encryption and decryption:

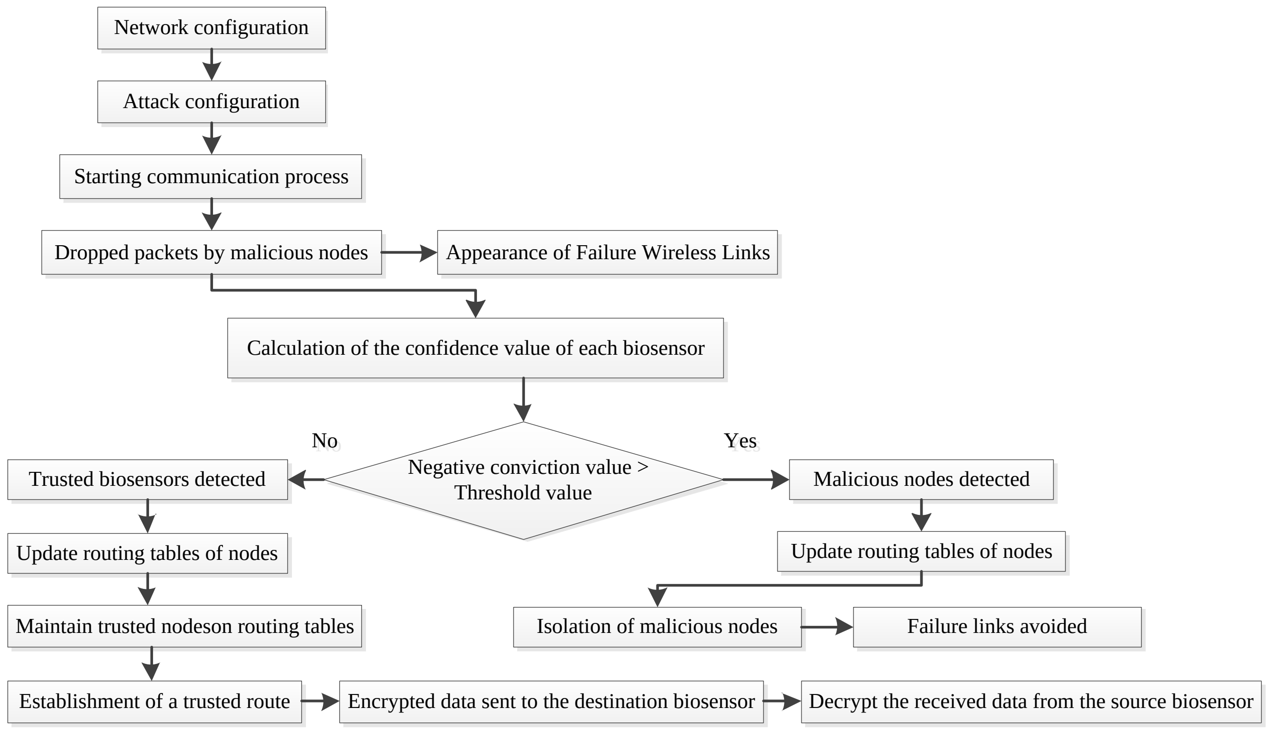

Network configuration
Attack configuration
Starting communication process
Dropped packets by malicious nodes
Appearance of Failure Wireless Links
Calculation of the confidence value of each biosensor
No
Yes
Negative conviction value > Threshold value
Trusted biosensors detected
Malicious nodes detected
Update routing tables of nodes
Update routing tables of nodes
Maintain trusted nodeson routing tables
Isolation of malicious nodes
Failure links avoided
Establishment of a trusted route
Encrypted data sent to the destination biosensor
Decrypt the received data from the source biosensor

Fig.8. Block of detection and isolation of malicious nodes and failure links in WBAN with data encryption block

$$Modified\ RSA\ Encryption: CT = PT^{e} mod\ N \tag{6}$$

$$Modified\ RSA\ Decryption: PT = CT^{d} mod\ N \tag{7}$$

Where:
$\boldsymbol{PT}$: *refers to Plain-Text.*
$\boldsymbol{CT}$: *refers to Cipher-Text*
$\boldsymbol{e}$: *refers to the public key of the encryption process*
$\boldsymbol{N}$: *represents part of the public-key*
$\boldsymbol{d}$: *refers to the secret key of the decryption process*

The modulus N utilized to perform modular arithmetic is the product of six large prime numbers symbolized by **p, q, u, v, w,** and **z**. In addition, a mathematical relationship exists between e and d, represented by the following formula:

$$e = d^{-1} mod\ \phi(N) \tag{8}$$

Where:
$\boldsymbol{\phi(N)}$: *Eleur's Phi function, and is computed as follows:*

$$\phi(N) = (p-1)(q-1)(u-1)(v-1)(w-1)(z-1) \tag{9}$$

If the public key N can be factored into p, q, u, v, w, and z, it would be possible to calculate ϕ(N) and the secret decryption key d using the following formula:

$$d = e^{-1} mod\ \phi(N) \tag{10}$$

The security of the modified RSA algorithm depends on the difficulty of factoring the modulus N. If the modulus N is large enough, it cannot be factored, making it impossible to obtain d. Thus, the modified RSA cipher uses 2048-bit keys and performs all arithmetic on 2048-bit numbers to ensure that a brute-force attack cannot easily break it.

The suggested modified RSA composed of seven steps are:

- Selection of six prime numbers to calculate the N parameter using the following equation:

$$N = p.q.u.v.w.z \tag{11}$$

- Calculation of Eleur's Phi function $\phi(N)$ using the equation (9).
- Selection of an integer e with $\gcd(N, e) = 1$ and $1 < e < N$
- Calculation of an integer d using the equation (10). The public key is: (N, e) and the secret key is: (N, d).
- Encryption operation is done using the equation (6).
- The decryption operation is done using equation (7).
- An update of the public and private keys is performed at each communication.

3.2. Features Selection and Extraction Process

During the characteristics extraction phase, a set of features is extracted from a vast database created based on network simulation outcomes using NS2v2.35 software. These features are utilized to solve classification problems.

This paper focuses on selecting four sufficient features from a large dataset to classify malicious nodes. These four features include distance metric, trust value, latency, and energy consumption. Another five sufficient features are selected from a large dataset to classify failure links. These five features include distance metric, weight factor, path loss, sensor mobility index, and residual energy.

Finally, these eight features are calculated as follows:

- Distance metric feature [14]: this metric determines the medical biosensor localization in the network, and is calculated by the following formula:

$$Dist_{metric}(Msn_i,\ MSink) = \sqrt{\big(X(MSink) - X(Msn_i)\big)^2 + \big(Y(MSink) - Y(Msn_i)\big)^2} \tag{12}$$

$$Dist_{metric}(Msn_i,\ Msn_j) = \sqrt{\big(X(Msn_i) - X(Msn_j)\big)^2 + \big(Y(Msn_i) - Y(Msn_j)\big)^2} \tag{13}$$

- Mobility index feature [14] gauges the medical sensor's motion over time, utilizing both its velocity and a weight factor. It's calculated as follows:

$$MI_f(Msn_i, Msn_j, MSink) = (V_i \times Wf)/(V_i \times Wf) \tag{14}$$

- Confidence value characteristic [14] is computed by analyzing the transmission and reception of packets among sensor nodes. The calculation of this feature is outlined by the following equation:

$$CV_f = PCT/(PCT + PCD) \tag{15}$$

- Latency feature [14] determines the elapsed time for the packet to reach its destination. The formula used to compute this metric is as follows:

$$L_f = \sum T_{Rec}(P) - \sum T_{tran}(P) \tag{16}$$

- Weight Factor Characteristic helps to differentiate between legitimate and illegitimate medical sensors. Illegitimate sensors discard transmitted packets from or to source or destination sensors, while legitimate sensors transfer packets to or from source or destination sensors. This characteristic is computed based on the behavior of the sensors:

$$Wf_f = (T_{ran} + R_{ec})/[(1 - T_{ran}) * (1 - R_{ec})] \tag{17}$$

- Path loss feature is related to signal attenuation. It occurs when wireless medical sensors move outside or inside the body, which can affect the conveyed signal. Attenuation varies with frequency and distance. This metric is calculated using the following formula:

$$PL_f = (4\pi . f_{req} . Dist_{metric})/c^2 \tag{18}$$

- Residual energy feature gauges the amount of energy that medical sensors retain following network data transmission, determining the medical sensor lifespan following a given period of data transmission. Medical sensors may be deemed illegitimate if they have low residual energy and produce damaged wireless links. The sensor residual energy is computed as follows:

$$RE = IE - CE \tag{19}$$

- Energy consumption function which varies depending on the nature of the sensor. An illegitimate medical sensor consumes more power than a legitimate medical sensor. This metric is calculated by the following formula:

$$CE = Time.Power \tag{20}$$

Where:
$\boldsymbol{Dist_{metric}}$: *parameter related to the distance metric between medical sensors.*
V_i: *parameter related to medical sensor velocity.*
$\boldsymbol{PCT}$: *parameter related to the correctly transmitted packets from the medical sink,* Ms_i*, or* Ms_j *biosensors.*
$\boldsymbol{PCD}$: *parameter related to the correctly dropped packets by illegitimate biosensors.*
$\boldsymbol{T_{tran}(P)}$: *time taken for packet transmission.*
$\boldsymbol{T_{Rec}(P)}$: *time taken for packet reception.*
$\boldsymbol{T_{ran}}$: *parameter related to packets transmitted from the medical sink,* Ms_i*, or* Ms_j *biosensors.*
$\boldsymbol{R_{ec}}$: *parameter related to packets received from the medical sink,* M_{si}*, or* Ms_j *biosensors.*
$\boldsymbol{f_{req}}$: *parameter related to the frequency.*
$\boldsymbol{c}$: *parameter related to light speed.*
$\boldsymbol{IE}$: *parameter refers to initial energy.*
$\boldsymbol{CE}$: *parameter refers to consumed energy.*

4. Results and Discussions

In the WBAN environment, we have successfully implemented an intrusion detection system to identify and isolate any unauthorized biosensors and failure links. To simulate the network, we utilized the NS2 version 2.35 Network Simulator tool and employed various metrics listed in Table 1 to construct the EEG network.

The EEG network simulation incorporates one hundred biosensors, of which twenty-five are illegitimate, and fifteen failure links have been introduced. Illegitimate biosensors hinder the transmission of packets from the sender to the receiver biosensor, while failure links cause disruption.

We conducted the network simulation to assess its performance in three distinct scenarios: in the normal case, under illegitimate biosensors, and after detecting and preventing malicious biosensors and failure links. We based the evaluation on measures such as data bit rate, transmission delay, consumed energy, and packet delivery ratio.

Table 1. Simulation setup

Various Metrics	Values
Medical sensors count	16-100 biosensors
Illegitimate medical sensors count	2-25 biosensors
Damaged wireless links count	10-15 failure links
The initial energy of medical sensors	1000 Joul
Amount of energy consumed by each medical sensor	30 mJoul
Count of transmitted packets by each medical sensor	300 packets
Square simulation area	1000m*1000m

Fig. 9 is a screenshot of the EEG network simulation taken at (t) time. The EEG network is simulated in the normal case (without malicious nodes) with one hundred sensors installed in a star topology with one sensor sink located in the center of the network represented by an ID number of 0, and twelve source or destination sensors located around of the sink and represented by ID numbers of 5, 28, 61, 53, 25, 76, 95, 51, 24, 75, 94 and 50. In this example, the sink source sends packets to the destination biosensor with an ID number of 53 through intermediate nodes with an ID number of 38 and 48. It is observed that the sensitive data transmission via the shortest route has been established between the sender biosensor and the receiver biosensor based on hop count and sequence number succeeding.

Fig. 10 is a screenshot of the previous EEG network simulation taken at (t) time. But here, the EEG network is simulated under twenty-five illegitimate sensors represented in red color with ID numbers of 2, 3, 6, 7, 10, 11,20, 33, 34, 37, 38, 41, 43, 47, 57, 58, 62, 63, 65, 66, 73, 82, 85, 87, 88. In this example, it is observed that the illegitimate biosensors with an ID number of 37 didn't forward any packets from the sink with an ID number of 0 to the destination sensor with an ID number of 53 and discarded the packets sent to it, in this case, a wireless link linked the source and the destination is considered as failure link.

Fig. 11 is a screenshot of the previous EEG network simulation taken at (t) time. In the present simulation, an Intrusion Detection System has been integrated to safeguard the network. The simulation demonstrates that the recommended secured routing approach, which is based on trust value and the RSA cipher algorithm, successfully enables the source biosensor identified by an ID of 0 to prevent unauthorized access by the biosensor with an ID of 37 and establish a dependable route to the destination sensor with an ID of 53. The source and destination biosensors can exchange encrypted messages using a modified RSA cipher algorithm.

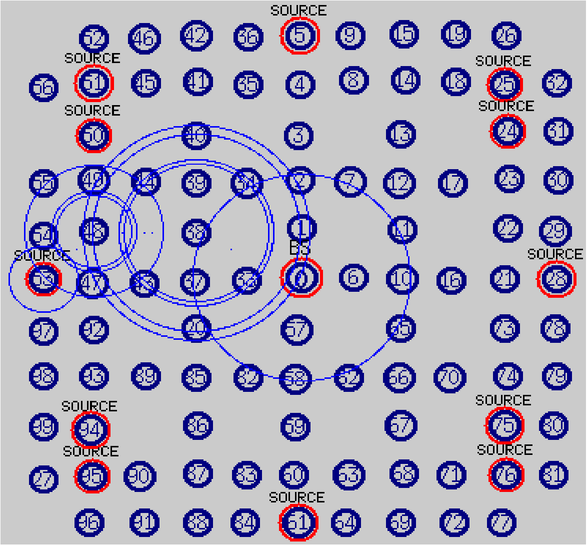


Fig.9. WBAN simulation in normal case

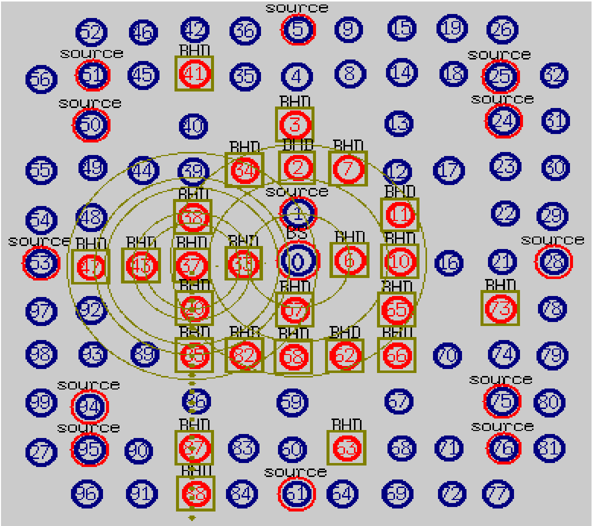
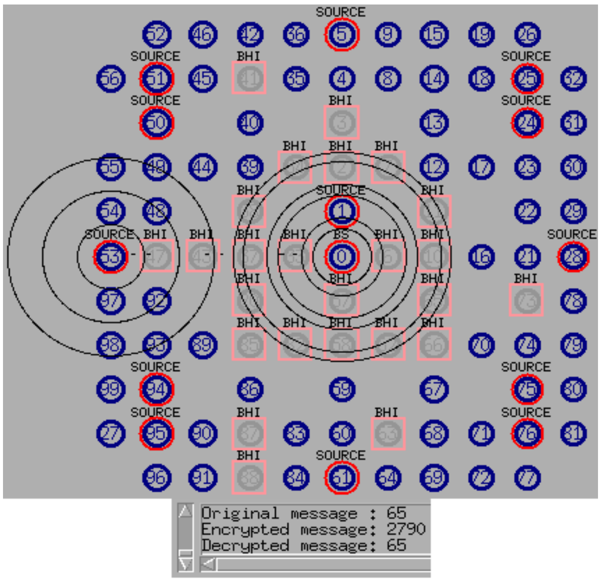


Fig.10. WBAN simulation under illegitimate biosensor attacks



```
Original message : 65
Encrypted message: 2790
Decrypted message: 65
```

Fig.11. Establishment of trusted and secured route establishment of trusted and secured route

Table 2 displays the obtained outcomes in terms of data bit rate, transmission delay, packet delivery ratio, and energy consumed in the normal case (without suspicious biosensors).

Table 2. The EEG network performances without illegitimate biosensors

Malicious nodes	Data rates (bit/s)	Delay (ms)	Packet Delivery Ratio (%)	Energy consumption (MJ)
0	897640	1.4549	92.6013	3.3489

Our findings, as presented in Table 3, illustrate the effects of illegitimate EEG biosensors on transmission delay, data bit rate, packet delivery ratio, and energy consumption measures. We noticed that an increase in the number of illegitimate EEG sensors directly corresponds to a rise in energy consumption and transmission delay. Conversely, the count of illegitimate EEG biosensors has an inverse relationship with the network data bit rate and packet delivery ratio.

Table 3. The EEG network performances with illegitimate biosensors

Malicious nodes	Data rates (bit/s)	Delay (ms)	Packet Delivery Ratio (%)	Energy consumption (MJ)
5	896983	1.3469	92.2155	15.783
10	896884	1.5527	92.2052	16.094
15	892128	1.8369	91.7162	16.404
20	887130	1.8893	91.2024	16.405
25	880950	2.3627	90.5670	16.410
Average	890815	1.7977	91.58126	16.2192

We analyzed the impact of the intrusion detection system on data bit rate, transmission delay, packet delivery ratio, and energy consumption, and our results are presented in Table 4. Our findings indicate that the system significantly enhances network performance. We also observed that the system effectively isolates malicious nodes as the performance measurements remain constant even with an increased number of illegitimate biosensors.

Table 4. The EEG network performances after the detection and isolation of illegitimate biosensors

Malicious nodes	Data rates (bit/s)	Delay (ms)	Packet Delivery Ratio (%)	Energy consumption (MJ)
5	929600	1.5536	98.0591	2.9955
10	929600	1.5536	98.0591	2.9955
15	929600	1.5536	98.0591	2.9955
20	929600	1.5536	98.0591	2.9955
25	929600	1.5536	98.0591	2.9955
Average	929600	1.5536	98.0591	2.9955

We compare the network performance of three simulated cases: an EEG network simulation under normal circumstances without illegitimate biosensors, under illegitimate biosensors, and when the suggested IDS is implemented. The network performance will be compared based on data bit rate, transmission delay, energy consumption, and packet delivery ratio. Table 5 presents the comparison results. The results show that implementing the suggested IDS enhances the data bit rate, energy consumption, and packet delivery ratio measures compared to an EEG network simulation with or without illegitimate biosensors.

Table 5. The variation of the network performances in three cases

Metrics	Data rates (bit/s)	Delay (ms)	Packet Delivery Ratio (%)	Energy consumption (MJ)
Normal case	897640	1.4549	92.6013	3.3489
With illegitimate biosensors	890815	1.7977	91.58126	16.2192
Without illegitimate biosensors	929600	1.5536	98.0591	2.9955

Table 6 displays the obtained outcomes in terms of malicious nodes and failure links classification rate, sensitivity, and specificity of the suggested optimized CNN-SVM (modified VGG16-SVM version) classifier compared to some classifiers such as support vector machine, traditional VGG16, and modified VGG16 models. The suggested optimized CNN-SVM (modified VGG16-SVM version) classifier achieved the highest value of malicious nodes and failure links classification rate, sensitivity, and specificity compared to other classifiers.

Table 6. Classification of malicious nodes and failure links using CNN-SVM

Classifiers	SVM	VGG16	Modified VGG16	Modified VGG16-SVM
Malicious nodes Sensitivity	89.16 %	100 %	90.15 %	90.15%
Malicious nodes Specificity	94.91 %	88.35 %	88.44%	88.43%
Malicious nodes Classification	97.60 %	99.00 %	99.52%	99.59 %
Failure links Sensitivity	94.00 %	100 %	100 %	100%
Failure links Specificity	94.91 %	93.81%	93.84 %	93.84 %
Failure links Classification	98.16 %	98.76 %	98.78 %	99.00 %

Compared to other techniques, such as those by Mahuwa Goswami et al. [15] and L. Maheshavel et al. [16], the suggested technique provides better outcomes in terms of Data Bit Rate and Transmission Delay without the presence of malicious nodes, as shown in Table 7.

Table 7. Comparison with other works in terms of network performances in the normal case

Techniques	Data bit rate (bit/s)	Transmission delay (ms)	Packet Delivery Ratio
Suggested IDS	897640	1.4549	92.00 %
Mahuwa Goswami et al. (2020) [15]	85672	29.3400	92.96 %
L. Maheshavel et al. (2021) [16]	71380	20.0177	99.38 %

Compared to other techniques, like Mahuwa Goswami et al. (2020), L. Maheshavel et al. (2021), and Biswaraj Sen et al. (2018). The suggested technique gives the best outcomes in terms of Data Bit Rate, Packet Delivery Ratio, and Transmission Delay under suspicious biosensors (table 8).

Table 8. Comparison with other works in terms of network performances with malicious node attacks

Techniques	Data bit rate (bit/s)	Transmission delay (ms)	Packet Delivery Ratio
Suggested IDS	890815	01.7977	91.58126
Mahuwa Goswami et al. (2020) [15]	6644.00	75.34800	17.1520
L. Maheshavel et al. (2021) [16]	18730.0	26.52430	16.8867
Biswaraj Sen et al. (2018) [17]	124379	2206.9285	20.1275

Compared to other techniques, like Dinesh Kumar Anguraj et al. (2019), Mahuwa Goswami et al. (2020), and Biswaraj Sen et al. (2018). The suggested technique gives the best outcomes in terms of Data Bit Rate, Transmission Delay, and packet delivery ratio after avoiding illegitimate biosensors and failure links (table 9).

Table 9. Comparison with other works in terms of network performances without malicious node attacks

Techniques	Data bit rate (bit/s)	Transmission delay (ms)	Packet Delivery Ratio
Suggested IDS	929600	1.5536	98.0591
Dinesh Kumar Anguraj et al. (2019) [4]	0.664	744.000	78.0000
Mahuwa Goswami et al. (2020) [15]	80810	12.546	88.0880
Biswaraj Sen et al. (2018) [17]	209310	2664.7463	33.0900

Table 10 shows the performance of the suggested modified RSA cipher algorithm compared to the classical RSA cipher algorithm in terms of the strength of the prime number, the prime number calculation time, and the update of keys. We distinguished that the suggested modified RSA cipher is more robust than the classical RSA cipher algorithm.

Table 10. Comparison between a modified RSA and a classical RSA cipher

Cryptographic algorithms	The strength of the number N	Prime numbers calculation time	Key update
Our modified RSA	Depends on six prime numbers	Before algorithm starts	Yes
Classic RSA	Depends on two prime numbers	During the data transmission	No
Modified RSA (2013) [18]	Depends on three prime numbers	Before algorithm starts	No
Modified RSA (2015) [19]	Depends on four prime numbers	During the data transmission	No

To assess the efficacy of our enhanced CNN-SVM approach in classifying malicious nodes, we conducted a comparative analysis with other methodologies, including those introduced by Katakam Tejaswini and Yannam Adilakshmi (2020), as well as Mahin Syeda Hajra et al. (2019). Our proposed techniques surpassed these approaches and attained the highest classification rate for malicious nodes, as evidenced by Table 11.

Table 11. Comparison with other works in terms of classification rate for detecting malicious nodes

Authors	Algorithms	Classification rate
Our classifier (2023)	SVM VGG16 Modified VGG16 Modified VGG16-SVM	97.60 % 99.00% 99.52% 99.59 %
Katakam Tejaswini et al. (2020) [20]	SVM	82.35 %
Mahin Syeda Hajra et al (2019) [21]	SVM	97.50 %

To evaluate the efficiency of our optimized CNN-SVM method in classifying failure links, we conducted a comparative analysis with other techniques, including the one suggested by S. Arockia Jayadhas et al. (2021). As presented in Table 12, our proposed approach demonstrated superior performance in terms of classifying failure links.

Table 12. Comparison with other works in terms of classification rate for detecting failure links

Authors	Algorithms	Classification rate
Our classifier (2023)	SVM VGG16 Modified VGG16 Modified VGG16-SVM	98.16% 98.76% 98.78% 99.00%
S. Arockia Jayadhas et al (2021) [22]	VGG16	98.40 %

Table 13. Comparison between a modified RSA et al. cipher algorithms

Cryptographic algorithms	Key Size	Architecture	Security level
Suggested modified RSA cipher	2048 bits	Asymmetric	High
One-Time Password Algorithm (2023) [23]	512 bits	Symmetric	Low
Elliptic Curve Cryptography (2022) [24]	512 bits	Asymmetric	High

Table 14. Advantages of the intrusion detection systems

Methods	Trusted route	Encrypted communication
Our methods	✓	✓
Rajesh Kumar D et al. (2021) [3]	✓	✗
Dinesh Kumar Anguraj et al. (2019) [4]	✓	✗
Ali Raza Bhangwar et al. (2017) [5]	✓	✗
Sangeetha Ramaswamy et al. (2022) [6]	✓	✗
Damanpreet Kaur et al. (2020) [7]	✗	✓
Sangwon Shin et al. (2019) [8]	✗	✓
A. Basnet et al. (2022) [9]	✗	✓
Gurbeer Kaur et al. (2017) [10]	✗	✓
Mohammed Ramadan et al. (2020) [11]	✗	✓
Mahuwa Goswami et al. (2020) [15]	✓	✗
L. Maheshavel et al. (2021) [16]	✓	✗
Biswaraj Sen et al. (2018) [17]	✓	✗
S. Arockia Jayadhas et al (2021) [22]	✓	✗
Dass, R, et al. (2023) [23]	✓	✓
Kaur, A., et al. (2022) [24]	✓	✓
Sangeetha Ramaswamy et al. (2012) [25]	✓	✗
Swapnil S. Bhalsagar (2019) [26]	✓	✗
Mallikarjuna Anantapur et al. (2021) [27]	✓	✗
Shin, S, et al. (2020) [28]	✗	✓
C. Senthilkumar et al. (2015) [29]	✓	✗
K. N. Ambili et al. (2016) [30]	✓	✗
Alattas, R (2020) [31]	✓	✗

Table 13 shows the performance of the suggested modified RSA cipher algorithm compared to other cipher algorithms in terms of the key size, the algorithm's architecture, and the security level. We distinguished that the suggested modified RSA cipher is more strength than other cipher algorithms.

Compared to other techniques, like Rajesh Kumar D et al. (2021), Dinesh Kumar Anguraj et al. (2019), Ali Raza Bhangwar et al. (2017), Sangeetha Ramaswamy et al. (2022), Damanpreet Kaur et al. (2020), Sangwon Shin et al. (2019), A. Basnet et al. (2022), Gurbeer Kaur et al. (2017), Mohammed Ramadan et al. (2020), Mahuwa Goswami et al. (2020), L. Maheshavel et al. (2021), Biswaraj Sen et al. (2018), Ambili, K. N et al. (2019), Dass, R et al. (2023), Kaur, A et al. (2022), Sangeetha Ramaswamy et al. (2012), Swapnil S. Bhalsagar (2019), Mallikarjuna Anantapur et al. (2021), Shin, S et al. (2020), C. Senthilkumar et al. (2015), K. N. Ambili et al. (2016), Alattas, R (2020). The suggested intrusion detection system offers both of trusted route and encrypted communication (table 14).

5. Conclusions

Wireless Malicious biosensor attacks can cause failure links and discard data packets, which can degrade the performance of wireless body area networks (WBANs). To combat this issue, we have developed a hybrid intrusion detection system (IDS) that combines an optimized convolutional neural network (CNN) with a support vector machine (SVM), a trust-based routing algorithm, and a cryptographic algorithm based on the modified RSA cipher.

Our system utilizes the optimized CNN with SVM to classify nodes and links as either malicious or not, and failures or not. It then employs a trust-based routing algorithm to detect and isolate malicious nodes by finding an alternate and trusted path. Finally, it uses the modified RSA cipher algorithm to ensure sensitive data protection against malicious attacks.

Extensive simulations have shown that our IDS enhances network performance in terms of packet delivery ratio, transmission delay, data bit rate, and energy consumption, while also bolstering network security by avoiding malicious nodes and failure links. Our approach achieves a 99.13% malicious nodes classification rate using the modified VGG16 with SVM classifiers, surpassing similar systems with a single SVM classifier that have achieved rates of 82.35% and 97.5%. Additionally, our approach achieves a 99.97% failure links classification rate using the modified VGG16 with SVM classifiers, surpassing a similar system with a single VGG16 classifier that has achieved a rate of 98.40%.

In the future, we plan to implement our proposed system in the WBAN environment using Arduino and Raspberry cards to prevent malicious node attacks.

References

[1] A. Ghumro, A. Ahmed, and A. K. Memon, "Node Misbehavior Attacks in WBAN: Effects and Countermeasures".

[2] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," Journal of Sensors, vol. 2016, pp. 1–16, 2016, doi: 10.1155/2016/4731953. I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," Journal of Sensors, vol. 2016, pp. 1–16, 2016, doi: 10.1155/2016/4731953.

[3] R. K. Dhanaraj, R. H. Jhaveri, L. Krishnasamy, G. Srivastava, and P. K. R. Maddikunta, "Black-Hole Attack Mitigation in Medical Sensor Networks Using the Enhanced Gravitational Search Algorithm," Int. J. Unc. Fuzz. Knowl. Based Syst., vol. 29, no. Supp02, pp. 297–315, Dec. 2021, doi: 10.1142/S021848852140016X.

[4] Anguraj, D.K., Smys, S. Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks. Wireless Pers Commun 104, 1–20 (2019). https://doi.org/10.1007/s11277-018-6005-x.

[5] A. R. Bhangwar, P. Kumar, A. Ahmed, and M. I. Channa, "Trust and Thermal Aware Routing Protocol (TTRP) for Wireless Body Area Networks," Wireless Pers Commun, vol. 97, no. 1, pp. 349–364, Nov. 2017, doi: 10.1007/s11277-017-4508-5.

[6] S. Ramaswamy and U. D. Gandhi, "Trust-Based Data Communication in Wireless Body Area Network for Healthcare Applications," BDCC, vol. 6, no. 4, p. 148, Dec. 2022, doi: 10.3390/bdcc6040148.

[7] D. K. E. Al. Damanpreet Kaur Et Al., and TJPRC, "Privacy Preserved Healthcare System for Wireless Body Area Networks," IJMPERD, vol. 10, no. 3, pp. 12191–12202, 2020, doi: 10.24247/ijmperdjun20201166.

[8] S. Shin, S. Choi, K. Won, and S. Shin, "Preprocessed symmetric RSA authentication for wireless body area networks in space," in Proceedings of the Conference on Research in Adaptive and Convergent Systems, Chongqing China: ACM, Sep. 2019, pp. 230–235. doi: 10.1145/3338840.3355675.

[9] A. Basnet, A. Alsadoon, P. W. C. Prasad, O. H. Alsadoon, L. Pham, and A. Elchouemi, "A Novel Secure Patient Data Transmission through Wireless Body Area Network: Health Tele-Monitoring," Int. j. commun. netw. inf. secur., vol. 11, no. 1, Apr. 2022, doi: 10.17762/ijcnis.v11i1.3801.

[10] G. Kaur and N. Kaur, "Cost Effective Energy Efficient and Secure Routing Protocol (CESR) for WBAN," IJCA, vol. 169, no. 4, pp. 37–43, Jul. 2017, doi: 10.5120/ijca2017914727.

[11] M. Ramadan, Y. Liao, F. Li, S. Zhou, and H. Abdalla, "IBEET-RSA: Identity-Based Encryption with Equality Test over RSA for Wireless Body Area Networks," Mobile Netw Appl, vol. 25, no. 1, pp. 223–233, Feb. 2020, doi: 10.1007/s11036-019-01215-9.

[12] K. Kalaiselvi, L. Vanitha, K. Deepa Thilak, T. Rajesh Kumar, S. Saranya, and K. Kumaresan, "RETRACTED ARTICLE: Performance Analysis of Malicious and Link Failure Detection System Using Deep Learning Methodology," Wireless Pers Commun, vol. 127, no. S1, pp. 25–26, Dec. 2022, doi: 10.1007/s11277-021-08790-9.

[13] 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.

[14] 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.

[15] research scholar , pacific university (PAHER), Udaipur ,Rajasthan, India., M. Goswami*, Dr. P. Sharma, HOD CSE , pacific university (PAHER), Udaipur ,Rajasthan, India, A. Bhargava, and Assistant Professor CSE, , pacific university (PAHER), Udaipur ,Rajasthan, India, “Black Hole Attack Detection in MANETs using Trust Based Technique,” IJITEE, vol. 9, no. 4, pp. 1446–1451, Feb. 2020, doi: 10.35940/ijitee.D1497.029420.

[16] L. Maheshavel and C. Senthilkumar, “Mitigation of black hole attack in MANETs: A sequence no-based approach,” J. Phys.: Conf. Ser., vol. 1917, no. 1, p. 012011, Jun. 2021, doi: 10.1088/1742-6596/1917/1/012011.

[17] B. Sen, M. G. Meitei, K. Sharma, M. K. Ghose, and S. Sinha, “Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold Mechanism,” vol. 13, no. 7, 2018.

[18] R. Patidar and R. Bhartiya, “Modified RSA cryptosystem based on offline storage and prime number,” in 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, Tamilnadu, India: IEEE, Dec. 2013, pp. 1–6. doi: 10.1109/ICCIC.2013.6724176.

[19] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[20] K. Tejaswini and M. Y. Adilakshmi, “Black hole Attack Detection Using Machine Learning Algorithms in MANET – Performance Comparision,” vol. 07, no. 06, 2020.

[21] “Detection and Interception of Black Hole Attack with Justification using Anomaly based Intrusion Detection System in MANETs,” IJRTE, vol. 8, no. 2S11, pp. 2392–2398, Nov. 2019, doi: 10.35940/ijrte.B1274.0982S1119.

[22] S. Arockia Jayadhas and S. Emalda Roslin, “Link Failure Detection in Multimedia Sensor Networks Using Multi-Tier Clustering Based VGG-CNN Classification Approach,” IJCNA, vol. 8, no. 6, p. 693, Dec. 2021, doi: 10.22247/ijcna/2021/210719.

[23] R. Dass et al., “A Cluster-Based Energy-Efficient Secure Optimal Path-Routing Protocol for Wireless Body-Area Sensor Networks,” Sensors, vol. 23, no. 14, p. 6274, Jul. 2023, doi: 10.3390/s23146274.

[24] A. Kaur and J. Kaur, “Trust based Security Protocol to mitigate black hole Attacks in Mobile Adhoc Networks,” In Review, preprint, Oct. 2022. doi: 10.21203/rs.3.rs-2197795/v1.

[25] M. Singh, G. Mehta, C. Vaid, and P. Oberoi, “Detection of Malicious Node in Wireless Sensor Network Based on Data Mining,” in 2012 International Conference on Computing Sciences, Phagwara, India: IEEE, Sep. 2012, pp. 291–294. doi: 10.1109/ICCS.2012.24.

[26] S. S. Bhalsagar, M. D. Chawhan, Y. Suryawanshi, and V. K. Taksande, “Performance Evaluation of Routing Protocol Under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms,” vol. 8, no. 5, 2019.

[27] “Ant Colony Optimization Based Modified AODV for Secure Routing in Mobile Ad Hoc Networks,” IJIES, vol. 14, no. 6, pp. 115–124, Dec. 2021, doi: 10.22266/ijies2021.1231.11.

[28] S. Shin, K. Won, and S. Shin, “Size efficient preprocessed symmetric rsa for wireless body area network,” SIGAPP Appl. Comput. Rev., vol. 20, no. 1, pp. 15–23, Apr. 2020, doi: 10.1145/3392350.3392352.

[29] C. Senthilkumar and N. Kamaraj, “Mitigation of Blackhole Attack Using Trusted AODV,” Australian Journal of Basic and Applied Sciences, 2015.

[30] K. N. Ambili and Jimmy Jose, “Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems,” in Information Science and Applications, K. J. Kim and H.-Y. Kim, Eds., in Lecture Notes in Electrical Engineering, vol. 621. Singapore: Springer Singapore, 2020, pp. 631–638. doi: 10.1007/978-981-15-1465-4_62.

[31] R. Alattas, “Detecting black-hole attacks in WSNs using multiple base stations and check agents,” in 2016 Future Technologies Conference (FTC), San Francisco, CA, USA: IEEE, Dec. 2016, pp. 1020–1024. doi: 10.1109/FTC.2016.7821728.

Authors’ Profiles

Mohammed Abdessamad Goumidi is a PhD student in Cryptography and Data Security at the University of Sciences and Technology of Oran, Mohamed Boudiaf (USTO), Algeria. He is attached to the Coding and Security of Information Laboratory (LACOSI) in the Department of Electronic and Electrical Engineering Faculty. His research interests include Artificial Intelligence, Cybersecurity, Wireless Networks, and Cryptography.

E-mail: mohammedabdessamad.goumidi@univ-usto.dz.

Ehlem Zigh is a full professor at the University of Sciences and Technology of Oran, Mohamed Boudiaf, Algeria. She is attached to the Coding and Security of Information Laboratory (LACOSI) within the Department of Electronic and Electrical Engineering Faculty. Her research interests include Image Processing, the Internet of Things, Soft Computing Techniques, E-learning, and Artificial Intelligence.

E-mail: ehlem.zigh@univ-usto.dz.

Naima Hadj-said is a full Professor at the University of Sciences and Technology of Oran, Mohamed Boudiaf in Algeria. She is attached to the Coding and Security of Information Laboratory (LACOSI) in the Department of Computer Science, within the Mathematics and Computer Science Faculty. Her research interests include Cryptography and Digital Communications.
E-mail: naima.hadjsaid@univ-usto.dz

Adda Belkacem Ali-Pacha is a full Professor at the University of Sciences and Technology of Oran, Mohamed Boudiaf in Algeria. He is attached to the Coding and Security of Information Laboratory (LACOSI) in the Department of Electronic, and Electrical Engineering Faculty. He is also the Head of the Coding and Information Security Research Laboratory. His research focuses on Cryptography and Digital Communications.
E-mail: adda.alipacha@univ-usto.dz.

How to cite this paper: Mohammed Abdessamad Goumidi, Ehlem Zigh, Naima Hadj-Said, Adda Belkacem Ali-Pacha, "A Hybrid Intrusion Detection System to Mitigate Biomedical Malicious Nodes", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.2, pp.117-133, 2024. DOI:10.5815/ijcnis.2024.02.10