**User-Based Authentication and DoS Mitigation Scheme for Wearable Wireless Body Sensor Networks**

**Nombulelo Zulu** *∗***, Topside E. Mathonsi***∗∗***, Deon P. du Plessis***∗∗∗***, and Tshimangadzo M. Tshilongamulenzhe***∗∗∗∗*

Tshwane University of Technology

2 Aubrey Matlakala St, Soshanguve,

Pretoria, 0001

South Africa

[*nombulelozuluh@gmail.com, MathonsiTE@tut.ac.za*](mailto:nombulelozuluh@gmail.com,%20MathonsiTE@tut.ac.za), duplessisdp@tut.ac.za, TshilongamulenzheTM@tut.ac.za

***Abstract***— **Wireless Body Sensor Networks (WBSNs) is one of the greatest growing technology for sensing and performing various tasks. The information transmitted in the WBSNs is vulnerable to cyber-attacks, therefore security is very important. Denial of Service (DoS) attacks are considered one of the major threats against WBSNs security. In DoS attacks, an adversary targets to degrade and shut down the efficient use of the network and disrupt the services in the network causing them inaccessible to its intended users. If sensitive information of patients in WBSNs, such as the medical history is accessed by unauthorized users, the patient may suffer much more than the disease itself, it may result in loss of life. This paper proposed a User-Based authentication and DoS mitigation algorithm in WBSNs. A five-phase User-Based authentication and DoS mitigation algorithm for WBSNs was designed by integrating Elliptic Curve Cryptography (ECC) with Rivest Cipher 4 (RC4) to ensure a strong authentication process that will only allow authorized users to access nodes on WBSNs.**

***Keywords:*** *User-based authentication, Denial of Service (DoS) attacks, Wireless Body Sensor Networks (WBSNs), Rivest Cipher 4 (RC4), Elliptic Curve Cryptography (ECC)*

# Introduction

Authentication is a crucial security requirement to avoid attacks against secure communication and to ensure that Denial of Service (DoS) attacks are not exploiting the limited resources of sensor nodes which may result in vital patient’s information getting tampered with. According to Peng, Wang, Guo, Wang & Deng [1] with the help of Wireless Body Sensor Networks (WBSNs), extensive, and uninterrupted health monitoring becomes easy and possible, and the user can enjoy the medical services provided by the application without limitations. Since sensitive data of users is transmitted on private channels, users’ privacy during data transmission is prone to attacks. In DoS attacks, an adversary gets connected with the WBSNs applications. Once the adversary gets a frequency slot in WBSNs, it starts sending a huge amount of traffic to the sensor node, which makes it impossible for the sensor node to process the traffic coming from legitimate nodes [2].

Most wireless network users require consistent and secure systems, however, this is not always the case with WBSNs applications, as the communication channels are visible to many attackers due to their unattended deployment nature. Since the information transmitted via the sensor node is very sensitive and critical, user authentication of such information is of prime importance. If sensitive information, such as the medical history is accessed by unauthorized adversaries, the patient may suffer much more than the disease itself, it may result in a wrong prescription and put the life of a patient at risk which can lead to death. Malicious users can access WBSNs private networks and launch DoS attacks, which can breach the availability of medical devices.

This paper proposed a User-Based authentication and DoS mitigation algorithm to protect WBSNs and ensure that data transferred over the network is kept safe and accessed by only authorized personnel. The algorithm is designed in a way that the user will initiate the process by attempting to log into the network. The first phase in the authentication process is to initialize the server to generate the master key that will be used in the encryption/decryption phase, and the registration of the user will take place to ensure that the user trying to access the network is from the trusted list or exist within the system.

The login (authentication) phase will grant the user access if known/exist else access will be denied, thereafter, the DoS mitigation phase will be processed to ensure that the network has enough power to transport data obtained via sensor nodes. When the network does not have enough power, packets will be dropped this is because the network will be weak and thus vulnerable to attacks. The encryption/decryption phase ensures that the user can access data and view the data using the master key generated from the initializing step, or else deny access if the key used does not match.

The contributions of this paper are as follows: 1) Initializing the server and registration of sensor nodes during data transmission can be used to ensure that data received is from a known and trusted source to minimize the amount of traffic coming from illegitimate nodes. This will ensure that only authorized users are able to access data in the network. 2) The integration of ECC and RC4 ensured that the proposed algorithm is efficient enough and fast when authenticating WBSN users. 3) The proposed User-Based authentication and DoS mitigation algorithm prevented malicious users to connect to the network and prevented attackers from launching a DOS attack in WBSN applications.

This paper is structured as follows: In Section 1, the paper introduced the background of WBSN applications by outlining the aim, the issue the study is attempting to solve, and the contributions of the paper. In Section 2, the paper highlighted the work done by the other researchers in WBSN applications. Section 3 presented the flowchart of the proposed User-Based authentication and DoS mitigation algorithm. In Section 4, this paper discussed the implementation of the proposed algorithm. In Section 5, the paper discussed the chosen simulation tool namely MATLAB. In addition, the section presented the simulation results of the compared algorithms namely, User-Based authentication and DoS mitigation algorithm, biometric authentication algorithm, and cryptographic techniques scheme. Lastly, Section 6 concludes the paper and presents future works.

# Related Works

Over the past years, several studies have been conducted on authentication schemes to protect the information of WBSNs users during the data transmission process.

Zhang, Wang, Vasilakos & Fang [3] proposed the Received Signal Strength Indication (RSSI)-based key agreement scheme. Their study showed that the key agreement process is treated as a simplified error-correcting encoding and decoding with only check symbols being passed from the initiating side to the responding side. Their study achieved both security and efficiency. Their study highlighted one big issue is that RSSI-based key generation and agreement have limited data density. The User-Based authentication and DoS mitigation algorithm proposed in this paper achieved both efficiency and security by integrating ECC with RC4. This was achieved by generating the public key from the private key while protecting the private key from being known when disclosing the public key during the user-authentication process which will mitigate DoS from having slots in the network.

The study conducted by Zhang, Wang, Vasilakos & Fang [3] presented an overview of attacks, principles, and solutions on the anonymity of two-factor authentication schemes. To improve the current schemes from being stuck with the security-usability tension. They proposed integrating “honeywords”, traditionally the purview of system security, with a “fuzzy-verifier”. Their scheme solves two issues, it does not only eliminate the security-usability conflict that is considered intractable in the literature but also achieves security guarantees beyond the conventional optimal security bound. The scheme proposed by Zhang, Wang, Vasilakos & Fang [3] resolved the various issues arising from user corruption and server compromise. Although their proposed scheme is computationally efficient, secure, and lightweight, it does not consider the anonymity of identities and unlikability service. During the authentication process, the proposed algorithm in this paper ensured that both anonymity identity, and unlikability are achieved.

Das, Chatterjee & Sing [4] proposed a biometric-based authentication scheme for hierarchical Wireless Body Area Networks (WBANs), where biometric verification with password verification was used. The efficient cryptographic hash function and symmetric key encryption and decryption algorithm were only required in their scheme and the scheme was lightweight. Later, the study conducted by [5] proved that the scheme could not provide real user anonymity and was easy to trace. Their study proposed and used a new anonymous authentication scheme with bilinear pairing for WBANs which proved that the study conducted by [4] study was easy to trace. The algorithm proposed in this paper ensured password verification during the login phase. The encryption/decryption algorithm is used to ensure that sensitive data is protected during the user authentication process.

The study conducted by [6] proposed a collection of optimization techniques to reduce the energy cost of watchdog utilization when maintaining the security of the network at an appropriate level. It includes the theoretical analyses along with the practical algorithms which can schedule the several tasks of the watchdog based on the position of the node and the trustworthiness of the destination nodes. The study conducted by [7], stated and proved that the scheme proposed in the study conducted by [6] does not provide mutual authentication and is prone to jamming attacks. The proposed algorithm in this paper provides mutual authentication by comparing the user logging detail with the existing information stored in the system. The system administration will ensure that the user is from the trusted list.

Chiou, Ying & Liu [8] proposed a scheme that guarantees anonymity, unlikability, and message authentication for uses. Their scheme has four phases: (1) the Healthcare center uploading phase (HUP), (2) Patient uploading phase (PUP), (3) Treatment phase (TP), and (4) Checking phase (CP). The hash function they used was Secure Hashing Algorithm (SHA)-256, the symmetric encryption algorithm was Advanced Encryption Standard (AES), and the signature algorithm is ECC. The scheme allows patients to consult with doctors directly and remotely in a safe way. However, the scheme still fails to provide patient anonymity and message authentication and it only stores patient medical data, without allowing patients to directly access medical advice. The User-Based authentication and DoS mitigation algorithm proposed in this paper ensured message authentication.

Li, Lee, & Weng [9] presented participant authentication in mobile emergency medical care systems for patient supervision. They propose a secure cloud-assisted architecture for accessing and monitoring health in WBANs. Chaotic maps-based authentication and key agreement mechanisms are utilized to provide data security and mutual authentication. Based on the proposed scheme by [9] designed another dynamic identity and chaotic maps-based authentication scheme and a secure data protection approach to prevent illegal intrusions into medical systems. They also proposed an improved secure authentication and data encryption scheme for smart devices in medical systems. Their scheme exposes the patient and the doctor to the flaw of private key revealing the problem and is failing to provide real-time monitoring service and non-repudiation evidence in doctor diagnosis. The proposed algorithm in this paper provided a key management mechanism during the encryption/decryption process to ensure that the text was encrypted or decrypted using the master key that is only known to the sender

Wu, Xu, Kumari & Li [10] presented a secure three-factor user authentication scheme for Wireless Sensor Networks (WSNs). However, in 2019, Mo & Chen [11] demonstrated that if the user inputs an incorrect password at the login phase in [12] scheme the smartcard does not check whether the password is verified, and the protocol will proceed until GWN finds that the login request of the user was invalid, so Gateway Node performs unnecessary computational resources. In the algorithm proposed, the authentication process ensured that when the credentials provided are incorrect, the user will not be granted access to the system without doing the necessary computational. Thus, the proposed algorithm produced better network throughput.

Koya & Deepthi [13] proposed an anonymous hybrid mutual authentication and key agreement scheme based on Electrocardiography (ECG). However, their scheme is vulnerable to sensor node capture attacks and lacks forward secrecy. Besides, physiological signal-based authentication schemes typically require sensors to monitor unique physiological signals, such as ECG, which makes such schemes lack universality. The integration of ECC and RC4 in this paper ensured that the secrecy in WBSNs was maintained during data transmission.

Wang & Park [14] used different mechanisms and consider sensor node types to avoid traffic analysis attacks in WBSNs applications. A Set of delays in different periods to avoid the traffic was added, by using the scheme the optimal solution was obtained to protect the network with no overheads. Their study also highlighted the drawback of this method is that the delay is twice the actual traffic signal length. The proposed algorithm in this paper seeks to mitigate DoS attacks in WBSNs that cause traffic in a network. The proposed User-Based authentication and DoS mitigation algorithm in this paper reduced the delay in transmitting data caused by the traffic signal length.

According to [15] ECC based authentication and key agreement protocol for Telecare Medicine Information Systems (TMIS) was proposed and declared that it could provide better security and performance. The same identified that the protocol is vulnerable to a replay attack and has an inefficient authentication phase. This paper integrates ECC and RC4 in order to ensure that the user authentication phase was efficient.

Gope & Hwang [17] proposed an efficient mutual authentication and key agreement scheme for global mobility networks. However, the study conducted by [10] pointed out that [17], the scheme lacks session key update and wrong password detection mechanisms, lacks forward secrecy, and is vulnerable to a DoS attack. This paper proposed a Used-Based authentication algorithm that mitigates DoS attacks in WBSNs.

The review of the literature has indicated that previous studies did not propose any scheme that can mitigate DoS attacks efficiently in the WBSNs. To overcome the identified limitation, this paper proposed an efficient User-Based authentication and DoS mitigation algorithm. The proposed algorithm was designed by integrating ECC and RC4 in order to obtain a strong encryption and decryption process protocol was demonstrated in the study conducted by [16] during the data transmission process in WBSNs.

# User-Based Authentication and DoS Mitigation Algorithm Design

The User-Based authentication and DoS mitigation algorithm was designed by integrating ECC and RC4 in order to ensure that sensitive data is kept safe within the WBSNs. The proposed algorithm has five (5) phases namely initialization, registration, login, DoS mitigation, and encryption/decryption. Based on the review of the literature, the attacker may try to change the information by positioning itself next to the victim. However, this cannot be the case in the proposed algorithm since the DoS mitigation phase will ensure that the patient's data is protected by preventing such attacks.

# User-Based Authentication and DoS Mitigation Algorithm Workflow

The overview of the entire system design is demonstrated as shown in Fig. 1. The flowchart illustrates the logic behind carrying out all five phases in the User-Based authentication and DoS mitigation algorithm.

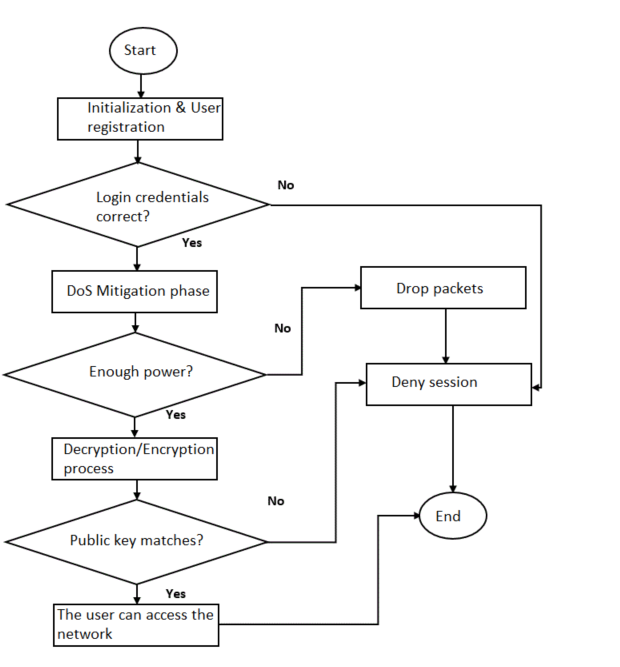


Fig 1: User-based authentication scheme flow diagram

ECC and RC4 were integrated in order to create faster, smaller, and more efficient cryptographic keys. According to Roy & Khatwani [18] ECC is a widely used technique in multi-factor authentication. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. ECC was used in this paper, because it helps to establish equivalent security with lower computing power and battery resource usage [19]. RC4 was used in this paper for the encryption/decryption phase in order to protect patient’s data [20]. RC4 was chosen due to its low computational requirements, speed, and simplicity when implemented. Sensor nodes have enough power to process and transmit data within the network. The authentication process is for individuals to access data within the network, data collected from different sensor nodes, and for the healthcare systems to be able to read and provide services to patients.

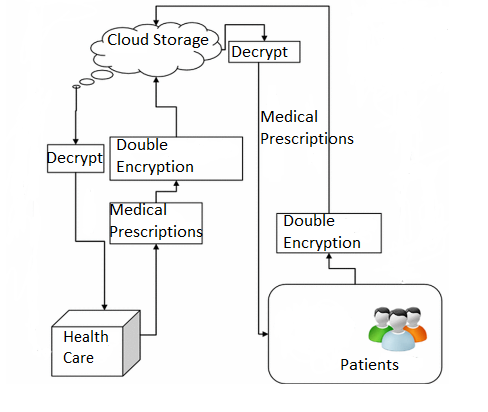


Fig 2: Elliptic Curve Cryptography Algorithm in Wireless Body Sensor Networks

The flow of information from patients (sensor node) to a healthcare server and vice versa is shown in Fig. 2.

Step 1 – Patients: Information is gathered by inserting a sensor node for a certain disease a patient is treated for. The initializing phase takes place in this step where the system administrator generates a master key that will be used by the healthcare server to decrypt the message.

Step 2 – Double encryption: this is where the patient's information gets encrypted by using the encryption algorithm to ensure that only authorized users can view the information being sent.

Step 3 – Cloud Storage: Information gathered from the patient via sensor nodes is saved in the cloud storage while waiting to be accessed by the healthcare institution, in this step the DoS mitigation algorithm is executed to make sure that data is protected against attacks while sitting in the cloud storage.

Step 4 – Decrypt: Data/information is decrypted by the registered user using the shared master key only known to the receiver and the healthcare institution to access and read the patient's record. Registration and Login phases are executed in this step to validate that the user logging in is registered. Step 5 – Healthcare: The assigned doctor reads the patient’s data and provides the necessary prescription which is transferred using the same process. Data gets encrypted and the information is saved in the cloud storage while waiting to be transferred to the sensor node by the system administrator. Information is accessible using the master key that is only known to the receiver.

# The Developed User-Based Authentication and DoS Mitigation Algorithm

The five phases are carried out, where all of them are executed one after another to ensure that patient's sensitive data is protected, and their privacy is maintained. If the response received from the server was negative the session was denied, and the user was requested to retry to enter the correct login details and register first where the user details are not found within the system. Below is the proposed User-Based authentication and DoS mitigation algorithm designed by integrating ECC and RC4 in order to minimize the security issues in WBSNs.

**User-Based Authentication algorithm**

Initialization phase:

1. Choose and Generate

Registration phase:

1. Choose , .
2. Compute || ||
3. through secure channel

Authentication phase:

Step 1

1. sends the
2. sends public key
3. For each authentication do
4. Generate

Step 2:

Forward (

1. Identity =

Step 3:

1. Generate and
2. Compute =

Step 4:

1. Check if are present in the database
2. Validate
3. Sensor validation ;;

DoS mitigation phase:

1. Read all
2. Matches the
3. = Enc (+) compute
4. If
5. Power is more/equals to SN power
6. Send packets
7. Else
8. Drop packets

Encryption phase:

1. Verify if is received
2. For to
4. Data is encrypted resulting in
5. Computed

Decryption phase

1. Extractfrom value
2. = j
3. Extractfrom value
4. Decrypt
5. Checks
6. END

User-Based authentication and Denial of Service Mitigation scheme ensures that there is a low computation cost, hence, the algorithm is more efficient and faster when transmitting data in the WBSNs.

# The Proposed Algorithm Implementation

The implementation of a User-Based authentication and DoS mitigation algorithm is presented in this Section. The algorithm is implemented using the IEEE 802.11s model developed using MATLAB version 2020a on the computing platform, a machine running Windows 10 with 8GB memory was used. 100 sensor nodes were randomly arranged with a radius of 20, and the nodes are randomly distributed and clustered. The connection radius is 1 unit, and the minimum distance between nodes is set to 0.6 cm because setting mesh routers closer to each other is not common in the real-world.

MATLAB was chosen in this paper because of its high-performance language for technical computing [21]. MATLAB is written in C language, and it supports the cross-platform operating system [22]. In addition, MATLAB provides various command-line functions as well as tools for measuring, analysis, and visualization of data like digital filtering, signal processing, and modulation of signaling. MATLAB and Simulink are integrated together, which allows the researchers to amend the functions in the control system toolbox, and Simulink [23]. The simulator is also useful when generating waveforms over wide range of signals and building to-test systems. MATLAB provides several applications to scientists, engineers, researchers, and educators for technical computing as shown in Fig. 3.

# 

Fig 3: MATLAB simulator interface

# Simulation Set-up

The main purpose of simulating the User-Based authentication and DoS mitigation algorithm was to evaluate if the proposed algorithm brings improvement in the WBSNs applications. MATLAB is a very high-performance simulation tool, the latest version currently available for download is MATLAB 2021a. The configured simulation topology in MATLAB is shown in Fig. 4.

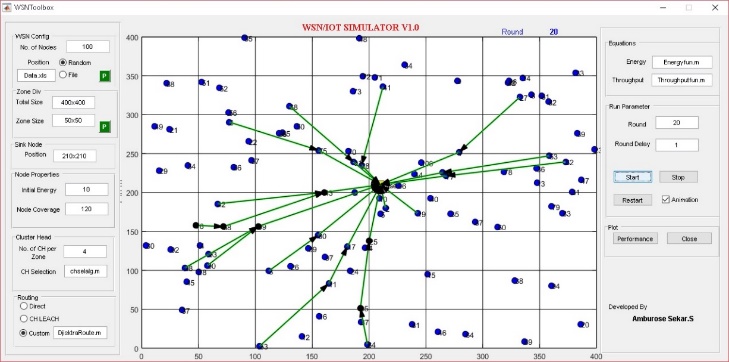


Fig 4: The configuration Parameters

The researchers in this paper chose to use the IEEE 802.11s protocol mainly because it allows the user to model communication between multiple Wireless Local Area Network (WLAN) nodes, allowing devices to interconnect to create wireless networks. MATLAB Simulink communication block set was used to build a complete WBSN system. The simulation procedure includes building the hardware architecture of the transmitting nodes, modeling both the communication channel and the receiving master node architecture. IEEE 802.11s protocol was used because it brings interworking and security by defining the secure password-based authentication and key establishment protocol.

# Simulation Results and Analyses

A simulation is beneficial as it allows the user to observe the efficiency of the proposed algorithm before implementing it in a real network environment. A network simulator allows researchers to review the performance of the proposed algorithm under various network conditions. The simulator can be modified to archive better results for the required analysis. This section presents and analyses the outcome of the used simulation to evaluate the effectiveness of the User-Based authentication and DoS mitigation algorithm from a variety of network configurations. Xgraph is used to present the evaluated MATLAB simulation results. Xgraph is used to input data stored in the data cell array with the individual simulation objects. Simulation results were obtained from 10 simulations.

# Experimental Evaluation

To measure the effectiveness of User-Based authentication and DoS mitigation algorithm, experiments were provided. The MATLAB simulation version R2020a was used, 100 random nodes were deployed which can run 10 or more rounds in the IEEE 802.11s protocol and each simulation was performed for the 60s to get stable output statistics. The minimum distance between nodes is 0.6 cm. The approach uses the IEEE 802.11s protocol for allowing the communication between multiple wireless networks between nodes. RC4 encryption was used for the encryption/decryption process, where different length keys known to a receiver were used.. In the real-world routers are usually placed closer together, thus nodes were randomly distributed and clustered in this paper.

# Simulation Results

A simulation scenario was applied to perform the simulations as explained in Section 4 to monitor the performance of the User-Based authentication and DoS mitigation algorithm with Cryptography-based techniques and a Biometric-based authentication algorithm. The simulation results presented in this paper have been gathered from an average of 10 simulations. The performance metrics analyzed in the simulations focus on the below parameters:

1. Network throughput: is the rate at which several bits are transferred across communication channels. It measures how fast data is transferred from the source to the destination.
2. Number of packet loss: Occurs when one or more packets of data responsible for transmitting data are failing to reach their destination.
3. Encryption/Decryption time: The encryption parameter measures the time taken when executing the encryption process, where an algorithm that takes less encryption time is considered efficient. Decryption is responsible for the amount of time the algorithm takes to decrypt the key.

This paper compared the performance of the proposed algorithm with Cryptography-based and Biometric-based techniques based on user authentication.

The biometric authentication algorithm was chosen because it provides a digital identity that is stored on network storage. Therefore, the process generates some time costs and consumes computational resources. In many cases, identification algorithms based on interactive proof are applied to authentication. The digital identity must be encrypted before sending, and the secret keys must also be distributed.

Cryptographic techniques are compared with the proposed algorithm because this technique uses a combination of asymmetric and symmetric cryptography when both parties have to agree on a secret key. After that, each message is encrypted with that same key, transmitted, and decrypted with the same key. However, Secure key distribution is the biggest problem when using symmetric cryptography. This paper compared the proposed User-Based authentication and DoS mitigation algorithm with the Cryptographic techniques because both utilize keys to encrypt/decrypt messages. However, the proposed algorithm considered the authentication of the user by integrating ECC and RC4 in order to ensure that encryption/decryption is faster so that the network is not attacked while sending data through the transmission channel.

1. Effects of Network Throughput

The effects of the network throughput capacity limitations on the performance of the three algorithms are presented as shown in Fig. 5. The performance of the three algorithms was analyzed when the gateway throughput capacity limitation differs from 2 to 18 while the delay limitation is set at 10 and the relay load constraint is relaxed.

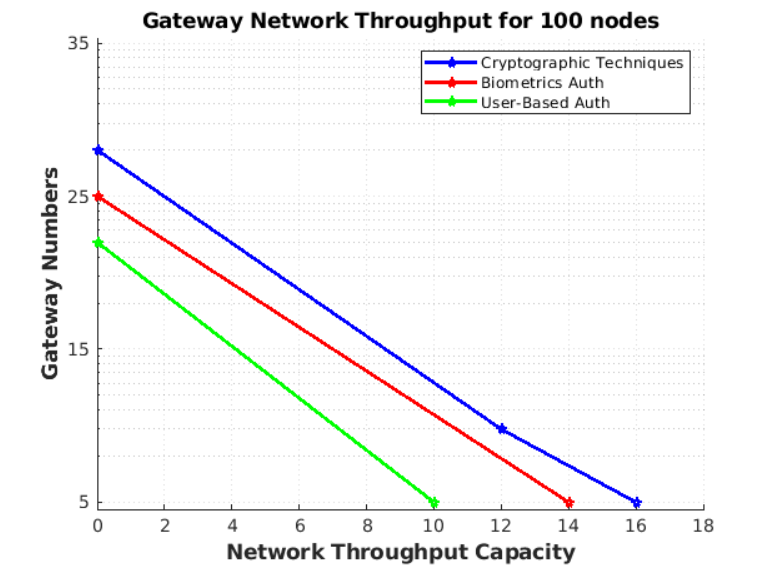


Fig 5: Comparison of the impacts of the gateway constraint on the performance of the three algorithms

The average network throughput for the three algorithms was monitored and compared under various network capacities being the volume of data sent, received, and speed at which data is transferred during the user authentication process. Biometrics authentication algorithm and Cryptographic techniques scheme are close to each other and achieved a higher gateway convergence as compared to User-Based authentication and DoS mitigation algorithm.

1. Number of packets lost

The parameter measures the probability of packet loss in the communication network. In this case, the program has a sufficient duration of 50 seconds. The program transfers 20 packets, this allowed the researcher to monitor and gather information about the number of packets lost, sent, and received during the authentication process.

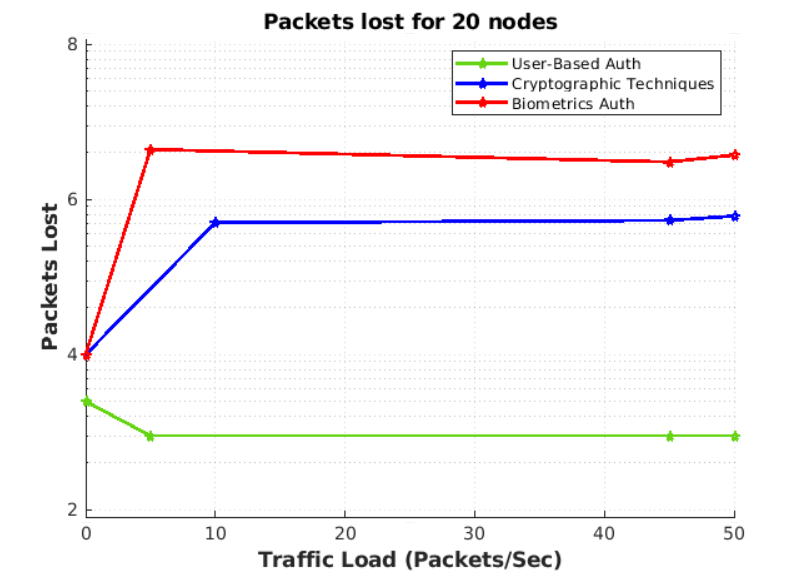


Fig 6: Average packet lost during the authentication process.

Simulation is repeated 10 times to obtain the average probability of packet loss for more accurate results. The proposed algorithm produced 30% at the time interval of 50 seconds where only 2.5% of packets were lost. The proposed algorithm outperforms both the Biometric authentication algorithm and Cryptographic techniques because the algorithm uses ECC which is known to be fast, having a benefit in processing time because of its smaller keys. Hence reducing the number of packet losses. While the other two algorithms produced 40% at the time of 50 intervals where more than 50% of packets were lost.

1. Effects of Encryption/Decryption Time

This parameter computes the time required for the execution of the User-Based authentication and DoS mitigation algorithm for encryption and decryption. The algorithm that takes less encryption and decryption time is considered efficient. The User-Based authentication and DoS mitigation algorithm was evaluated with different password lengths. When the password length was 10 bytes, the User-Based authentication and DoS mitigation algorithm took 160 ns to encrypt as shown in Fig. 7.

Using different lengths of the user password during the authentication process is done to get the amount of time it takes for each password to encrypt if the key is known to a receiver. User-Based authentication and DoS mitigation algorithm take less time to encrypt as compared to Cryptographic Techniques and Biometrics authentication algorithm. Cryptographic Techniques and Biometrics authentication algorithms took a long to encrypt data. When the password length was 10 bytes, the Cryptographic Techniques scheme took 220ns to encrypt data. When the password length was 10 bytes, Biometric Authentication took 250ns to encrypt data.

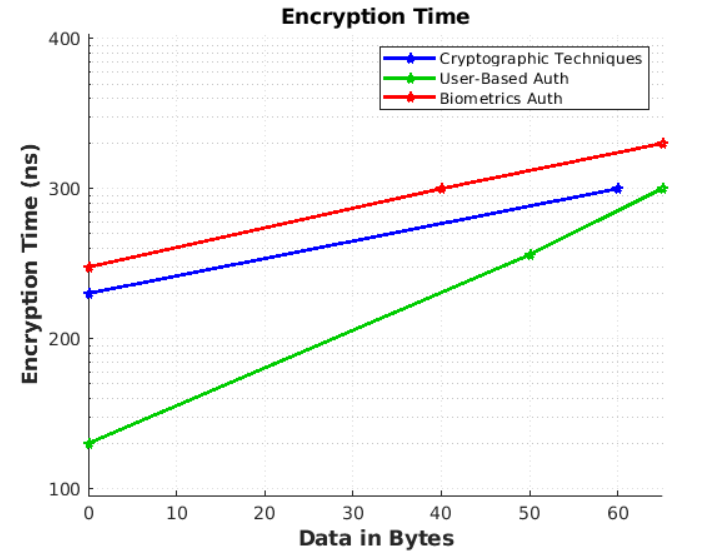


Fig 7: Encryption time versus byte of data

The decryption parameter calculates the time required to convert the received ciphertext to plaintext. The same process performed for encryption was followed where a User-Based authentication and DoS mitigation algorithm was evaluated using different password lengths to analyze the time it takes for each data to decrypt if the key is known to the receiver. Multiple data lengths versus the amount of time it takes to decrypt are shown in Fig. 8. Biometric authentication and Cryptograph techniques took more time to decrypt the data as compared to the User-Based authentication and DoS mitigation algorithm.

The encryption and decryption time of the three algorithms is shown in Fig. 7 and Fig. 8. The results were calculated based on the amount of data versus the number of bytes, which is the volume of data/ that went through the process and how long it took the algorithm to encrypt/decrypt the text. User-Based authentication and DoS mitigation alSgorithm provide data security with less encryption and decryption time. While the Biometric authentication and Cryptographic techniques took more time to decrypt the data provided as compared to the User-Based authentication and DoS mitigation algorithm.

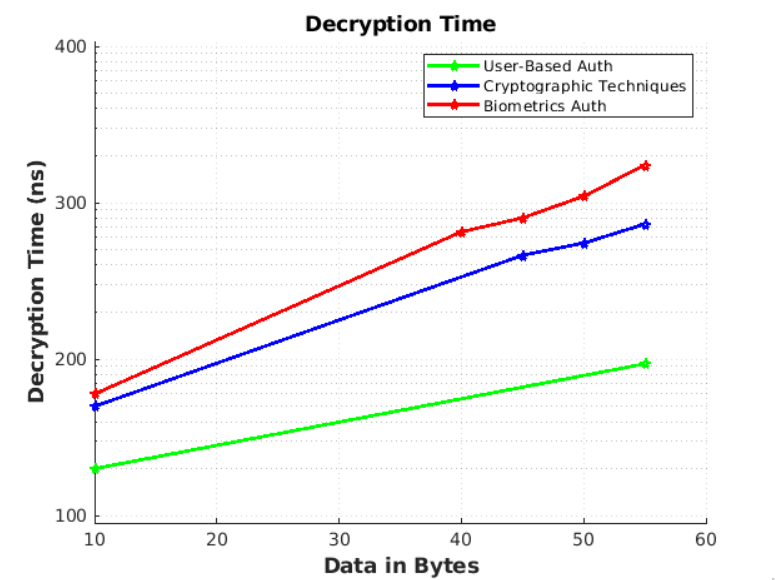


Fig 8: Decryption time versus byte of data.

# Conclusion

This paper presented the design of the User-Based authentication and DoS mitigation algorithm integrating ECC and RC4 in order to improve security in WBSNs. The effectiveness of the proposed User-Based authentication and DoS mitigation algorithm in WBSNs was evaluated against the Biometric authentication algorithm and Cryptographic techniques. The analyzed results were presented based on the following network parameters namely network throughput, packet loss, encryption, and decryption time. According to the presented simulation results, the proposed algorithm outperformed both the Biometric authentication algorithm and Cryptographic techniques in all mentioned network parameters.

In this paper, it is assumed that the computation time is not maintained during the user authentication process as the focus was on mitigating DoS attacks. Therefore, in the future, the computation time which includes key generation speed can be investigated to ensure that the security of WBSNs is maintained in all aspects, and evaluating the performance of the User-Based Authentication and DoS mitigation algorithm in more complex network systems can be investigated.

# Acknowledgment

The authors would like to thank the Tshwane University of Technology for financial support. The authors declare that there is no conflict of interest regarding the publication of this paper.

# References

* 1. PENG, Y., WANG, X., GUO, L., WANG, Y. & DENG, Q. 2017. An Efficient Network Coding-Based Fault-Tolerant Mechanism in WBAN for Smart Healthcare Monitoring Systems.
  2. [2] NAYYAR, A. & SINGH, R. 2015. A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs).
  3. ZHANG, Z., WANG, H., VASILAKOS, A. & FANG, H. 2013. Channel information-based cryptography and authentication in wireless body area networks, in Proc. 8th Int. Conf. Body Area Network. (BodyNet).
  4. DAS, A., CHATTERJEE, S. & SING, J. 2015. A new biometric- based remote user authentication scheme in hierarchical wireless body area sensor networks.
  5. WANG, C. & ZHANG, Y. 2015. New authentication scheme for wireless body area networks using the bilinear pairing.
  6. ZHOU, P., JIANG, S., IRISSAPPANE, A., ZHANG, J., ZHOU, J. & TE, J. 2015. Toward energy-efficient trust system through watchdog optimization for WSNs.
  7. GOVINDASAMY, J. & PUNNIAKODI, S. 2018. Optimized watchdog system for detection of DDOS and wormhole attacks in IEEE802.15.4-based wireless sensor networks.
  8. CHIOU, S., YING, Z. & LIU, J. 2016. Improvement of a privacy authentication scheme based on cloud for medical environment.
  9. LI, C., LEE, C. & WENG, L. 2016. A secure cloud-assisted wireless body area network in the mobile emergency medical care system
  10. WU, F., XU, L., KUMARI, S. & LI, X. 2018. An improved and provably secure three-factor user authentication scheme for wireless sensor networks.
  11. MO, J. & CHEN, H. 2019. Lightweight secure user authentication and key agreement protocol for wireless sensor networks. Secure Communication Network.
  12. WU, F., XU, L., KUMARI, S. & LI, X. 2018. An improved and provably secure three-factor user authentication scheme for wireless sensor networks.
  13. KOYA, A. & DEEPTHI, P. 2018. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network.
  14. WANG, S. & PARK, J. 2010. Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model.
  15. XU, X., ZHU, P., WEN, Q., JIN, Z., ZHANG, H. & HE, L. 2013. A secure and efficient authentication and key agreement scheme based on ECC for the telecare medicine information system.
  16. ISLAM, S. & KHAN, M. 2014. Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems.
  17. GOPE, P. & HWANG, T. 2016. An efficient mutual authentication and key agreement.
  18. ROY, S. & KHATWANI, C. 2017.Cryptanalysis and Improvement of ECC-Based Authentication and Key Exchanging Protocols.
  19. MNIF, A., CHEIKHROUHOU, O. & JEMAA, M. 2011.An id- based user authentication scheme for wireless sensor networks
  20. CHIOU, S., YING, Z. & LIU, J. 2016. Improvement of a privacy authentication scheme based on cloud for medical environment.
  21. ALI, I., ABDULMAOWJOD, A. & MOHAMMED, H. 2019. Simulation & Performance study of wireless sensor network (WSN) using MATLAB.
  22. SINGH, A. & JAIN, A. 2017. A Survey on Wireless Network Simulators. Bulletin of Electrical Engineering and Informatics.
  23. XIE, D., LI, J. & GAO, H. 2020. Comparison and Analysis of Simulation methods for TSN Performance IOP Conf.