International Journal of Electronic Devices and Networking

E-ISSN: 2708-4485
P-ISSN: 2708-4477
IJEDN 2022; 3(1): 139-145

www.electronicnetjournal.com
Received: 23-01-2022
Accepted: 26-03-2022

Fares
SRM Madurai College for Engineering and Technology, Madurai, Tamil Nadu, India

Goswami
SRM Madurai College for Engineering and Technology, Madurai, Tamil Nadu, India

Correspondence
Fares
SRM Madurai College for Engineering and Technology, Madurai, Tamil Nadu, India

PUF for device authentication in multi-hop body area networks

Fares and Goswami

DOI: https://doi.org/10.22271/27084477.2022.v3.i1a.57

Abstract
Wireless sensor technology has several applications in the military, the medical field, and the corporate world. A Wireless Body Area Network (WBAN) is a novel use of wireless sensor networks in the area of human health monitoring; it enables individuals to keep track of their personal vitals in real time and respond appropriately in the event of an emergency. Access to reliable data, as provided by nodes in WBAN, is crucial for providing successful patient care. We solved the problem of unreliable data in this study by assigning trustworthiness ratings to each sensor node. In this research, we employ a physically burning anthracite or bituminous coal function (PUF) as a hardware-centric security factor for cloud-based lightweight identification in multi-hop oriented WBAN. In this setup, the cloud is the TTP that records all sensors. The sensor node and the CR pair are uploaded to the cloud, where the washbasin validates them. The authentication time for nodes was cut down by using a hierarchical system. Hence, the cloud server has a hierarchical system for storing credentials for nodes. There was a considerable improvement over the baseline system in terms of the ratio of packets delivered, packet arrival quality, packet delivery latency, and the quality of the intermediate hops in our proposed system.

Keywords: Hierarchical based authentication, device security provisioning, PUF, and multi-hop body area network

Introduction
When it comes to the human body, the wireless body area network (WBAN) is used for monitoring and diagnosis purposes [1, 2]. Sensing devices & wearable devices make up WBAN, and they are continually collecting data and transmitting it to a coordinator (Healthcare professionals including physicians, nurses, pharmacists, and EMS workers) through a gateway. Smartphones and other devices/controllers are used to gather sensor data. WBAN considers energy efficiency to be a key priority. The sensors themselves use very little power, but there is a cost associated with sending the data. In the past, people have tried to address the issue of energy scarcity by creating more efficient processes. Also, QoS affects how often retransmissions are required. There may be a wide range of QoS requirements for different kinds of traffic (emergency and non-emergency). It is challenging to deliver varying quality of service (QoS) standards in WBAN due to the limited resources of sensors and the unreliable communication between them. Several potential causes of these problems are discussed below (1). Single-hop, long-distance communication (2). When networks employ (3) multi-hop communication without first checking relay conditions, they are vulnerable to attacks in which rogue packets are broadcast throughout the network. Several solutions to this kind of issue are listed below (1). Sensors of the same kind and function may be grouped together for easier management (2). The optimal method of instantaneous data transmission (3). MAC scheduling with such a periodic on/off period. These strategies were developed with energy efficiency in mind [3-5].
The physical layer of WBANs is increasingly under attack. Current literature suffers from a single weak spot that lengthens the delivery of security and thus increases the rate at which energy is used during data transfer [6-8, 18].
Security is another choice that takes into consideration both rising energy use and individual privacy. While cryptographic methods that allow for lightweight computations have received a lot of attention in recent decades, these schemes still have significant shortcomings in terms of security, privacy, integrity, & secrecy [19, 20]. This means that an attacker's

techniques may change over time and that they may get access to any data stored on a web computer in a matter of minutes. More and more people are turning to blockchain, a distributed ledger that guarantees complete confidentiality and immutable results. Moreover, the traditional blockchain design does not facilitate scalability, energy efficiency, etc. The fundamental objective of the study is to enhance the safety and efficiency of data transmission. The goal is to significantly reduce authentication time by considering key authentication criteria while placing as little strain as possible on established health authorities [9, 10].

Literature Review

Authors proposed a healthcare system based on wearable devices for off-site monitoring. A smartphone was used at the patient side to receive the information from the body implanted and wearable devices [21-23]. This paper proposed a recommendation system that sends alerts for the people when it detects any abnormal behavior. For achieving accurate recommendation, machine learning algorithm (Naïve Bayes and Neural Networks) was used which analyzes reports from various hospitals and healthcare institutions to diagnose the exact health alarms. Finally, the performance of neural networks shows better performance compared to naïve Bayes. Just patient alarms were produced in this work, with no recommendations for the best alarms to use. The only data used by machine learning comes from sensors and other devices. Unfortunately, patients are also impacted by their surroundings, and this article does not provide reliable alarm prediction or transmission. This paper's authors developed a Secure Authentication Method for WBAN in Hospital IoT that makes use of Lightweight Hash Chains. The network model encompasses [11, 12] the following three entities: (1). Sensors, (2). (2). Centralized hubs and (c). Medical Personnel (users). Although gateways are equipped with enough processing power to serve as a trustworthy communication entity, sensor nodes are responsible for sensing and collecting data about the human body. This organization provides a safe connection between sensors and medical professionals. This article discusses many security assaults, including insider attacks, user tracking attacks, offline guessing attacks, session key disclosure attacks, impersonation attacks, and forgery attacks, to ensure that unauthorized users cannot access any data, sensitive or otherwise. In this research, we present a lightweight and secure key exchange and authentication mechanism for the medical IoT [13]. There's a name for it: LAKS-NVT. Using the Burrows-Abadi-Needham (BAN) logic, a real-or-random (ROR) model was developed to guarantee the safety of the session key and to provide secure mutual authentication. Users or sensor ID, password, and secret key were all examples of security credentials that may be used for checking in and proving identities. As a result, LAKS-NVT protects individual privacy in realistic medical IoT settings. Weak ID, password, and secret key security credentials weaken the effectiveness of network security. Key agreement and authentication mechanisms were accomplished via the deployment of a cloud-assisted light individual depends anonymous protocol in this study. Both user anonymity and mutual authentication were handled in this cloud-assisted WBAN solution. Diffie-Hellman and the Random Oracle Model, two well-known computational works, were employed for security assessments. Authentication process, client privacy, session key safety, unlink ability, perfect forwards secrecy, stolen validator attack, account hijacking, and man-in-the-middle attack were all attained by the security study. Authentication often has a significant computational complexity. It takes a significant amount of power to authenticate sensor nodes. In this work, we introduce the lightweight authentication methodology in WBAN. In general, WBAN receptors sense very sensitive information relating to human health. So, a secret plan was necessary for sending these medical files [14]. Data encryption as well as decryption using attributes was offered as a solution to this problem. At first, a patient's data was registered with a unique identification, and a secret key was generated by the healthcare authority (HA) and sent through encrypted means. The cloud provider creates an access policy for the users of the data, and the owners of the data review and approve it. To counter resynchronization attacks in WBAN, a privacy-preserving authentication mechanism is provided here. The forward secrecy and resistance to resynchronization assaults of this system are the result of the usage of the pseudonym identification approach, the serial number method, and the one-way hash chain techniques. BAN logic & ProVeri schemes provided authentication process and security verification [15].

Proposed Model

To facilitate efficient communication between the sensors in WBAN, we have built a PUF system as part of this study.

The first step in building a WBAN is to install n sensors. We began by verifying the legitimacy of each sensor using the authenticator. The node count is determined by the total number of WBANs registered for a certain area. This decreases the required time for authentication and the burden on the authenticator. Biological PUF provides compelling evidence of improved performance over Si & SRAM PUF. Node-based sensing and session ID generation begin when authentication is complete with the authenticator. After verification of session ID only, sensed information from the sensor is accepted. Otherwise, it’s discarded. Our proposed system proved to provide increased communication with reduced loss of packet. Some of the drawbacks present in the existing systems are,

- Did not consider the blockage during relay selection
- Low security strength

Advantages of our proposed system

- Increased Packet delivery ratio and quality
- Reduced Packet delivery delay
- Minimized intruder effect

WBAN Architecture: The installation of sensor nodes is the first stage in developing a WBAN. All of the sensors are split into two groups, one nearer to the sink nodes as well as another farther away, using hierarchical authentication. The nodes closest to the sinks are called "inlayer," while the others are "out layer. "It is assumed that the green vertices in Figure 1 are a component of the system, whereas the remaining nodes are outside it.

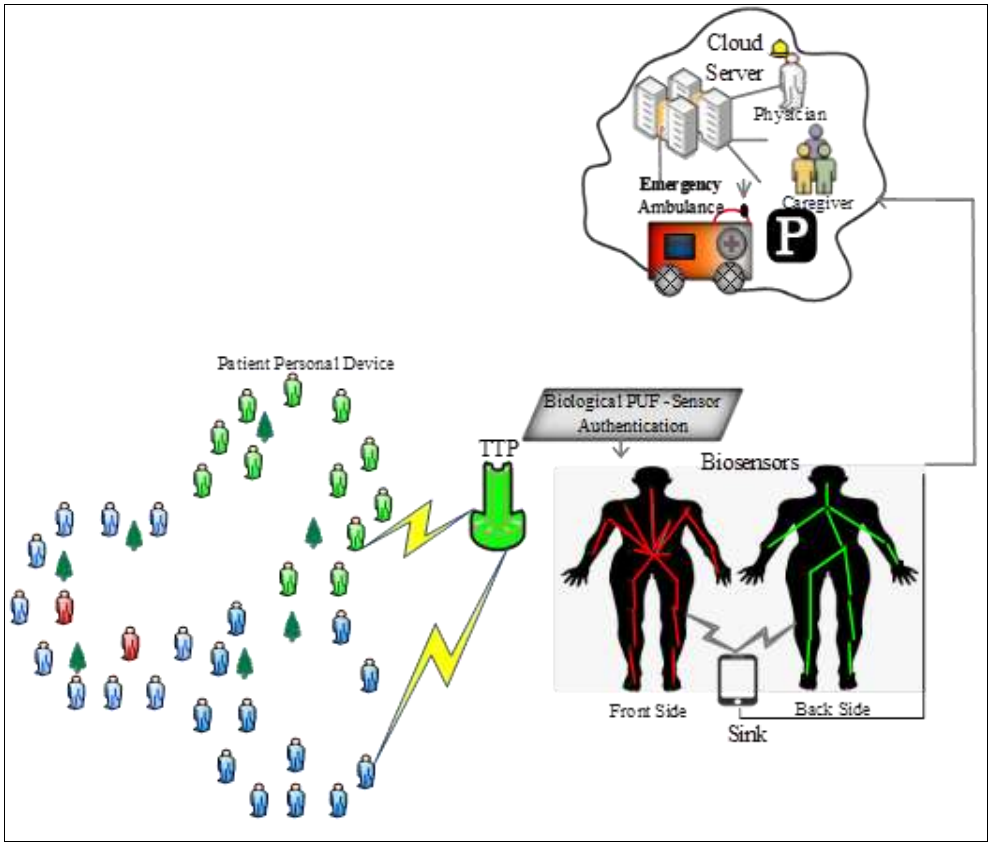

Fig 1: Proposed Architecture

There must be two distinct authentication processes for these two types of nodes. According to the concept of trust, if a sink node is authenticated by an inlayer node, the sink node is obligated to trust the inlayer sensor node. The outer node will trust the topology of the network if it has evidence that an inlayer node is reliable, and the sink node will be expected to share that confidence. After the n number of packets classification, the sensor nodes in the WBAN is classified by any one of the follows,

- **Legitimate device:** The legitimate devices / users are the entities that are registered properly with the reputed administrator authority. Such devices are also subjected to critical issues as stealing of security parameter and modification of data by intermediate attackers in the channel.
- **Unauthenticated device:** These devices are the entities which are not registered in the administrator database. These types of device purposely enter into the system for crashing the servers with unnecessary authentication request and also it tries to extract data from other devices.
- **Compromised device:** The compromised devices are the legitimate devices that are affected by attackers who compromise a device and make it to participate in the system. Hereby the attackers gather information from such compromised devices. The devices can be compromised for various reasons either for the intention of destroying the network of selfishness.

Security Metrics

Security is becoming a major requirement and also it is being a significant part in any type of application. The authentication is carried over between server and the client. Server is responsible to authenticate the credentials of particular user. ID, Password, and PUF are considered as the initial security metrics in WBAN for security improvement. In this phase the sensor node and TTP communicates with each other by establishing a link between them. A challenge will be sent by the TTP to the PUF for ensuring the device is legitimate. On receiving the challenge from TTP, then the PUF replies with the corresponding response. In this way all the challenges are response by the PUF. The server stores all the pairs of challenge and response which used while authenticating the sensor node.

PUF based Authentication

Using a one-to-many authentication approach, both the outside sensed data and the inner sensor node are authenticated using a common key across the nodes. To verify identity, two parties exchange their shared keys and check if they are the same. Distributing the shared-key may be done using key pre-allocation. It has already been mentioned, however, that doing so would increase expenditures. It's also possible for attackers to easily obtain all the keys using modelled attacks after the stable key pool has been built. If a node's authenticating connection is compromised after all the credentials have been taken, the node is worthless. Hence, PUF is in charge of establishing trust between the two sensor nodes. Firstly, enroll phase is conducted using the above metrics. Next after enrollment of each sensor in WBAN, they are ready for data transmission with authentication. The authentication is completed successful only after verifying the entire security credentials one after the other. A need for PUF,

- Prediction of threat into the system is easier
- Improve the level of security
- Enable access only for legitimate users
- Eliminate participation of illegitimate users

- Avoid stealing of security credentials.
- Performance Evaluation

In conclusion, we focus on three useful characteristics of PUFs:

- Several instances may be distinguished from one another by their unique responses to the same challenge;
- Consistently identifying a single instance based on its responses to a single challenge constitutes reliability;
- It is impossible to (1) physically replicate the CRPs of one instance using those of another instance, or (2) infer the CRPs from knowledge of the manufacturing process of a device or from previously released CRPs.

Let $P \in \mathbb{P}$ be a PUF instance P from the collection of all PUF examples P of some PUF type. R seems to be a random process representing the outcome $\mathrm{R}: \mathbb{S}_P \to \{0,1\}^N$ a system for mapping between the physical states $\mathbb{S}_P$ between the sets among all binary representation of length N and the PUF instance P, indicated $\{0,1\}^N$. In specifically, the answer is conditional on a user's current status $S_{P,C} \in \mathbb{S}_P$ of the PUF instance P brought on by the test $\mathrm{C} \in \{0,1\}^N$

We can determine the reliability and freshness of P through analysing the dispersion of R for various combinations of P and C. By contrasting how several examples handle the same issue, we may gauge how well our notion performs as a PUF.

The Hamming distance measures how dissimilar two discrete strings are to one another:

$$D(\mathrm{A},\mathrm{B}) = \sum_{i=1}^{N} \mathrm{A(i)} \oplus \mathrm{B(i)} \quad (1)$$

Where A & B are indeed the two discrete strings being compared, and their lengths are $N, \mathrm{A(i)}$ and $\mathrm{B(i)}$ correspond to the i'th byte in both A and B, $\oplus$ means XOR, a logical operation. The average Hamming distance for random strings is N2. Normalizing its Hamming distance by might also be helpful $N: d(\mathrm{A},\mathrm{B}) = D(\mathrm{A},\mathrm{B})/N$. For random strings A and $\mathrm{B}, d(\mathrm{A},\mathrm{B}) = 1/2$. Here we'll compare two answers to the same set of problems C_c. The same PUF instance may provide these results when subjected to the same challenge string (Indexed by p) on two separate occasions (indexed by r for repetition), $\mathrm{R}_c^{p,r}$ and $\mathrm{R}_c^{p,r'}$, They may also arise by repeating the task on two distinct PUF instances, $\mathrm{R}_c^{p,r}$ and $\mathrm{R}_c^{p',r}$. Reliability may be tested by iterative usage; ideally, two instances of PUF would have identical answers to the same task (i.e., $d\left(\mathrm{R}_i^{p,r}, \mathrm{R}_i^{p,r'}\right) = 0$ for all p, r, and r'). Two PUF instances should respond to the identical challenge in ways that look random and uncorrelated when compared. This is how uniqueness is measured. With respect to Hamming distances, $d\left(\mathrm{R}_i^{p,r}, \mathrm{R}_i^{p',r}\right) \approx 1/2$ (nevertheless, this does not account for bit-level correlations).

We provide a concise summary of these measures:

- $c \in [0, N_{\text{challenges}})$: Distinct challenge;
- $r, r' \in [0, N_{\text{repeats}})$: Different situations call for different solutions;
- $p, p' \in [0, N_{\text{chips}})$: Keep PUF instances apart.
- Assuming that each answer is a string of N bits, the proportion of different bits between them is denoted as

$$\begin{aligned} \mathfrak{R}(c,p,r,r') &= d\left(\mathrm{R}_c^{p,r}, \mathrm{R}_c^{p,r'}\right), \\ \mathfrak{U}(c,p,p',r) &= d\left(\mathrm{R}_c^{p,r}, \mathrm{R}_c^{p',r}\right). \end{aligned} \quad (2)$$

Above, $\mathfrak{R}$ (mnemonic 'reliability') intra-device fractional analysis The hamming distance among r and s apps' answers to a particular PUF instance p and r' of challenge c. Likewise, $\mathfrak{U}$ (mnemonic 'uniqueness') Does the fraction between devices exist? When comparing two answers from PUF instance p and q, the p' as a direct outcome of applying the constant r to the difficult c.

We first aggregate over paired combinations used to create these distances to get distributions for each challenge, and then we aggregate over the leftover indices to provide mean measures of dependability μ_{intra} and individuality μ_{inter}. Specifically, if we let $\langle\cdot\rangle_{a,b}$ if you want to show the median value of anything between a and b, then

$$\begin{aligned} v(c) &= \langle \mathfrak{R}(c,p,r,r') \rangle_{r,r^r,p}, \\ u(c) &= \langle \mathfrak{U}(c,p,p',r) \rangle_{p,p',r}. \end{aligned} \quad (3)$$

Thus that the aforementioned measurements are always available, we keep track of the network's progress throughout time using a series of N-bit strings. Taking a per-chip reliability measurement is as easy as not averaging over p in (8)

In the proposed authentication method, the authenticator is the one responsible for decrypting the relevant data, passing it along to the initiator, and selecting a MidNum. After that, we encrypt the MidNum using a bijective function and transmit it to the initiator. This number is XORed with the decrypted response generated by the initiator to determine the Result. The Outcome must be encrypted using a bijective function before being sent to the authenticator. After receiving the message, the authenticator will XOR the Result to create its own Answer. After performing the XOR, the outcome is compared to a MidNum to verify its legitimacy. Even if an attacker has both the encryption MidNum and the encryption Result before reaching the authenticator, the resultant XOR value will not be the shared-key. Let's suppose an attacker manages to get their hands on the authentication data being transferred between nodes. In this scenario, an adversary may more easily gain trust by pretending to be a reliable node provided the information it transmits always conforms to the same standards. None the less, because of MidNum number is random, it is possible to effectively address this concern. Even if an opponent may extract an encrypted MidNum from authenticator and the data supplied by the authentic MidNum and Responder, a sharable among two sensor nodes remains unobtainium. A MidNum results and the information provided to a authenticator must be gathered at the same time for the shared-key to be generated. The initiator may judge the validity of the authenticator by

comparing a randomly generated Rand A, as well as the authenticator can validate the sensor node's identity by matching the MidNum. As this is the case, reciprocal authentication between sensor nodes is initiated by the external authentication system. Therefore, careful monitoring of the consecutive authentication frequency of the sensor nodes is essential. If there have been more than three unsuccessful authentication attempts, there may have been an intrusion into the network and it should be investigated. Changing a authentication interval counter will enable this function. Lightweight and secure sensor node authentication is made possible by using an outer layer.
Finally, the security and privacy performance analysis is conducted to show the improvement by using PUF based WBAN.

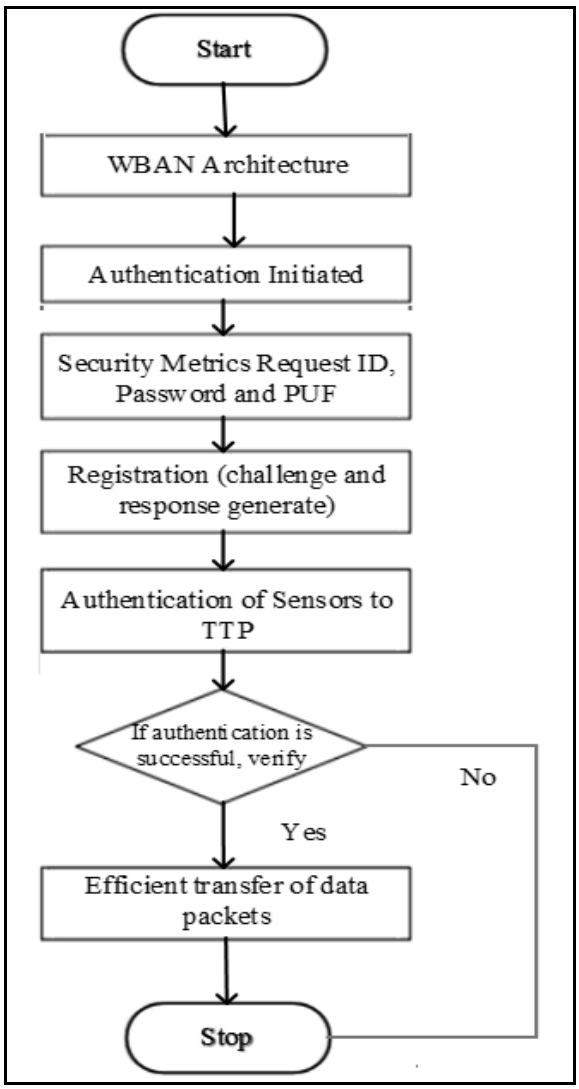

Fig 2: Dataflow diagram

Experimental results
Three of the most well-known wireless network simulators are NS2, OPNET, &OMNET++, all of which may be used to simulate sensor networks. Although NS2 has broad support in the academic world, OPNET is a for-profit communications-system simulation environment, while OMNET++ is extensively utilised across the academic and industry worlds for discrete-event modelling. The node definition tools in OMNET++ are powerful, and the program's interface is intuitive. Hence, it served as a pilot study for these conclusions. Outer nodes, inner nodes, and sink nodes are each defined in their own corresponding NED file inside the OMNET++ topological description. A file titled WBAN. ned contains detailed information on the whole network. When these variables are adjusted, the.cc file will utilise the parameters defined in the.h file while loading and processing.

Throughput: An Analysis
It's the most used metric for tracking enhancements to packet transport in networks. A communication channel's throughput is the max speed at which a specified quantity of packets can be transmitted to a specified destination during a specified period. Another way to put it is,

$$Throughput = \frac{\sum No.of\ packets\ received\ suuccessfully}{Unit\ time} \quad (4)$$

Throughput is the actual amount of data sent over a network connection in a given time period, whereas bandwidth is the highest limit of information that can be transmitted over a network channel. This metric is often expressed in bits per second, which may also be thought of as data packets per second. If this metric is high, the network is functioning very well; otherwise, it is underachieving. Communication channel constraints, computing power, the availability of efficient routing mechanisms, and similar factors all influence this metric. One technique to increase network performance is to use more efficient transmission protocols.

Reason for Consideration
Throughput was selected as the performance metric because it provides insight into the efficiency of the routing protocol. Throughput refers to the pace at which information may be sent. If the routing works, more data will go where it needs to go. We have thus used this measure to evaluate the performance of the routing protocol we have suggested. But, without any malicious actions or selfish nodes, the network's throughput will likewise rise. More information will arrive securely at its destination if there are fewer malicious nodes in its path. As a result, throughput also provides the advantages of effective in-built network security measures. A routing algorithm's and a security system's efficacy may be measured by their throughput. A network's throughput, or the amount of data it can send in a given amount of time, may be used as an indicator of how well its routing and security procedures are functioning.
The gathered findings for the suggested PUF technique for throughput measure are shown in Table.6.1 and compared with the current multifactor approach. As can be seen in the table below, the suggested PUF algorithm improves with each iteration. Based on simulations conducted during a comparable time period, the PUF approach is shown to be superior than the multifactor methodology (which provides 2.6 packets/second) in terms of data throughput (three packets). The PUF approach improves the simulations as a whole, rather than being a hasty fix that may be reversed in two seconds.

Column 1: Comparison of Throughput

Simulation time (Sec)	Throughput(packets/sec)	
	Multifactor method	PUF algorithm
2	2.6	3
4	2.6	2.8
6	2.9	3
8	2.8	2.9
10	2.6	2.7
12	2.8	3
14	2.5	2.7
16	2.5	2.8
18	2.55	2.7

Column 2: Average Throughput Comparison

Metric	Technique	
	Multifactor method	PUF Procedure
Quantity (packets/10seconds)	26	28.44

An average speed of the multifactor method and the PUF algorithm are compared in Table.6.2. Our proposed PUF method can produce 28.44 packets/sec throughput, whereas the multifactor technique only yields 26 packets/sec. The multifactor approach's poor efficiency may be traced back to its lack of security (The author's exclusive emphasis on secure communication based on the trust factor). Our experiments highlight the value of including military-grade communication security in OSN-based software. Effective delivering service that provides reliable transmission and outstanding security is shown to be the key to achieving high throughput efficiency. PUF route with security nodes improves data transmission efficiency while decreasing vulnerability to cyber-attacks. A high throughput indicates that the routing protocol and security mechanism are functioning well. The network can now transfer more packets of data in the same time frame thanks to the PUF technique.

The results of the trials show that the disagreement continues to exist, despite efforts at communication. The main reason for this is because when more and more nodes join the network, the likelihood of collisions between them increases as they try to transmit data to the same channels at the same time. The sink node may become stuck in a perpetual state of conflict if the number of nodes grows too great.

Conclusion

In this study, we developed WBAN for authentication of sensor nodes to the trusted third party (TTP). Communication among sensors inside the human body is authenticated and trusted to ensure the communication is secure. Firstly, enrolment is conducted for all sensor nodes to the TTP by ID, password and PUF. In this research, we offer a lightweight authentication technique for multi-hop BANs based on PUFs with cloud support. By including the crossing RO PUF into the sensor node & storing sufficient CRPs of a inner node in the cloud, tree multi-hop networks alleviate the storage strain on a single node inside the body area network.

The suggested method outperforms existing methods in regards to packet delivery rate, packet delivery quality, hop count, and latency. Our proposed is very well suited for implementing in the WBAN secure scenarios since the security threat effect is greatly reduced. In future, we planned to enhance the security of the proposed system by large. So far, the node being selected as the relay node is not checked as malicious hacker or intruder by blockchain. This cause serious effects as the data of crucial information as video record of a crime scene and so on. Thus, we will ensure the credentials of the relay node and verify its accountability using lightweight cryptography algorithms.

References

1. Kumar M, Samundiswary P. Wireless body area network security issues-survey. In: Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT); Kuala Lumpur, Malaysia; c2016. p. 190–194.
2. Manukonda KR. Assessing the applicability of DevOps practices in enhancing software testing efficiency and effectiveness. Journal of Mathematical & Computer Applications; c2022.
3. Pang Z, Zhang J, Qiang Z, Gong S, Tang B. Crossover ring oscillator PUF. In: Proceedings of International Symposium on Quality Electronic Design; Santa Clara, CA, USA; c2017. p. 237-243.
4. Yenugula M, Kodam R, He D. Performance and load testing: Tools and challenges. International Journal of Engineering and Computer Science. 2019;1(1):57-62. DOI:10.33545/26633582.2019.v1.i1a.102.
5. Manukonda K. Efficient test case generation using combinatorial test design: Towards enhanced testing effectiveness and resource utilization. European Journal of Advances in Engineering and Technology. 2020;7(12):78-83.
6. Karlof C, Sastry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks. In: Proceedings of International Conference on Embedded Networked Sensor Systems; Hangzhou, China; c2004. p. 162.
7. Perrig A, Canetti R, Tygar JD, Song D. The TESLA broadcast authentication protocol. CryptoBytes. 2002;5(2):2-13.
8. Luk M, Mezzour G, Perrig A, Gligor V. MiniSec: A secure sensor network communication architecture. In: Proceedings of International Symposium on Information Processing in Sensor Networks; Berkeley, CA, USA; c2007. p. 479-488.
9. Almheiri SM, Alqamzi HS. Data link layer security protocols in wireless sensor networks: A survey. In:

Proceedings of IEEE International Conference on Networking; Xi'an, China; c2013. p. 312-317.
10. Yenugula M, Kodam R, He D. Multiple data centers intended for latency minimization using artificial intelligence algorithms. International Journal of Computer and Artificial Intelligence. 2020;1(1):39-45. doi:10.33545/27076571.2020.v1.i1a.79.
11. Zhao N, Ren A, Hu F, Zhang Z, Rehman MU, Zhu T, *et al*. Double threshold authentication using body area radio channel characteristics. IEEE Communications Letters. 2016;20(10):2099-2102.
12. Ma L, Yu G, Zhu Y. TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. Wireless Personal Communications. 2014;77(2):1077-1090.
13. Liu Y, Liu D, Yue G. A body Gauss-Markov-based mobility model for body area networks. Tsinghua Science and Technology. 2018;23(3):277-287.
14. Salama MH, Taha S, Elmahdy HN. PMAS: A proposed mutual authentication scheme for wireless body area networks. In: Proceedings of International Conference on Information and Communication Technology Convergence; Jeju Island, Korea; c2015. p. 636-641.
15. Yuan J, Lu S, Yu S, Ming L. Authenticated secret key extraction using channel characteristics for body area networks. In: Proceedings of ACM Conference on Computer and Communications Security; Toronto, Canada; c2012. p. 1028.
16. Zhang J, Qu G. Recent attacks and defenses on FPGA-based systems. ACM Transactions on Reconfigurable Technology and Systems (TRETS). 2019 Aug 21;12(3):1-24.
17. Kompara M, Islam SH, Hölbl M. A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. Computer Networks. 2019;148:196-213.
18. Pouraghily A, Wolf T. A lightweight payment verification protocol for blockchain transactions on IoT devices. In: 2019 International Conference on Computing, Networking and Communications (ICNC); c2019. p. 617-623.
19. Yenugula M. Examining partitioned caches performance in heterogeneous multi-core processors. International Journal of Communication and Information Technology. 2022;3(2):31-32. DOI:10.33545/2707661X.2022.v3.i2a.70.
20. Makhdoom I, Abolhasan M, Ni W. Blockchain for IoT: The challenges and a way forward. In: ICETE 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications; c2018.
21. Tan X, Zhang J, Zhang Y, Qin Z, Ding Y, Wang X. A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology. 2020;26(1):36-47.
22. Yenugula M. Optimizing load balancing for green cloud via efficient scheduling. International Journal of Advanced Academic Studies. 2022;4(3):224-230. DOI:10.33545/27068919.2022.v4.i3c.1125.
23. Singh DP. Forecasting of supermarket sales using big data analytics and machine learning techniques in business sector. International Journal of Core Engineering & Management. 2023;7(6):18-30.
24. Singh DP. An efficient system for customer relationship management on churn prediction using machine learning technique. International Journal of Core Engineering & Management. 2022;7(4):19-34.