SIGNATURE BASED KEY AUTHENTICATION PROTOCOL FOR WIRELESS BODY SENSOR NETWORKS

[1]M.AYYADURAI, [2]Dr.S.VARALAKSHMI, [3]Dr.K.CHOKKANATHAN, [4]K. SENTHIL KUMAR

[1]Assistant Professor, Saveetha School of Engineering
[2]Associate professor, Adhi College of Engineering and Technology
[3]Assistant Professor, Madanapalle Institute of Science & Technology
[4]Associate Professor, Rajalakshmi Institute of Technology

Abstract:

Providing strong security is mandate to prevent unauthorized and corrupted messages from forwarding into the network. Real time data access from nodes is essential for critical applications in Wireless Body Sensor Networks (WBSN). A novel scheme, which includes Data Encryption and Signature based Authentication protocol (DESA) is proposed here and the objective is to provide reciprocated authentication based on signature verification ID. To offer secured communication with low overheads this mechanism is proposed in order to ensure the secrecy of the sensed data within the WBSN entities. Sender sends the encrypted message text labeled with the set of attributes and the signature ID is assigned properly to indicate node authentication. The authorized signature ID is verified and the data encryption is done at the receiver end. Therefore proposed DESA scheme has the capability to tolerate a number of security attacks, provides high security compared existing security mechanisms.

***Keywords**:* Data encryption, Signature generation, SHA algorithm, Wireless Body Sensor Network.

1. Introduction

Wireless sensor nodes are widely used to sense and pass the same information about the infrastructural description. Sensor nodes comprises of minimal cost, limited memory capacity with low operating power resources. Health care monitoring, environment monitoring, civil and military applications, goal tracking are some of the application area of WSN. Several nodes are placed in the sensing network and rigid to maintain its security because malicious nodes can easily infuse false info into the system.

WBSN is a promising innovation for our current lives where communication technology helps us to report our health status to the medical specialists much faster than any time before. However, the dependability and security chances related with this innovation are expanding because of the practicality of catching delicate data by means of WBSN channels and inappropriate design procedures. Each node that enters in to the network needs to be authenticated first therefore unauthorized access from the nodes can be prevented. Verifying and validating the node identity in the whole network is must for authentication purpose that assures the source info. Data authenticity is made so that the sensed info can only be access by authorized users.

2. Related works

Some of the securities related authentication mechanisms were discussed here for the reference. An authentication protocol named Lightweight Dynamic client Authentication Scheme [1] was proposed to act in opposition to replay and forgery attacks. This method has three steps such as registration, login and authentication. Additional requirements such as Username and password are recommended for registration purpose once the user registered successfully a query with allotted time period can be submitted. If allotted time period gets expired because of some processing or transmission delays, then client needs to start again a new cycle by doing registration steps again.

Group-based cooperation [2] using symmetric secret key generation was proposed via Received Signal Strength Indicator (RSSI) information also the functional process was examined. Here, a co-operative group solution was implemented for increasing similarity measure, fluctuation and data's RSSI density for the consequences of high competent key generation. Main motive of this scheme is to make complete use of multiple channels that exists among a participant node and a group node or between two groups to randomly synthesize RSSI data. Scalable Energy based Trust model for Security and Data Encryption (SETS-DE) with the private key was proposed [3]. Sensor nodes have restricted capacity so significant calculations for security methods are not appropriate subsequently; therefore by utilizing its energy utilization esteem the trust estimations of nodes are registered for security reason.

Assessment of a safe network confirmation and transmission subsystem dependent on a polynomial-based validation plot [4] was proposed. The strategies in this subsystem to build up keys for each biosensor are communication effective and energy proficient. Additionally, an enemy eavesdropping in a BSN faces unavoidable channel errors. The adversary's uncertainty regarding are exploited for PHI transmission to refresh the individual key progressively and improve key mystery. Joint enhancement of the actual layer security with start-finish delay the executives are concentrated in the remarkably obliged setting of WBANs.

A game-theoretic framework was proposed [5] wherein body-worn sensor devices co-operate actively using wire-tappers also in circumstances of blurring channel conditions to locate the most secure multi-bounce way to the center point, while holding fast to the start to finish defer prerequisites forced by the application. The issue is demonstrated for Nash network geography where no one-sided deviation in arrangement subsequently any single sensor node can ready to improve the transmission mystery rate. This gives a conveyed calculation ensured to join to a Pareto-predominant Nash arrangement. For building up and refreshing the keys among the sensor nodes [6] a productive and versatile scheme was proposed. In this component all sensor nodes keeps up a table called key store to deal with the keys. This key reserve checks for the current key pair among the nodes and confirms by coordinating the key with base station.

Binomial Principle System (BPS) technique was utilized for ignoring the malignant nodes from routing. Fake route is produced by applying BPS to the source, sink, and routing node Id's so that the original node Id's [7]. Distributed Privacy Preserving Access Control (DPPAC) [8] scheme was proposed. Here the network owner generates the token by using unsighted signature. The users buy signatures from the network owner and these signatures can be verified by any other sensor node present in the system. However the scheme DPPAC is not much proficient if the signature is used already and contains limited memory storage.

Mark based admittance control with security was proposed to DPPAC [9] constraints and to give secrecy in a dispersed admittance control climate. In this strategy three unique members are considered, for example, network proprietor, sensor organization and its clients. An exploitative client or malevolent client may dispatch an assault in the organization henceforth the organization clients with various advantages requires security for their produced questions. Secret word based client access control conspire with property based encryption was proposed in various characterized sensor network [10]. Legitimate key should be utilized with coordinating arrangement of traits to recover the data from the organization; hence information given for higher access favoured clients cannot be accessed by lower special clients.

Negative Correlation Attack using Physical Key Extraction (NCA-PKE) on sensors for WBSN [11] was proposed. Here negative connection can be abused and represents a huge threat for sensors using key extraction strategies that depend on the actual layer and utilize channel-state data. Moving normal is a regularly utilized technique to improve key arrangement between real gatherings that improves the certainty of the contrarily related aggressor by 23%. Quantizer boundaries should be chosen cautiously for maintaining a strategic distance from information spills. Lightweight client verification instrument for WSNs [12] utilizes shared confirmation and meeting key arrangement. Some current and conventional attacks are utilized to show the strength against the equivalent. This technique was demonstrated to show classification, respectability, common confirmation and generating the session key.

User validation for remote sensor network is planned generally for made sure about correspondence. This mechanism requires simple operation such as single way hash utility for secured communication. To secure the data communications between wearable sensors and the data consumers (medical practitioners) Ciphertext Policy Attribute Based Encryption (CP_ABE) [13] was proposed on basis of communication architecture. CP-ABE and signature to store the data in cipher-text format at the info sink therefore this process ensures data security.

3. Proposed Method

Data Encryption and Signature based Authentication protocol (DESA) is proposed here and the objective is to provide reciprocated authentication based on signature verification ID. This mechanism is proposed to offer secured communication with low overheads also to ensure the secrecy of info that is sensed by the sensing ndoes fixed over the body. Sender sends the encrypted message text labeled with the set of attributes and the signature ID is assigned properly to indicate node authentication. The authorized signature ID is verified and the data encryption is done at the receiver end. The signature is encrypted along with the data at the sender side and the decryption process is done at the recipient side based on signature authentication. The signatures generated by the BS are sectioned with time-label to avoid replay attacks and to reduce man-in-the-middle attacks. If gateway needs to access data from the sensing node fixed over the body, then following phases are to be carried out.

(i) Check-in level

Once the node enters the network should get registered with BS for completing the check-in process. The node N_a sends Check-in request Message (CM) to BS with the key named Snd( ) operation key. Then the node is registered and the particular id is stored in the BS for further reference. If CM has no issues while registering with BS then it is labeled as authorized node ‘NA_a’. If specific node needs to communicate with its neighbours like sending or receiving the sensed info, the allotted Id is must to initiate the process. The node gets started to communicate once owner verifies the node with the key ‘Ka’. The check in request message is calculated using equation 1.

$$CM \xrightarrow{BS} Snd\left(IdN_a \,\|\, \mathrm{K}a\right) \tag{1}$$

(ii) Signature generation

BS generates signature keys for all the CM nodes for data encrypting. The nodes with the keyed signatures have network access for fetching required info and these generated signatures. BS further creates a random secret number S_n and computes the private key for the generated signature ID (SId_j) of the legal user node L_j. If the lock key created for signature is set as public then the nodes that is registered with various signature key can able to access the data. Consequently matching confidential key verifies the signature and announces the node is legal. Once the signature is signed with the strong key then it will be available only for the authenticated node service. Node’s that has authenticated signature is declared to be a legal (can be accessed by all authorized nodes) node in the system so as to authorized user can access the data by decrypting process.

Algorithm

1. Using SHA1- hash value is computed for node.
2. Preceding 8 byte series is taken from created hash value.
3. Backing operation is done on 8-byte series.
4. Obtained reversed series is termed as generated signature (encrypted) key.

(iii) Message encryption

Random key generator creates signature key M_k for encrypting sensed info process. If the legal node needs to login the gateway, then it sends the login request message to the BS. Once receiving info_request message, gateway initiates the authentication process using signature verification process and validates the node for authorized access. Sensed data is encrypted using secured hash algorithm, then M_k is sent to the destination with the encrypted signature SId_j(key) which is affixed in the header section of the encrypted message.

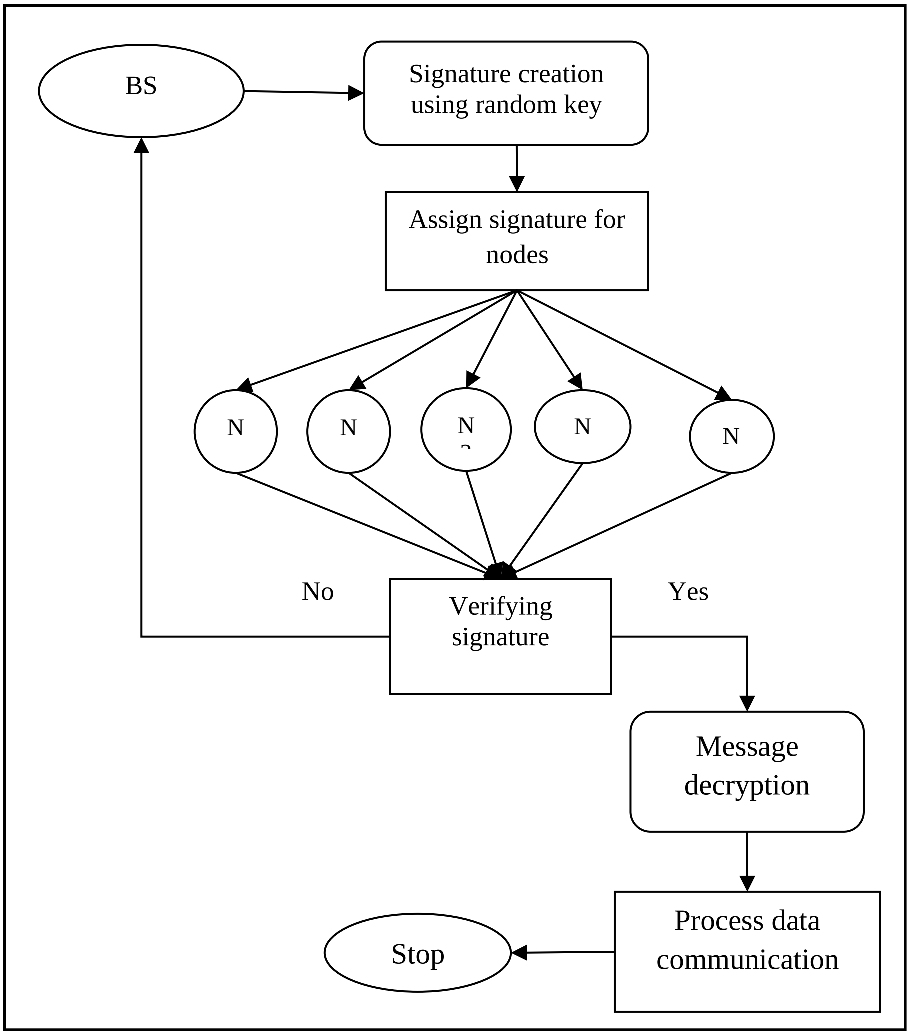
BS
Signature creation using random key
Assign signature for nodes
N
N
N
N
N
No
Verifying signature
Yes
Message decryption
Process data communication
Stop

Figure 1: Signature based Message Security

BS checks for the signature verification, if the received signature matches with the preloaded signature key, then the data is decrypted using decryption algorithm. Else, signature id tagged node is identified as attacker or malicious node and the information received from the node is neglected. The sensed information is accessed in a distributive manner; hence there is high chance of injecting false information. Figure 1 shows the flow diagram of signature based message security for data transmission in WBSN. The main objective of the proposed DESA protocol is for providing data privacy and user authentication in order to prevent from false injection of data by the malicious nodes.

4. Results and Discussion

The simulation investigation is finished utilizing the system test Network Simulator (NS-2). It is a progression of open source discrete event test system and offers generous support for simulation of TCP, routing and multicasting conventions over wired and remote systems.

The coding part is written in C++ and OTCL (Object oriented Tool Command Language). The proposed scheme DESA and the conventional scheme NCA-PKE are analyzed and contrasted with the obtained results. The system traffic in the recreation model is dealt with utilizing traffic model such as Constant Bit Rate (CBR). Table 1 describes about the parameters used for simulation.

Table 1: Simulation Parameters

Parameter	**Value**
Type of channel	Wireless Channel
Time of Simulation	50 ms
Nodes count	100
MAC type	802.11
Traffic model	CBR
Area of Simulation	1000×850
Communication range	250mts
System interface Type	WirelessPhy

The parameters utilized for the simulation of the proposed system are tabulated above. Broadcasting waves are propagated by utilizing the proliferation model two beam ground. The exhibition of the proposed plot is assessed by the measurements delivered packet proportion, delay, energy consumption and key mismatch rate.

Delivered Packet Rate

Delivered Packet Rate (DPR) is estimated by taking the number of packets that is reached successfully to the receiver node with respect to the packet that is sent by the source node. Equation 2 is used to calculate DPR.

$$DPR = \frac{Packets\ Rcvd}{Total\ Packets\ sent} \tag{2}$$

The delivery rates of packet for the proposed DESA method has higher delivery rates than the ratio of the conventional scheme NCA-PKE and it is exposed in figure 2. The more prominent estimation of packet delivery ratio implies the better execution of the protocol.

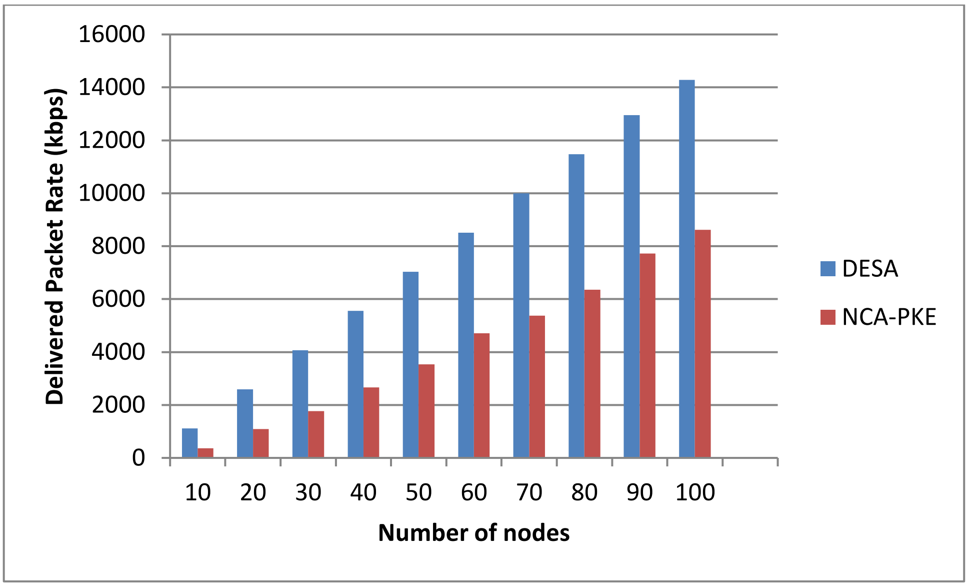

Figure 2: Packet Delivery Proportion

Delay

Average delay is defined to be the time contrast taken for the packets received currently to the previous packet received. It is calculated by the equation 3.

$$Delay = \frac{\sum_{0}^{n} PktSendTime - Pkt\,\mathrm{Re}\,cvTime}{Time} \tag{3}$$

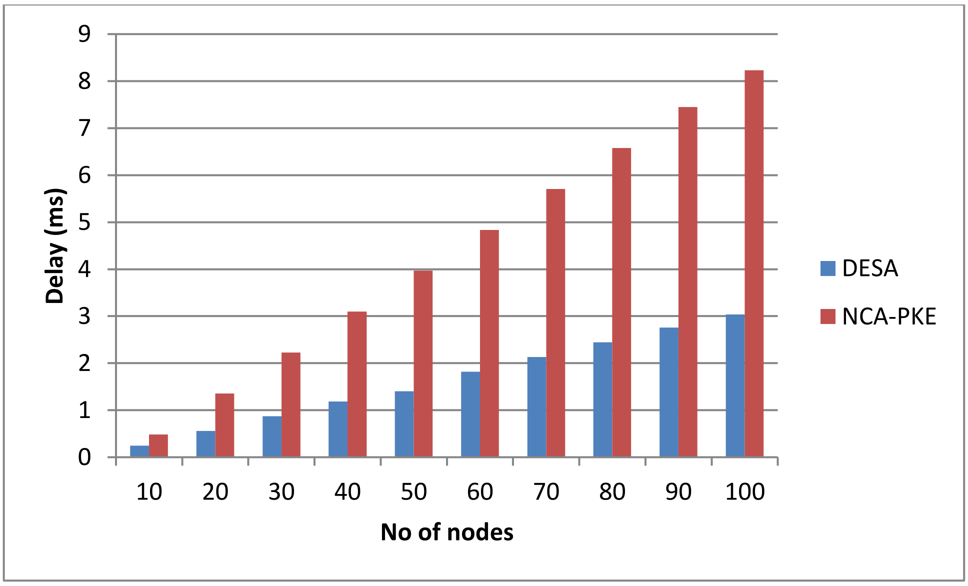

Figure 3: Delay

Figure 3 show that the delay value is low for the proposed scheme DESA compared to conventional NCA-PKE scheme. The base estimation of delay implies that higher estimation of the throughput of the system.

Energy Consumption

Nodes consume certain level of energy to process a data transmission and is said to be energy consumption. The power level that is used for sensing, processing, transmitting and receiving the data is said to be energy expenditure rate.

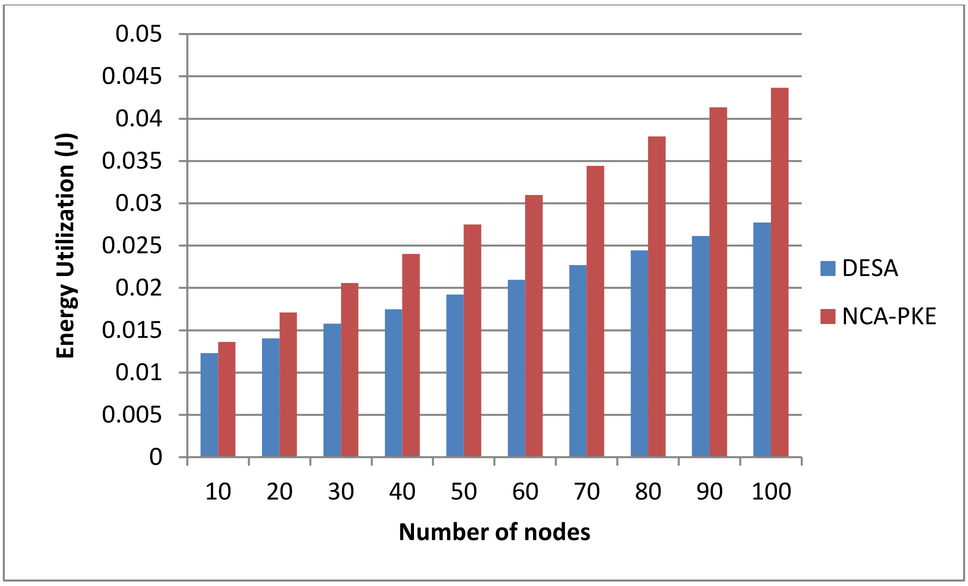

Figure 4: Energy Consumption

Figure 4 shows that the proposed method DESA consumes less energy consumption level compared to the existing NCA-PKE method.

Key Mismatching Ratio

Key Mismatch Ratio (KMR) is defined as the main metric to recognize false private keys generated by malicious nodes which gets mismatch when paired with BS.

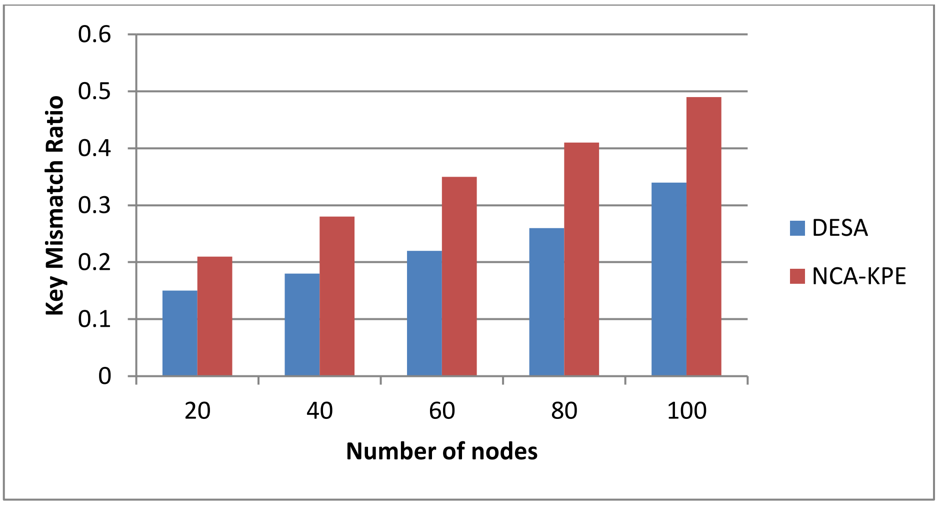

Figure 5: Key Mismatch Ratio

The ratio between various numbers of bits in the secret keys with the total number of key bits created for signature verification is said to be KMR. Figure 5 describes about key mismatch ratio for both proposed scheme DESA and conventional NCA-PKE scheme. The proposed has less key mismatch ratio since using strong signature private keys when compared to the conventional NCA-PKE protocol.

5. Conclusion

A novel scheme which includes Data Encryption and Signature based Authentication protocol is proposed to provide secured communication in wireless sensor networks. The data access with security is provided by using token based message encryption process. Signature Id tagged node which is verified by the base station is identified as legal node and the information received from the node is accessed and headed as legal data. The overheads are greatly reduced and the malicious nodes and the messages from the node are neglected by the signature based message verification system.

References

1. Cheikhrouhou, Omar, Anis Koubaa, Manel Boujelben, and Mohamed Abid. "A lightweight user authentication scheme for wireless sensor networks." In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010, pp. 1-7. IEEE, 2010.
2. Li, Z., Wang, H., & Fang, H. (2017). Group-based cooperation on symmetric key generation for wireless body area networks. *IEEE Internet of Things Journal*, *4*(6), 1955-1963.
3. Kumar, A. S., & Logashanmugam, E. (2017). Secured Optimal Routing Based on Trust and Energy Model in Wireless Sensor Networks. *IIOAB JOURNAL*, *8*(3), 13-18.
4. He, D., Chen, C., Chan, S., Bu, J., & Zhang, P. (2012). Secure and lightweight network admission and transmission protocol for body sensor networks. *IEEE journal of biomedical and health informatics*, *17*(3), 664-674.
5. Moosavi, H., & Bui, F. M. (2016). Delay-aware optimization of physical layer security in multi-hop wireless body area networks. *IEEE Transactions on Information Forensics and Security*, *11*(9), 1928-1939.
6. Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010.
7. Suresh, G., & Kumar, A. S. (2020). Secure Transmission Using Bivariate Principle System for WSN. *Helix*, *10*(03), 47-51.
8. R Zhang, Y Zhang, and K Ren, "DP2AC: Distributed privacy preserving access control in sensor networks," IEEE Transactions on Parallel and Distributed Systems vol.23, no.8, Aug 2012.
9. Tanuja, R., Y. R. Shruthi, S. H. Manjula, K. R. Venugopal, and L. M. Patnaik. "Token Based Privacy Preserving Access Control in Wireless Sensor Networks" In *Advanced Computing and Communications (ADCOM), 2015 International Conference on*, pp. 45-50. IEEE, 2015.
10. Cheikhrouhou, O., Koubaa, A., Boujelben, M., & Abid, M. (2010, May). A lightweight user authentication scheme for wireless sensor networks. In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010 (pp. 1-7). IEEE.

11. Dautov, R., & Tsouri, G. R. (2019). Effects of Passive Negative Correlation Attack on Sensors Utilizing Physical Key Extraction in Indoor Wireless Body Area Networks. *IEEE Sensors Letters*, *3*(7), 1-4.
12. Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, *8*(9), 1752-1771.
13. Hu, C., Li, H., Huo, Y., Xiang, T., & Liao, X. (2016). Secure and efficient data communication protocol for wireless body area networks. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(2), 94-107.