INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Lightweight Cryptography Using Pairwise Key Generation and Malicious Node Detection in Large Wireless Sensor Network

Sunny Sall[1]*, **Rajesh Bansode**[2]

1 Research Scholar, Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, Maharashtra, India
2 Professor, Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, Maharashtra, India

OPEN ACCESS

Received: 29-12-2022

Accepted: 14-08-2023

Published: 27-09-2023

Citation: Sall S, Bansode R (2023) Lightweight Cryptography Using Pairwise Key Generation and Malicious Node Detection in Large Wireless Sensor Network. Indian Journal of Science and Technology 16(36): 3002-3008. https://doi.org/10.17485/IJST/v16i36.2503

* **Corresponding author**.

sunny_sall@yahoo.co.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To design and develop pairwise key generation techniques for malicious node detection in wireless sensor network. **Method**: The lightweight key generation method has been used for data encryption with the collaboration of the sender node, entry node and destination. The unique identity of the destination server has utilized for data encryption and decryption as a master key. The proposed method generates a concise key length that reduces encryption and decryption time. It also helps to detect the misbehaviour of internal nodes when it takes higher time for data decryption and transmission. **Findings**: The proposed system reduces end to end delay around 10%, the packet delivery ratio improves by 3.30%, throughput by 9.87, and energy consumption by 20.50% than Advanced Encryption Standard and Rivest Shamir Adleman algorithm. The proposed encryption algorithm compresses the cypher data, reducing the network overhead, and detecting malicious nodes, providing higher security from internal and external intruders. This simulation obtains better results than existing systems that enhance around 7-9% throughput with all QoS parameters. **Novelty**: The proposed system eliminates network overhead of key transmission to the destination. Using this approach, the sender node generates a lightweight key for data encryption using the destination node, which means only the destination node can decrypt the data using the generation of similar keys. When any random node tries to generate such keys, it violates time-bound, and system detects as a malicious node.

Keywords: Wireless Sensor Network; Intrusion Detection System; Energy Consumption and Conservation; Broadcast Tree Construction; Lightweight Key Encryption; Pairwise Key Generation

1 Introduction

Data security and misbehaving node detection is very important in Wireless Sensor Network (WSN). The sink receives either the raw data or the data that has been aggregated from the sensor nodes. The sink can command the network to assign jobs to the sensors and makes judgments based on the combined data. These decisions are based on the combined data. Wireless sensor nodes have additional vulnerabilities on top of the multiple fundamental security issues they already have. This is because they are often installed in areas that are not overseen and rely on substandard radio connectivity. End users may get erroneous sensing data as a result of several attacks, which can be damaging in contexts such as war monitoring and environmental monitoring. To ensure that systems are protected in an appropriate manner, appropriate security measures need to be implemented.

The paired key encryption and watchdog system that has been presented is designed to automatically recognise hostile nodes and shut them down before the system is hacked while it is moving data. The system may also be capable of enabling secure communication while detecting many forms of network attacks, including active attack, network attack, denial of service attack, Man in Middle attack, jammer attack, and passive attack. Internal nodes use the least amount of energy, which results in the network's lifespan being extended and the quality-of-service metrics being improved more efficiently. The building approach known as broadcast tree reduces any network and packet overhead that may be present on the internal nodes by making use of the fewest resources feasible. The system is equipped with three essential features, namely intrusion detection systems, intrusion prevention systems, and intrusion responding systems, which block malevolent nodes from talking with other network nodes for a certain amount of time after an intrusion has occurred.

In 2020, Pallavi Joshi describes an WSN security that describes an over the past ten years, WSNs have been widely used for a variety of purposes, giving rise to route-discovering techniques, often known as routing protocols. Discovering the optimum path is a fundamental requirement for any sensor network because SNs are energy-constrained. This paper discusses the application of various routing protocols, mostly responsive and composite. The protocols have been contrasted in regards to energy usage in transmission and receiving modes for multiple situations and duty cycles. According to analysis, reactive protocols such as Dynamic Source as well as Dynamic MANET on Demand Routing function best than composite protocols such as Zone Routing Protocol when used in sensor systems with higher duty cycles.[(1)]

Liu, W. et al.[(2)] proposed technique describes a revolutionary lightweight key establishment architecture built on top of random key distribution. It can boost the likelihood of communication between two nearby sensors, and the second approach can also let sensors verify the pairwise key that has been formed. Both algorithms only need the XOR operation, making them lightweight and particularly suited for WSNs. The main problem with this method is how long it takes to generate significant amounts of XOR operations.

According to[(3)] are vulnerable to numerous assaults, including wormhole, sinkhole, Sybil, jammer, and selective forwarding. This suggested strategy is focused on determining trust value. The monitoring node constantly determines the trust level. Every node whose trust value falls underneath the threshold is labelled as hostile.

Gautam, A.K. et al.[(4)] described current key management, authentication, and trust management scheme in WSN made effort to identify the one that best satisfies the application's needs.

According to[(5)] the Denial-of-service attack is one of the most common ones. To prevent assaults, it is necessary to identify and mitigate them.

Pathak, G. et al.[(6)] the Blom-Yang essential agreement process as a centralised lightweight session key mechanism for LPWAN standards. The accuracy of this session key was also checked on the Mininet-WiFi emulator. The proposed session key method offers protection against replay attacks available with the present LPWAN session key schemes while using fewer transmissions than the existing LPWAN session key mechanisms. The possibility of a collision attack renders this system susceptible sometimes.

Vandervelden T. et al.[(7)] proposed an approach significantly varies from conventional group key management techniques, where a single compromised node renders the system inoperable. The fundamental foundation of the suggested course is a hash chain with numerous outputs specified at the gateway and distributed to additional network nodes. The main issue with this approach is its massive key generation, which results in network overhead during crucial transmission.

Mohamed Ali Kandi et al.[(8)] describes an approach that makes use of smart contracts and blockchain technologies. When an entity fails, the system still functions and that the whole network is not in danger when an entity is compromised. This system further indicates that the solution satisfies the IoT standards for performance and security.

Zhou, L. et al.[(9)] proposed a lightweight critical generation method for effective data transmission and secure encryption. This method is much more efficient and consumes less power than traditional digital encryptions through actual power consumption in large sensing environments. The major limitation of this method is it can send small data parts in a specific time.

In [10], created a system to produce randomly chosen multi path routes. The "shares" of various packets follow distinct routes under this arrangement, which changes over time. All packets are encrypted before being sent, and it is then decoded once received all. Therefore, even if the adversary learns the routing scheme, they still are unable to determine the exact pathways that every packet takes. The created paths are quite capable of ignoring black holes because they are highly dispersive, energy-efficient, and unpredictable.

2 Methodology

Lightweight Encryption Method: In the first phase, as shown in Figure 1, it proposes a lightweight encryption method using pairwise key generation approach. Initially source node $S_N$select the destination node D_N, then each D_N having own identity such as ip address or MAC address. So, S_N usage the encryption as D_N identity for data encryption and forward it to destination node. The source node message generation is defined in below equation.

M ← encrypt (msg, D_N)

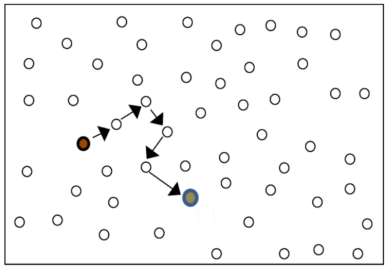

Fig 1. Proposed System Model for Lightweight Data Encryption between Source to Destination

The major advantage of this method, only D_N can decript of cipher data by using own identity otherwise remaining nodes are not able to decrypt received encrypted data due to incorrect keys. The description process done by destination node is describes as below:

Msg ← decrypt (M, D_{id})

The M is the cipher text, D_{id} is the destination nodes and Msg is the recovered plain text data. This method gives assurance of no data leakage and data loss issues.

Attack Detection Model:

The watchdog technique is a mechanism that depends on broadcast capabilities and may be used in WSNs to discover rogue nodes in the network. A node, such as node A, that has the aim of transferring the data to another node, such as node C, may listen in on the sent traffic of another node, node B, and determine whether the other node, node B, will transport the data to the node C, as shown in Figure 2.

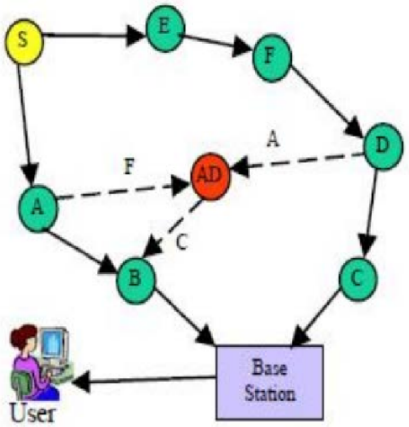

Fig 2. Proposed System Model for Malicious Node Detection in Wireless Sensor Network

The Figure 2 demonstrates a detection of malicious nodes between source and sink nodes. It tries to provide a unique approach that is based on the Watchdog methodology but is altered to improve the security of WSNs. Improved Watchdog is the name given to this approach. In contrast to the basic technique, which considers node A to be the watchdog and assumes that the cluster heads were the first layer watchdogs, the I-Watchdog approach presupposes that the cluster heads were the first layer watchdogs.

Proposed Encryption Model using Lightweight Key Encryption Model

1: Client generate text ***msg*** for sending to destination server

M ← Genereate_Message_Block(***msg***)

2: Select destination node using below function

$$Dest\,(IP) = \sum_{n=1}^{m} (s_n\ random(n,m))$$

3: Extract mac id of both destination nodes and sender node

$$Dest\,(Mac_{id}) = GetMaccAddress(Dest\,(IP))$$

$$Source\,(Mac_{id}) = GetMaccAddress(Source\,(IP))$$

The $GetMaccAddress()$ is the method which helps extract MAC address of specific device, it is also similar to $GetInetAddress()$ in socket programming using TCP-IP and UDP protocol. In step 3 we extracting MAC address of individual machine using IP address.

4: Apply XOR on both mac address

Enc_Key[] ← New_XOR($Dest\,(Mac_{id})\,, Source\,(Mac_{id})$)

Here we applied XOR function that take input the Source MAC address and Destination MAC address for generation of encryption keys. We generate here max 128-bit keys that provides minimum time for cyclic encryption.

Plain-byte[] ← M-text.toByteArray[]

encData[]=apply cipher-data method on (***Plain-byte[],*** *Enc_Key*)

Enc-string=Encode 64BaseEncoder on(***encData[]***)

Send ***Enc -String to*** $Dest\,(IP)$

5: extract mac id of both sender nodes and destination node

$$Dest\,(Mac_{id}) = GetMaccAddress(Dest\,(IP))$$

$$Source\,(Mac_{id}) = GetMaccAddress(Source\,(IP))$$

Dec_Key[] ← New_XOR($Dest\,(Mac_{id})\,, Source\,(Mac_{id})$)

6: Byte_Data[] ← Decode 64BaseDecoder(***Dec_key , Enc_String***)

byte utf [] =apply decipher method on (***Byte_Data[] , key _data***)

p_data = convert into string class (utf)

The ***p_data*** is final decrypted string

The primary benefit of the algorithm is only the destination node can decrypt data using a secure key generation function. If any attacker or internal nodes generates malicious activities and tries to decrypt the cipher data using multiple random key generations. In that case, the algorithm raised an error due to invalid keys because these keys are generated using invalid destination MAC id. This technique also reduces the network overhead due to no need to transfer keys via network stream to destination node or any secure storage. The destination node can generate decryption keys itself.

3 Results and Discussion

In the extensive experimental analysis, we calculate the time for data encryption and description for both the source node and destination nodes end. Below, Figure 3 describes the data encryption time for different data size and compare it with various existing models. This figure takes fewer time data for data description with different sizes. It obtains better results than Liu [(2)],

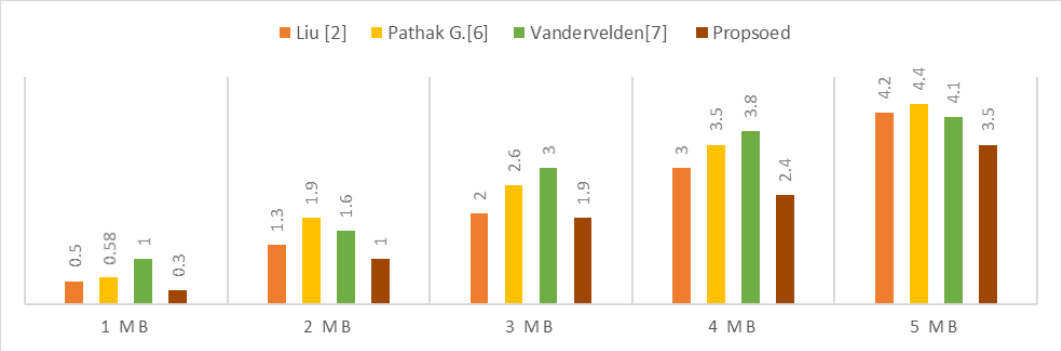

Fig 3. Time required for data encryption using proposed lightweight key in large WSN

Pathack G.[6] and Vandervelden[7]. The proposed system reduces data encryption time due to small key generation. The system improvement time should be 15-18% off than existing approaches.

Once data is received by destination nodes, it evaluates the identity of nodes and, based on that, performs the decryption process. Figure 4 below demonstrates the time required for data decryption with different data sizes, such as 1 MB to 5 MB. Due to the small and secure key, the decryption process also takes lower computation.

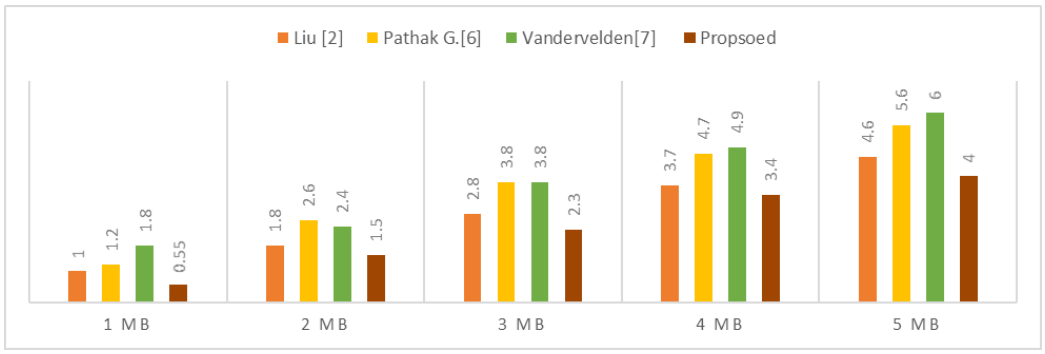

Fig 4. Time required for data decryption using proposed lightweight key in large WSN

In the second experiment, the attack detection has done with various network sizes such as 100, 200 and 500 nodes. Detecting such nodes that are doing abnormal behaviour considers the system malicious. Figure 5, demonstrates the detection of various network attacks and compares them with state-of-the-art methods.

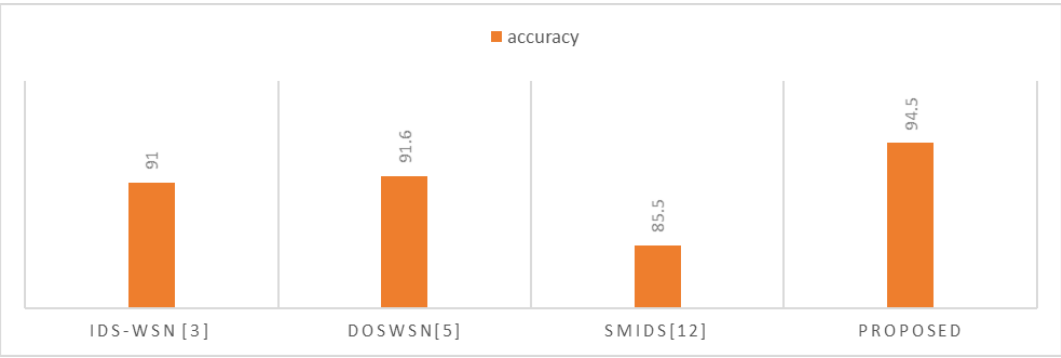

Fig 5. Attack detection accuracy of proposed method and comparison with various existing systems

Figure 5, describes the proposed model obtains higher results than IDS based methods such as[3,5,11] [5] in large WSNs.

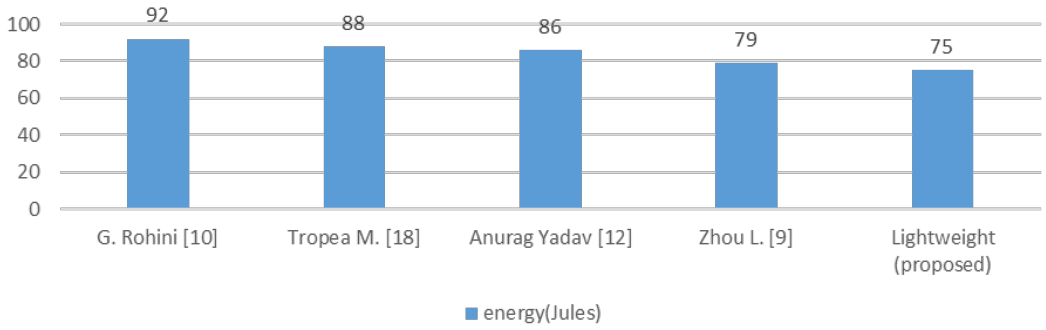

Fig 6. Energy consumption for data encryption and decryption using various methods; min data size 1 kb

According to Figure 5 and Figure 6, the proposed lightweight key generation method required minimum time and energy for data encryption and decryption. It shows almost 20.50% lower energy consumption than other encryption mechanisms such as [10,12].

Standard and Rivest Shamir Adleman algorithm:

Table 1. Comparative analysis for key generation time required with various bit encryption techniques

Method	Key_size (char)	Generation Time (sec)	Bit_encryption (bits)
G. Rohini [10]	1 to 10	23	64
Tropea M. [12]	1 to 12	25 and 46	64 and 128
Anurag Yadav [11]	1 to 8	21 and 39	64 and 128
Zhou L. [9]	1 to 5	9 and 17	32 and 64
Lightweight (proposed)	1 to 5, 10	8, 13 and 34	32,64 and 128

The above Table 1, describes a key size as well as time required for generation of keys using different bit encryption techniques. In this mechanism we provide hassle free key extraction model for destination node. This table demonstrates proposed system required minimum time for key generation using all 32-, 64- and 128-bit encryption methods. It also requires minimum time compare to other key generation techniques such as [9–18].

In another experiment we evaluated the traces after simulation completion and evaluated the QoS parameters such as Throughput, energy consumption, end to end delay, network overhead and packet drop ratio. According to evaluation the proposed system reduce end to end delay around 10%, the packet delivery ratio improves by 3.30%, throughput by 9.87.

4 Conclusion

This work describes lightweight cryptography using pairwise key generation to detect malicious nodes in large WSNs. The source node and destination have collaborated to generate public and private keys. Similar keys are used for data encryption and data decryption also. The significant benefit of this system is that only the destination node can decrypt the data using self-generated keys. This system gives assurance to provides higher security and eliminates collision attacks. According to QoS parameters, the proposed model increases the packet delivery ratio by 3.30%, throughput by 9.87 times, and energy usage by 20.50% compared to AES and RSA. The proposed system reduces the end-to-end latency by about 10%. Using a tree structure for finding the destination node from the source to achieve low-time computation and overhead will be the future work of this system.

References

1) Joshi P, Singh G, Raghuvanshi AS. Impact of Duty Cycle and Different Routing Protocols on the Energy Consumption of a Wireless Sensor Network. In: 2020 International Conference on Communication and Signal Processing (ICCSP), 28-30 July 2020, Chennai, India. IEEE. 2020. Available from: https://doi.org/10.1109/ICCSP48568.2020.9182140.
2) Liu W, Harn L, Weng J. Lightweight key establishment with the assistance of mutually connected sensors in wireless sensor networks (WSNs). *IET Communications*. 2022;16(1):58–66. Available from: https://doi.org/10.1049/cmu2.12312.

3) Patel MM, Patel PK. Intrusion Detection System Based on Trust Value in Wireless Sensor Networks. In: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), 12-14 June 2019, Coimbatore, India. IEEE. 2019. Available from: https://doi.org/10.1109/ICECA.2019.8822081.
4) Gautam AK, Kumar R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Applied Sciences*. 2021;3(50):1–27. Available from: https://doi.org/10.1007/s42452-020-04089-9.
5) Kurniawan MT, Yazid S. Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 12-13 June 2020, Istanbul, Turkey. IEEE. 2020. Available from: https://doi.org/10.1109/ICECCE49384.2020.9179255.
6) Pathak G, Gutierrez J, Ghobakhlou A, Rehman SU. LPWAN Key Exchange: A Centralised Lightweight Approach. *Sensors*. 2022;22(13):1–16. Available from: https://doi.org/10.3390/s22135065.
7) Vandervelden T, De Smet R, Steenhaut K, Braeken A. Symmetric-Key-Based Authentication among the Nodes in a Wireless Sensor and Actuator Network. *Sensors*. 2022;22(4):1–11. Available from: https://doi.org/10.3390/s22041403.
8) Kandi MA, Kouicem DE, Doudou M, Lakhlef H, Bouabdallah A, Challal Y. A decentralized blockchain-based key management protocol for heterogeneous and dynamic IoT devices. *Computer Communications*. 2022;191:11–25. Available from: https://doi.org/10.1016/j.comcom.2022.04.018.
9) Zhou L, Kang M, Chen W. Lightweight Security Transmission in Wireless Sensor Networks through Information Hiding and Data Flipping. *Sensors*. 2022;22(3):1–16. Available from: https://doi.org/10.3390/s22030823.
10) Rohini G. Dynamic router selection and encryption for data secure in Wireless Sensor Networks. In: 2013 International Conference on Information Communication and Embedded Systems (ICICES), 21-22 February 2013, Chennai, India. IEEE. 2013. Available from: https://doi.org/10.1109/ICICES.2013.6508249.
11) Yadav A, Gupta H, Khatri SK. A Security Model for Intrusion Detection and Prevention over Wireless Network. In: 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 21-22 November 2019, Mathura, India. IEEE. 2020. Available from: https://doi.org/10.1109/ISCON47742.2019.9036288.
12) Tropea M, Spina MG, De Rango F, Gentile AF. Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer. *Future Internet*. 2022;14(5):1–20. Available from: https://doi.org/10.3390/fi14050145.
13) Karthigadevi K, Balamurali S, Venkatesulu M. Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to Detect and Prevent the Sinkhole Attack in Wireless Sensor Network. *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*. 2019. Available from: https://doi.org/10.1109/INCOS45849.2019.8951406.
14) Siasi N, Aldalbahi A, Jasim MA. Reliable Transmission Scheme against Security Attacks in Wireless Sensor Networks. *IEEE*. 2019;p. 1–6. Available from: https://doi.org/10.1109/ISNCC.2019.8909123.
15) Skoufas K, Spyrou ED, Mitrakos D. Identifying DDoS Attacks from Fluctuations in Wireless Traffic in an Intelligent IoT Road Network. *2020 International Wireless Communications and Mobile Computing (IWCMC)*. 2020;p. 451–456. Available from: https://doi.org/10.1109/IWCMC48107.2020.9148242.
16) Sall S, Bansode R. Energy Efficient Approaches for Dynamic Cluster Head Selection Using Optimized Genetic Algorithm in Cluster Networks of WSN". *Turkish Online Journal of Qualitative Inquiry*. 2021;12:2742–2752. Available from: https://www.tojqi.net/index.php/journal/article/view/8055.
17) Sall S, Bansode R. Broadcast Tree Construction for Shortest Path Finding Techniques in WSN IEEE802.11n. *Design Engineering*. 2021;2021(9):3295–3310. Available from: http://thedesignengineering.com/index.php/DE/issue/view/31.
18) Sall S, Bansode R. Secure Data Aggregation and data Transmission using HMAC Protocol in Cluster base Wireless Sensor Network", Intelligent Computing and Networking. *Lecture notes in Networks and Systems*. 2020;146. Available from: https://doi.org/10.1007/978-981-15-7421-15_21.