

Proximate node aware optimal and secure data aggregation in wireless sensor network based IoT environment

Sushma Priyadarshini¹, Asma Parveen²

¹Department of Computer Science and Engineering, Kallerawan Charitable Trust Engineering College, Gulbarga, India

²Department of Applied Sciences, Faculty of Engineering and Technology, Khaja Bandanawaz University, Gulbarga, India

Article Info

Article history:

Received Jul 26, 2022

Revised Apr 20, 2023

Accepted May 11, 2023

Keywords:

Data aggregation

Internet of things

Proximate node aware-SDA

Secure data aggregation

Wireless sensor network

ABSTRACT

Internet of things (IoT) has become one of the eminent phenomena in human life along with its collaboration with wireless sensor networks (WSNs), due to enormous growth in the domain; there has been a demand to address the various issues regarding it such as energy consumption, redundancy, and overhead. Data aggregation (DA) is considered as the basic mechanism to minimize the energy efficiency and communication overhead; however, security plays an important role where node security is essential due to the volatile nature of WSN. Thus, we design and develop proximate node aware secure data aggregation (PNA-SDA). In the PNA-SDA mechanism, additional data is used to secure the original data, and further information is shared with the proximate node; moreover, further security is achieved by updating the state each time. Moreover, the node that does not have updated information is considered as the compromised node and discarded. PNA-SDA is evaluated considering the different parameters like average energy consumption, and average deceased node; also, comparative analysis is carried out with the existing model in terms of throughput and correct packet identification.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Sushma Priyadarshini

Department of Computer Science and Engineering, Kallerawan Charitable Trust Engineering College

Gulbarga, Karnataka, India

Email: sushmapriyadarshini12@gmail.com

1. INTRODUCTION

Wireless sensor network, also popularly known as WSN comprises some sensors. One can define it as a wireless network that is self-configured and it does not have and specific infrastructure. The purpose of this is to document and observe the environment and its physical circumstances. Moreover, internet of things (IoT) collaborated with WSN possesses enormous application; the information that is collected will be preserved in a centralized position. Lately, the WSNs have got substantial recognition due to its applications in various fields like military, healthcare industries and underwater observations as it is inexpensive, consumes minimal area [1]–[3].

Lately, the WSNs have stretched their applications to various sectors like intelligent factories, and smart cities. Here, the device, data, and network administration techniques of the WSNs play an important role. To implement the factory operations intelligently, the sensor nodes are used for accumulating information on machines and products. The vital part of planning a smart city is the efficient usage of the available resources without any wastage. Hence, the WSNs are employed to provide the people and the municipal workers a well-organized service. Figure 1 shows the typical data transmission in the WSN based environment; moreover, it comprises source devices i.e. sensor node, cluster head also known as CH, and base station. Moreover, the data is sensed through the source device and it is sent to the cluster head further and through the cluster head, it is sent to a base station.

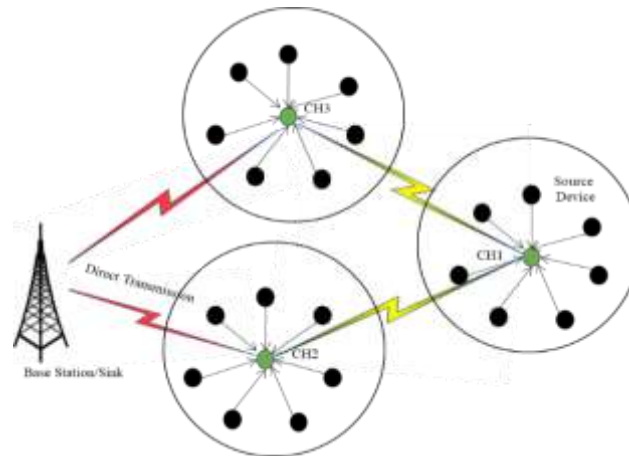


Figure 1. Typical data transmission in WSN environment

We can observe the distribution of the sensor nodes over a maximum area as it can sense the monitoring information and transmit the data to a server or a sink. For the successful transmission of the accumulated data to the server, the multi-hop transmission method is employed. The server, where the data storage takes place will be positioned far away from the source sensor node viz. out of the range of transmission. For the determination of an ideal sink route, sensor node accumulation is done [4]–[6]. One can expect some redundancy in the source information as the information is being accumulated by many sensors and they follow the same phenomena though they are positioned in their respective areas. The popularly employed method in WSN for redundancy removal and the reduction of the transmission or information size is data aggregation (DA) viz. for the processing within the network. This method decreases the energy consumption during the data collection. In various applications of WSN, there is no requirement to transmit the exact data that is collected at the sensor node to the sink node and there can be processing done on the data for easy transmission. Based on the observing purposes of applications, multiple aggregation methods can be employed for the abstraction or compression of the raw information present in the network.

The techniques that are used here are, abstracting as {mean, variance}, maximum and minimum values, lossy compression, feature domain reduction, and information prediction. An increase in the value of the correlation between the information accumulated by multiple sensors increases the efficiency of the DA. DA can successfully enhance the data accumulation's energy efficiency where the aggregation of the sensed information is done by the relaying nodes [7]. DA has a plethora of applications because of its dominance inefficient energy usage. But assuring its security is a significant thing as the WSNs are mostly used in a neglected or hostile domain where forging of the data in the process of delivery or the capturing of the sensor nodes may be the consequences. We can say network security aims to assure confidentiality, integrity, and availability (CIA). To achieve these multiple approaches are delineated namely, encryption, vulnerability analysis, authentication, and detection of the attack. Yet, conventional security approaches cannot be employed to DA directly as they can clash with a WSN with DA [8]. Considering the encryption as an example, during the process of aggregation operations (i.e. add, multiply, subtract, divide, max/min, sum, and average) there is a requirement of the actual plain text but the encryption of the data restricts the relay nodes from plaintext being used.

An ideal remedy to solve this issue is the usage of a sharing key, initially, the two nodes should get the sharing key, and then the source will encrypt its sensed information to a ciphertext and the destination gets the ciphertext then decrypts the text using the shared key. By utilizing this method, the plaintext is transmitted without making itself visible to other nodes [9]. Furthermore, in past, several types of research were carried out for secure DA; the few of them have been reviewed further. Girao *et al.* [10] concealed data aggregation (CDA) was introduced; symmetric homomorphic encryption is the base for this algorithm. Here, aggregation of the encrypted information can directly be performed by individual nodes. However, this approach has the disadvantage of not providing proper security as every node in the CDA shares a similar key. So, if one node is failed it troubles the whole global network. Research by Castelluccia *et al.* [11] delineates an algorithm that is implemented using the one-time pad for the CDA to be enhanced. For assuring information accuracy this algorithm needs extra data which, in turn, exceeds the communication overhead; a technique is developed where the encryption of the information present in the network would be done using the fully homomorphic encryption method [12]. This method will strengthen security and will decrease energy consumption. Research

by Zhang *et al.* [13] presented an algorithm is presented which is efficient in DA and it utilizes techniques like exclusive-or (XOR) homomorphic encryption and the method of probabilistic coding. Chim *et al.* [14] presented by using the features of Parlier homomorphic encryption and the bloom filters. According to Cheon *et al.* [15] a unique method is used where homomorphic cryptography plays an important role. By using this method, there is no requirement for secret key management. Hence, this method removes the problem of encrypting and decrypting the information inside the network. According to Acs and Castelluccia [16] gamma distribution and the method of homomorphic encryption are used for introducing a new scheme. The methods guarantee that the intruders and the aggregators cannot get the original information of each user in the process of aggregation. According to Ding *et al.* [17] for the deduction of the overhead during the process of encryption or decryption, the homomorphic encryption method is presented. This method will improve the security also against quantum computation. Research by Kapusta *et al.* [18] delineates a method called as additively homomorphic encryption and fragmentation (AHEF) scheme. Research by [19], [20] this scheme, put backs additively homomorphic fragmentation at the place of additively homomorphic secret sharing which is employed in the current methods. Data volume reduction and reduction in energy intake can be observed after these changes are made in the technique, [21] and [22] also developed a secure approach for DA, which was promising; however, they failed to address the nodes privacy [23]–[25].

In general, sensor nodes in WSN operate with limited resources like energy, storage due to the simplicity of WSN architecture. There are several motivational areas such as energy utilization, which can increase the network lifetime; furthermore, DA is one of the mechanisms, which helps to tackle the issue of computation overhead, data redundancy and improvises the network lifetime. However, secure DA remains a foremost issue in the DA; hence motivated by these, this research work designs and develops PNA-SDA mechanism, further contribution of research work is given as: i) in this research work, the PNA-SDA mechanism is introduced for secure and optimal DA, ii) PNA-SDA mechanism is a proximate node aware aggregation where proximate nodes hold the information of others and further it is updated in each state, and iii) PNA-SDA is evaluated considering average energy consumption, average deceased node; also, comparative analysis is carried out with the existing model and PNA-SDA outperforms the existing model.

This research work comprises various distinctive section and sub-section, the first section of the research work starts with background and application of WSN based IoT; further in the same section security issue is addresses and different related work is reviewed. Moreover, this section ends with the motivation and contribution of our research work. The second section involves the mathematical design of the PNA-SDA mechanism along with the algorithm. The third section of the research work evaluates the methodology along with comparative analysis and discussion.

2. PROPOSED METHOD

In this section, we design and develop a secure and efficient DA method. This not only preserves the particular node privacy but also provides efficiency for network lifetime such as optimal energy consumption. Moreover, the PNA-SDA methodologies are divided into several parts i.e. network design problem definition, optimal, and secure DA.

2.1. Network model and problem definition

PNA-SDA methodologies initialize the network and assume that in a network nodes are self-arranged in any given cluster; further, this network follows a hierarchical level of clustering where each node holds the same probability of selected as cluster head as r . Let us consider any connected graph with characteristics of undirected graph denoted as $J = (X, G)$ which represents the node-set and communication link. The main intention to develop the communication link is to secure the network topology information. Furthermore, any communication link (k, l) belongs to G if and only if two distinctive edges k and l can communicate with one another. Furthermore, let us consider P_k as the proximate node-set, then the proximate node is mathematically formulated as (1).

$$P_k = \{k | l \in X, (k, l) \in G, l \text{ is not equal to } k\} \quad (1)$$

Furthermore, let $|X| = p \geq 3$ be the number of nodes in a given network and $a_k(0)$ be initial node state which is initialized as $z(0) = [z_1(0), \dots, z_p(0)]^V \in \Omega_z^0 \subseteq T^p$.

2.2. Problem definition

To develop a secure DA mechanism, each node will communicate with the proximate node and update the information; moreover, in order to secure, the model additional data (randomly added data similar to noise) is added and information is sent to the proximate node. Moreover, the information sent is given through as (2).

$$z'(m) = \mu_k(m) + z_k(m) \quad (2)$$

In (2), μ_k indicates the additional data with k belongs to X ; further, the updated equation can be written as (3).

$$z_k(m+1) = \sum_l y_{kk} z_l(m) + y_{kk} z_k(l) \text{ for all } k \text{ belongs to } X \quad (3)$$

The equation can be formed in terms of the matrix is written as (4).

$$x(k+1) = Wx(k) \quad (4)$$

The equation w_{ij} and w_{ii} are considered as the weight matrix where w_{ij} and w_{ii} is greater than 0; also W is a stochastic matrix where the average is computed through the (5).

$$\lim_{k \rightarrow \infty} x(k) = \frac{\sum_{l=1}^n x_l(0)}{n} = \bar{x} \quad (5)$$

Considering the node's privacy, initial state sharing is a real concern and the node might not be willing to share the real state to its prominent nodes; thus, we use the additional data added to the original state whenever nodes tend to communicate with the proximate nodes. Moreover, this can be mathematically represented as (6).

$$\tau = \begin{cases} z'(m) = z(m) + \mu(m) \\ Z(m+1) = Y'_z(m) \end{cases} \quad (6)$$

Thus, we design an algorithm by adding the additional data such that the designed objective in the equation.

2.3. Proximate node aware secure data aggregation algorithm

The Algorithm 1 is designed for k number of nodes. Γ indicates the threshold iteration which is equal to r^2 . Furthermore, p^2 gives the guarantee of absolute DA. Also, each involved node ends the iteration once the proximate nodes are found.

Algorithm 1. PNA-SDA algorithm

Step 1. Selecting the individual element in $\mu_k(0)$ from random data.

Step 2. Consider $\hat{z}_k(0) = z_k(0) + \mu_k(0)$.

Step 3. Transmission of $\hat{z}_k(0)$ to the proximate node.

Step 4. Replace $\mu_k(0)$ with Γ_k and initialize $l = 1$.

Step 5. While ($m < \chi$) do.

Update $z_k(m)$ considering the initialization of k and $\hat{z}_l(m-1)$ and $\hat{z}_l(m-1)$.

Step 6. Choose $\Gamma_k(m)$ data packets randomly.

Step 7. Compute $\mu_k(0)$ as: $\mu_k(m) = \Gamma_k(m) - \Gamma_k(m-1)$.

Step 8. $\hat{z}_k(m)$ using the (1); further, transmit the data packets to the proximate node.

$m = m + 1$

End step 5 (while statement).

In the case of secure DA, node k in the PNA-SDA model only sends the sequence i.e. $\hat{z}_k(m)$ where $m = 0.1$ to the proximate nodes; further, in case of each data packets of $\hat{z}_k(m)$ there is additional data $\mu_k(0)$ which is added to $z(m)$. Thus, any external node or apart from the proximate node, other nodes will not have any kind of information. Further, when k is greater than or equal to 1, then $\hat{z}_k(m)$ is updated and it will be different from the initial state since each update comprises the averaging process from the information through the proximate nodes. Thus, for all $k \in P_k$, the information set for the available node i at given iteration m is given as (7).

$$K_k(m) = \{z_k(0), \hat{z}_k(0), \dots, z_k(m), \hat{z}_k(m); \hat{z}_k(m) \text{ for all } l \in P_k\} \quad (7)$$

In (1), packets of node i along with proximate node output are included in:

$$K_k(m); \text{ also } K_k(\infty) = \lim_{m \rightarrow \infty} K_k(m).$$

Once the mathematical model is designed and security is analyzed, then PNA-SDA is evaluated in the next section of the research.

3. PERFORMANCE EVALUATION

In this section of the research, we evaluate the PNA-SDA model; moreover, the PNA-SDA model is evaluated through designing the specific network parameter given in the Table 1. Furthermore, evaluation is carried out on the Windows 10 platform using the visual studio 2017 integrated development environment (IDE) using the sensoria simulator; moreover, system architecture follows the 8 GB of Cuda enabled Nvidia RAM and 1 TB of a hard disk. Furthermore, a sensoria simulator is used for the simulation.

Table 1. Network parameter and value

Network parameter	Value
Sensor nodes	50
Initial energy	0.05 joule
Compromised nodes induced	20%, 40%, and 60%

3.1. Energy consumption

Energy plays an important role in network lifetime; thus, we adopt suitable DA, which can optimize the energy consumption. Figure 2 depicts the energy consumption considering the various percentage of dishonest nodes. In the case of 20% dishonest nodes, the average energy consumption is 0.00712 mj, for 40% dishonest nodes energy consumed is 0.07709 mj. Similarly, in the case of 60% of nodes, the average energy consumption is 0.008189 mj.

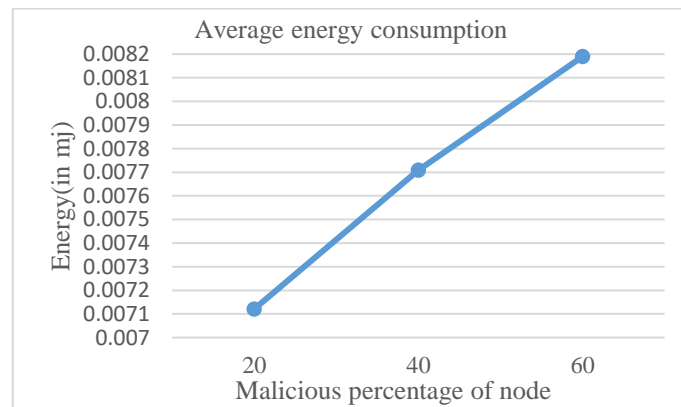


Figure 2. Energy consumption

3.2. Packet identification rate

In general, considering the secured DA, the network model comprises two distinctive types of nodes i.e. sincere nodes and compromised nodes. Thus, compromised nodes have the compromised packet. Packet identification rate is one parameter that identifies the correct node identification. Figure 3 shows correct packet identification comparison with the existing model through varying the percentage of compromised nodes.

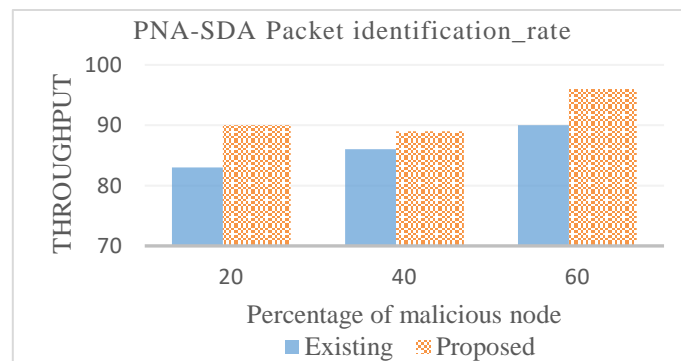


Figure 3. Packet identification rate

Moreover, in the case of 20% compromised nodes, the existing model achieves the packet identification of 83 whereas the PNA-SDA model achieves an identification rate of 90. In the case of 40% compromised nodes, the existing model identifies 86 correct packets whereas the PNA-SDA model identifies 89 packets. Similarly, for 60% of compromised nodes, existing model identifies 90 packets whereas the PNA-SDA model identifies 96 packets.

3.3. Throughput

A general definition of throughput is the rate at which work is being done; it is one of the primary parameters that is considered to prove the model efficiency. Figure 4 shows the throughput comparison of the existing and PNA-SDA model by varying the number of compromised nodes (in percentage). Thus, in case of 20% nodes, throughput of existing model is 0.5395 whereas PNA-SDA model gets the throughput value of 0.585, similarly in case of 40% compromised nodes, existing model achieves the throughput of 0.3182 whereas PNA-SDA model gets throughput of 0.3293. At last, for 60% compromised nodes, existing model gets throughput of 0.189 and PNA-SDA model gets throughput of 0.2016.

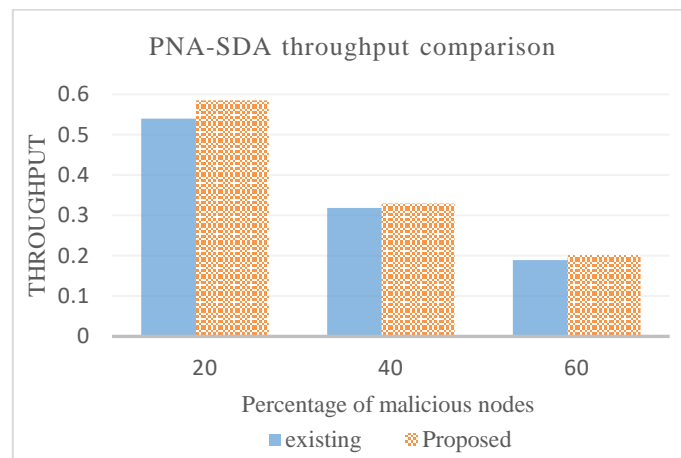


Figure 4. Throughput comparison

3.4. Average deceased nodes

Nodes are primary components of WSN; however, number of alive nodes makes model more efficient and it further increases the network lifetime, as less energy is required for the data transmission. Figure 5 shows the average number of deceased node in network with various percentage of compromised nodes. In case of 20% nodes, average node deceased is 0.03. Similarly, for 40% and 60% of compromised node, deceased nodes are 0.21.

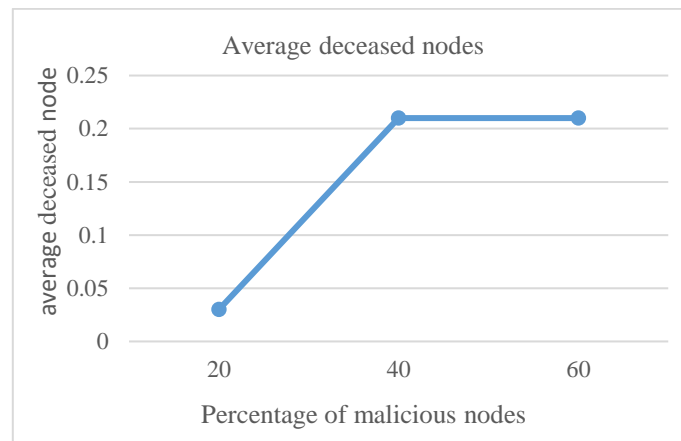


Figure 5. Average number of deceased node in the network

3.5. Comparative analysis and discussion

In this section, we present the improvisation of PNA-SDA model over the existing model considering the security and model efficiency as primary concern. Table 2 shows the improvisation of PNA-SDA model over the existing model considering the packet identification. Moreover, considering other parameters like average deceased nodes we observe that only 0.03 nodes fails on an average for 20% compromised nodes and in case of 40% and 60% only 0.21 nodes fails to survive the network.

Table 2. Improvisation observed for correct packet identification

Percentage of compromised nodes	Improvisation observed
20%	15.66%
40%	3.48%
60%	6.66%

4. CONCLUSION

WSN generates a huge range of application-based data; moreover, these data require processing and transmission to the base station. Meanwhile, since WSNs are resource constrained, efficient data processing and energy conservation is the primary challenge. However, these issues can be tackled through DA which helps in avoiding redundancy and increasing the network lifetime; furthermore, security has been a major constraint, thus this research work designed a novel mechanism named PNA-SDA which aims at secure and efficient DA by adding the additional data and proximate node monitoring. In order to evaluate model efficiency, average energy consumption and deceased node were considered on 20%, 40%, and 60% compromised nodes; also, from the security, perspective packet identification parameter is evaluated along with a comparison with an existing model. Comparative analysis indicates the improvisation of 15.66%, 3.48%, and 6.66% of improvisation in comparison with the existing model on 20%, 40%, and 60% compromised nodes in respective manner. Although PNA-SDA outperforms the existing model, there are other parameters like packet misclassification, node identification need to be evaluated which would be carried out in future work.





REFERENCES

- [1] Y. Jin, K. S. Kwak, and S.-J. Yoo, "A novel energy supply strategy for stable sensor data delivery in wireless sensor networks," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3418–3429, Sep. 2020, doi: 10.1109/JSYST.2019.2963695.
- [2] W.-K. Yun and S.-J. Yoo, "Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks," *IEEE Access*, vol. 9, pp. 10737–10750, 2021, doi: 10.1109/ACCESS.2021.3051360.
- [3] T. H. Kim, C. Ramos, and S. Mohammed, "Smart city and IoT," *Future Generation Computer Systems*, vol. 76, pp. 159–162, 2017, doi: 10.1016/j.future.2017.03.034.
- [4] K. Cengiz and T. Dag, "Energy aware multi-hop routing protocol for WSNs," *IEEE Access*, vol. 6, pp. 2622–2633, 2017, doi: 10.1109/ACCESS.2017.2784542.
- [5] J. Huang, Y. Hong, Z. Zhao, and Y. Yuan, "An energy-efficient multi-hop routing protocol based on grid clustering for wireless sensor networks," *Cluster Computing*, vol. 20, no. 4, pp. 3071–3083, 2017, doi: 10.1007/s10586-017-0993-2.
- [6] P. Guo, J. Cao, and X. Liu, "Lossless in-network processing in WSNs for domain-specific monitoring applications," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2130–2139, 2017, doi: 10.1109/TII.2017.2691586.
- [7] S. A. Putra, B. R. Trilaksono, A. Harsoyo, and A. I. Kistjantoro, "Multiagent system in-network processing in wireless sensor network," *International Journal on Electrical Engineering and Informatics (IJEI)*, vol. 10, no. 1, pp. 94–107, 2018, doi: 10.15676/ijeii.2018.10.1.7.
- [8] J. Cui, L. Shao, H. Zhong, Y. Xu, and L. Liu, "Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 5, pp. 1022–1037, 2018, doi: 10.1007/s12083-017-0581-5.
- [9] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7204–7212, Oct. 2021, doi: 10.1109/TII.2020.3035006.
- [10] J. Girao, D. Westhoff, and M. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," *IEEE International Conference on Communications*, vol. 5, no. May, pp. 3044–3049, 2005, doi: 10.1109/icc.2005.1494953.
- [11] C. Castelluccia, A. C. F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 5, no. 3, pp. 1–36, 2009, doi: 10.1145/1525856.1525858.
- [12] N. K. Prema, "Efficient secure aggregation in VANETs using fully homomorphic encryption (FHE)," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 434–442, 2019, doi: 10.1007/s11036-018-1095-y.
- [13] Y. Zhang, Q. Chen, and S. Zhong, "Efficient and privacy-preserving min and kth min computations in mobile sensing systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 9–21, 2017, doi: 10.1109/TDSC.2015.2432814.
- [14] T. W. Chim, S. M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, 2015, doi: 10.1109/TDSC.2014.2313861.
- [15] J. H. Cheon *et al.*, "Toward a secure drone system: flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, 2018, doi: 10.1109/ACCESS.2018.2819189.
- [16] G. Acs and C. Castelluccia, "DREAM: differentially private smart metering," *Computing Research Repository*, pp. 1–29, 2012.





- [17] H. J. Ding, Z. X. Wang, R. B. Wu, and Q. C. Zhao, "Enhancing the security of multi-agent networked control systems using QKD based homomorphic encryption," *Proceedings of the IEEE Conference on Decision and Control*, vol. 2018-December, pp. 2080–2084, 2018, doi: 10.1109/CDC.2018.8619432.
- [18] K. Kapusta, G. Memmi, and H. Noura, "Additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended wireless sensor networks," *Annales des Telecommunications/Annals of Telecommunications*, vol. 74, no. 3–4, pp. 157–165, 2019, doi: 10.1007/s12243-018-0684-x.
- [19] Y. Su, Y. Li, J. Li, and K. Zhang, "LCEDA: lightweight and communication-efficient data aggregation scheme for smart grid," *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15639–15648, 2021, doi: 10.1109/JIOT.2021.3074503.
- [20] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said, and A. Tolba, "Multifunctional and multidimensional secure data aggregation scheme in WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2657–2668, Feb. 2022, doi: 10.1109/JIOT.2021.3077866.
- [21] S. Lata, S. Mehfuz, and S. Urooj, "Secure and reliable WSN for internet of things: challenges and enabling technologies," *IEEE Access*, vol. 9, pp. 161103–161128, 2021, doi: 10.1109/ACCESS.2021.3131367.
- [22] D. Thomas, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay, "SEC 2: a secure and energy efficient barrier coverage scheduling for WSN-based IoT applications," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 622–634, Jun. 2021, doi: 10.1109/TGCN.2021.3067606.
- [23] A. Ullah, M. Azeem, H. Ashraf, N. Jhanjhi, L. Nkenyereye, and M. Humayun, "Secure critical data reclamation scheme for isolated clusters in IoT-enabled WSN," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2669–2677, Feb. 2022, doi: 10.1109/JIOT.2021.3098635.
- [24] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.
- [25] M. Alotaibi, "Improved Blowfish algorithm-based secure routing technique in IoT-based WSN," *IEEE Access*, vol. 9, pp. 159187–159197, 2021, doi: 10.1109/ACCESS.2021.3130005.

BIOGRAPHIES OF AUTHORS



Sushma Priyadarshini     working as an assistant professor in the Computer Science and Engineering Department of Kallerawan Charitable Trust Engineering College, Gulbarga with experience of 19 years of teaching and a Ph.D. in the area of the wireless sensor network. She had a workshop and faculty development program (FDP) area of interest in computer networks and cloud computing. She can be contacted at email: sushmapriyadarshini12@gmail.com.



Dr. Asma Parveen     got graduated in electrical engineering, in 1993 and completed post-graduation in computer science and engineering in 2004 and in 2016. She was awarded Ph.D. in computer science and engineering. She has published many research papers in leading international journals and conference proceedings. She can be contacted at email: drasma.cse@gmail.com.