Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

Strategies For Secure Data Aggregation in Wireless Sensor Networks and Optimization Issues: A Comprehensive Survey

Ganesh Srinivasa Shetty
Research Scholar, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India
And
Assistant Professor, Department of Electronics and Communication Engineering, Shri Madhwa Vadhiraja Institute Of Technology, Bantakal, India, ganeshshetty27@gmail.com Orchid ID: 0009-0007-5165-3326

Dr. Raghu N
[2]Associate Professor, Department of Electrical Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India, raghu1987n@gmail.com Orchid Id: 0000-0002-2091-8922

Dr. Ganesh Aithal
Vice Principal, Department of Electronics and Communication Engineering, Shri Madhwa Vadiraja Institue of Technology, Udupi, Karnataka, India, viceprincipal@sode-edu.in Orchid Id: 0000-0003-2777-9897

Raghunatha
[4]Assistant Professor, Department of Electronics and Communication Engineering, Shri Madhwa Vadhiraja Institute Of Technology, Bantakal, India, raghunathmd@gmail.com Orchid Id: 0009-0007-8108-6000

***Corresponding Author:** Ganesh Srinivasa Shetty
*Research Scholar, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India
*****Assistant Professor, Department of Electronics and Communication Engineering, Shri Madhwa Vadhiraja Institute Of Technology, Bantakal, India, ganeshshetty27@gmail.com Orchid Id: 0009-0007-5165-3326

Abstract
Recent improvements to wireless sensor networks (WSNs) have led to new ways to use them, such as for surveillance and monitoring the environment. The energy that SNs use to send and receive data is a disproportionately large part of the total energy that the network uses. Data aggregation methods, on the other hand, can cut down on energy use by preventing unnecessary data from being sent back to the sink node. It is very important to protect the privacy of personally identifiable information when it is being gathered and sent over a network, because nodes can be changed by what is around them. As a result, researchers are increasingly interested in finding data aggregation strategies that reduce redundant data while still providing assurance of security. In this paper, we will look at the various security measures that may be taken while aggregating data using WSN. Despite WSNs' impressive task-handling capabilities, it is challenging to strike a balance between competing priorities such as long network life, low-latency transmissions, wide coverage, and low packet loss. In addition, this study provides a brief overview of the multi-objective optimization (MOO) approach, which is being used to solve contemporary research issues in WSN with competing objectives.

Keywords: Data Aggregation, Attacks, Confidentiality, Security, Network Optimization

1. Introduction

The invention of wireless sensor networks (WSNs) was one of the most important things to happen in the 21st century. WSNs have been a godsend for modern technology because they make it possible to get data from sensors in different parts of the world about a wide range of environmental phenomena [1]. Their uses in fields like ecosystem tracking, climate prediction, and military surveillance are vast. Due to their compact size, sensor devices have limited storage, weak processing capabilities, and limited power supplies, all of which negatively impact the network [2]. According to the findings, the transmission of data rather than the processing of data consumes the majority of the energy of small nodes. Hence, reducing the amount of communication among WSN nodes is crucial [3]. Yet, the communication burden is increased due to redundant data sensing and transmission due to the dense placement of sensor nodes (SNs). Data aggregation is a method that combines many data packets containing unnecessary information into a single, streamlined packet in order to reduce or eliminate duplicate data [4].

WSNs are made when tens to thousands of SNs that can sense, communicate wirelessly, and do calculations are spread out in an unsupervised environment. These nodes can send and receive data wirelessly and also do sensing and computing tasks [5]. The Internet of Things (IoT) relies heavily on WSNs today. Advantages of the IoT include increased situational awareness, smarter data processing, and more secure data transmission on a global scale. Realizing the information exchanges between a

human and a gadget is crucial [6]. The three main components of an IoT application are the "perception," "network," and "application" layers. The network and application layers are deployed using high-power devices, whereas the perception layer is deployed using a low-power WSN to protect sensitive information [7]. WSNs maintain network functionality by modeling topology and updating the routing table at the perception layer using several different protocols. After then, the WSN will begin gathering information from various sources before sending it on to the edge router, as seen in Figure 1.

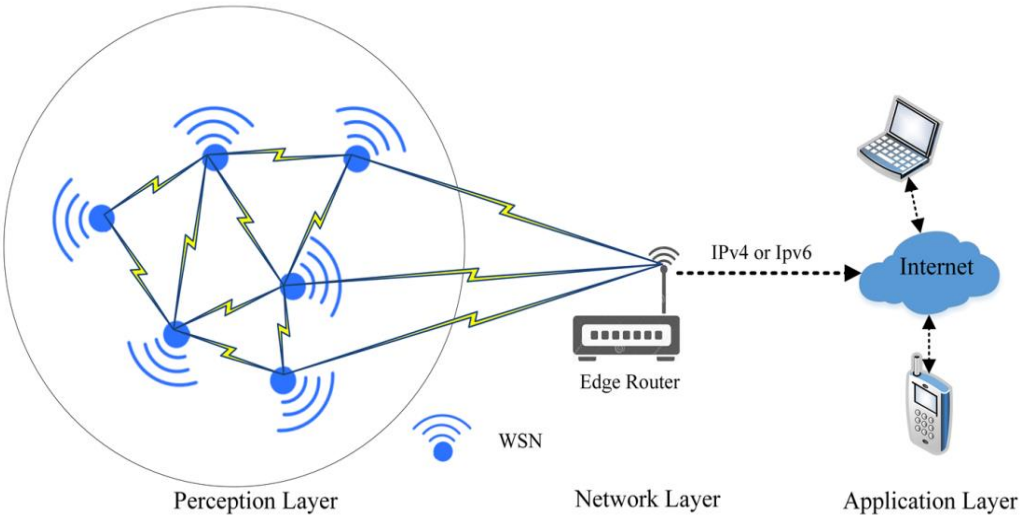

Figure 1: Layer-to-Layer Interactions in a WSN.

Once the data has reached its final destination, it must be put together in a way that meets the performance criteria and security standards for WSN activities. In this network, sensor nodes communicate with other nodes, such as aggregators, to share data. As can be seen in Figure 2, each individual aggregator will collect the data and send it in a unified fashion. The ability to compile relevant data into a cohesive whole is what we mean when we talk about aggregation. Communication between sensor nodes, collection nodes, and the Sink uses a lot of power [8].

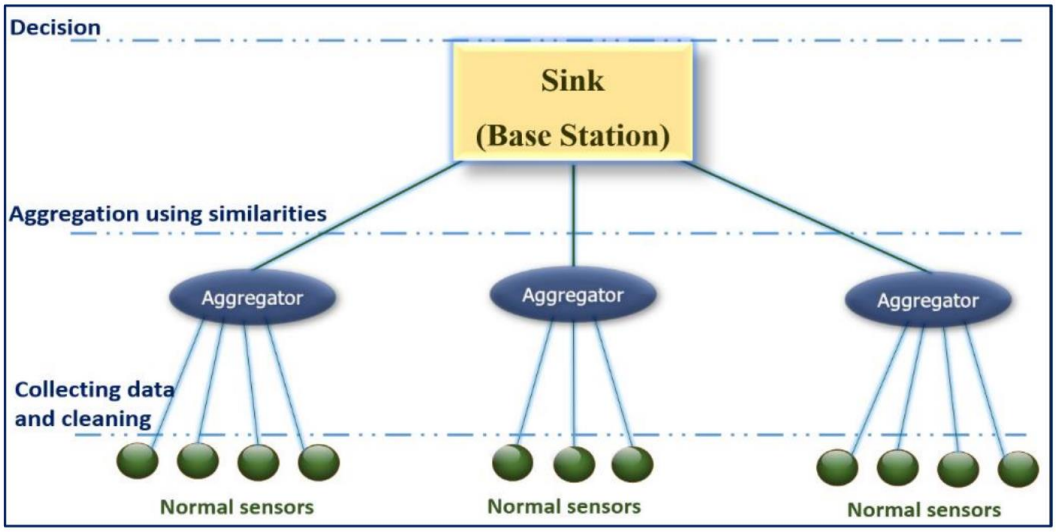

Figure 2: Data Aggregation in WSN.

A lot of research into the security challenges of WSN management protocols is focused on the "Triangle" of privacy, integration, and authentication. Keeping sensitive information secret while in transit between WSN nodes is what we mean by "confidentiality." Under the integrity condition, the network must be ready to stop attackers from changing messages. Disruption beams can modify an assault's poles. Availability completes the triangle of safety requirements. "Available" means that the WSN Services may be accessed whenever necessary. Attackers can disable essential network services or even wipe out the network entirely [10]. While the denial of service (DoS) attack affects all levels, other

malicious assaults are exclusive to each layer (Figure 3).

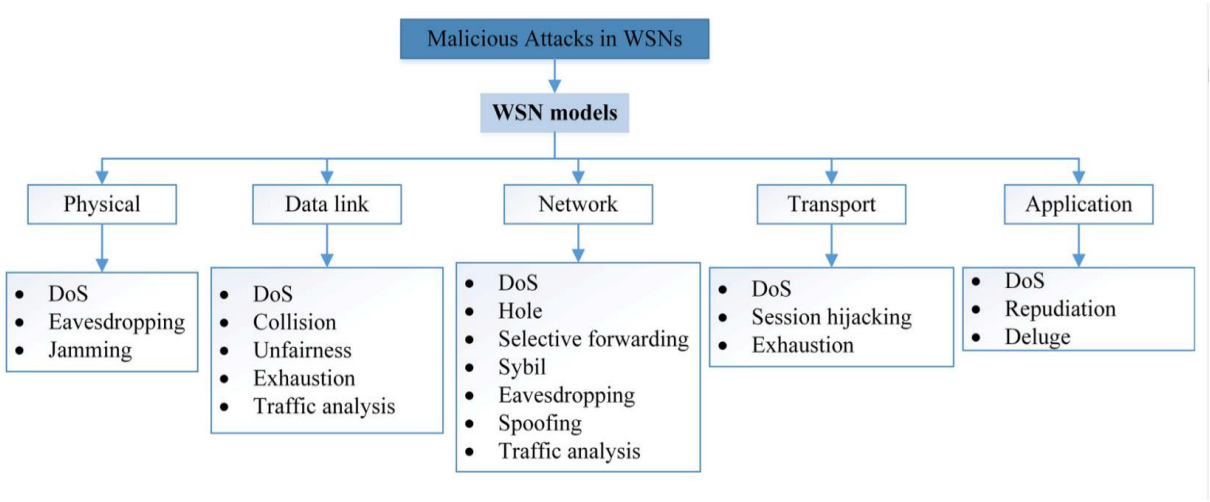

Figure 3: The Categorization of Malicious Attacks.

Even though these levels are similar, they each do something a little different to make sure that data management and transmission within a network are secure. Many assaults are now aimed at WSNs. Every day, these assaults get more powerful [11].

2. Prerequisite for Security

In WSNs, information packets can only be sent and received using real SNs. In WSNs, it is well known that wireless communication channels are used. As a result, there is a risk of data corruption during transmission between SNs as a result of data loss, information leakage, or malicious activity on the part of the attacker [12, 13]. Consideration of security needs in WSNs is essential for shielding data packets from a variety of threats, as seen in Figure 4.

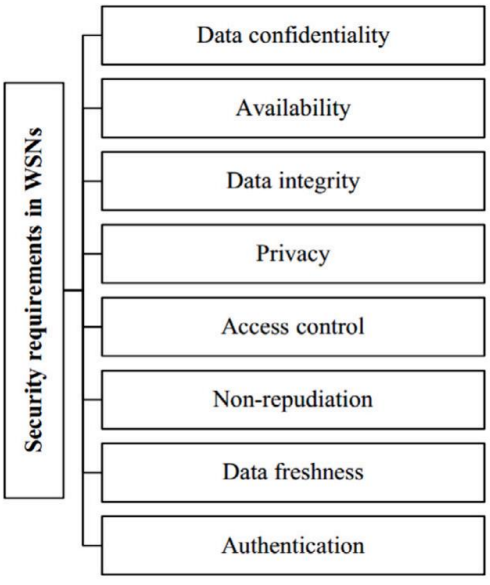

Figure 4: Prerequisite for Security in WSN

The network's data and services must always be available. Availability is defined as the average percentage of time that SNs are doing their main job [14]. Invalid nodes are prevented from accessing private data by data confidentiality safeguards. Data secrecy guarantees that the contents of data packets sent and received between SNs and the base station are not revealed in the distributed environment [15]. A legitimate sender node may be confirmed, giving the recipient confidence. The authentication procedure is the first line of protection against potential threats to a network [16]. The "data freshness" property [17] guarantees the use of only brand-new, never-before-used data packets. With the assurance of non-repudiation, the validity of the claims is beyond dispute. Using a legal concept called "non-repudiation," those with knowledge of information security may verify the authenticity of data and ensure that it has not been altered [18].

2.1. A few severe threats to WSN Security

Most WSNs are vulnerable to several assaults since they are usually set up in unprotected locations. WSN routing is data-centric because of its ad hoc nature. As a result, there is a probability that attackers may intercept data en route to the base station by keeping an eye on the communication connection and carrying out other potentially dangerous operations. The most typical assaults against WSNs will be described here.

a) Black hole attack: The availability criterion is being actively threatened by an external threat. Some nodes, known as black holes, boast of having free paths. As a result, benign nodes in the vicinity must send their traffic via the malicious SNs [19, 20].
b) Sinkhole attack: Similar to a black hole attack, except the attacker already knows where the sink

node is. As the malicious node here is attempting to persuade all SNs to choose it as next-hop to approach the sink node, this attack is more hazardous and destructive than a black hole attack [21].

c) Wormhole attack: Two hostile nodes collaborate in order to set up a wormhole channel between them, making this an active and external threat which poses a danger to the availability requirements. A threat hacker can eavesdrop on SN conversations, steal sensitive data, and alter network flows [22].
d) Sybil attack: An assailant steals a number of legitimate IDs from the system. The Sybil node may become the next-hop for data transmission if other SNs believe it to be a neighbour. The goal of this attempt is to trick the system into thinking it is receiving legitimate data packets, which will then cause the network to crash [23].
e) Flooding attack: As the target node maintains data linked to the connection request, the malicious node repeatedly makes this request, overwhelming its memory. The SNs memory is therefore at capacity, and it is unable to respond to genuine queries [24].

3. Data Aggregation and Security Concerns in WSN

As data transmission is the main energy consumer in WSNs, researchers have concentrated their efforts there. Effective routing protocols and mobility sinks have been made to cut down on the amount of data that needs to be sent [25]. Redundant data results from the typically dense deployment of SNs. This has a significant impact on how much bandwidth is used for transmissions. As a result, it is crucial for wireless sensor networks to employ data aggregation, which lessens the amount of transmission needed by combining data that is already available. Additionally, because of the lack of physical protection and monitoring and the unreliable transmission medium, sensor nodes installed in hostile distant locations are vulnerable to man-in-the-middle attacks [26]. Thus, privacy-protecting methods are required.

Witness-based studies [27] speculate on the possibility of using a data fusion node. All of a node's white-box data validation (WDA) is sent to the same-cluster information repository (base station). Witness nodes collect the data at the base station but don't broadcast the results, and each of those nodes must provide proof by computing the result's message authentication code (MAC). By postponing assembly and validation at higher levels, secure data aggregation (SDA) provides a measure of flexibility against node leveling, hence solving the problem of data collection in the event of a compromised node [28]. As a result, sensor readings are relayed unaltered and combined in the subsequent hop rather than the initial one.

The data's veracity is at risk if any of the two higher-ups in the hierarchy is corrupted. If no action is taken to mitigate the damage caused by a hacked node's discovery, data availability in the system would suffer. Using efficient safe aggregation (ESA) [29], after the grandpa's node discovers that it has been hacked, it cannot be certain that the dishonest node is the child's node. Because of the nature of the sole communication line with numerous hops, communication loss is more likely to occur in a network topology in which the nodes are organized as a tree. The existence of a unique route also precludes the nodes from flexibly switching roles with one another [30]. In [31], the authors solve the issues with both tree and cluster topologies by dividing the network into layers, with each layer consisting of nodes that are a certain hop distance from the network's origin.

Several approaches strive to identify corrupted nodes throughout data aggregation, making them resistant to DoS attacks, whereas the vast majority rely on detecting an intermediary node altering a partial aggregate result [32]. [33] Presented a modification to SDA that would allow for the identification of malicious nodes through the use of statistical anomaly detection and random grouping of nodes. Their strategy is useless when a hacker adapts its behavior to comply with statistical detection guidelines. In order to maintain secrecy between hops, the encrypted data must be decrypted and aggregated at each hop. By gaining access to the aggregator node, an intruder can unwrap an encrypted packet and get access to the contents contained inside. The real data is shielded from potential hackers by being chopped up into smaller parts. Utilizing privacy homomorphism (PHM), a novel method for concealing data was proposed, in which an aggregation function would be used on encrypted data rather than plain data [34]. Intruders positioned along the path to the sink node can falsify encrypted data using privacy homomorphism-based encryption, which guarantees secrecy but is susceptible to mutability attacks. Utilizing a shared complete symmetric state key among the sink node and the SNs, a safe additive homomorphic aggregation approach was suggested [35]. It uses an asymmetric key generated by the elliptic curve cryptosystem (ECC) to ensure the safe transfer of the state's entire key. Using homomorphic encryption, this system provides fool-proof authentication, complete data concealment, and collective integrity of data. All of the systems we've discussed so far reject the whole aggregated value, including any legitimate data, if the collective integrity verification fails.

People in the fields of automated control and signal processing have paid a lot of attention to consensus as a key strategy for distributed computing. An

average consensus algorithm is a key part of the distributed aggregation process. It lets each node figure out on its own what the average state of all the nodes is. Y. Wang [36] came up with an innovative method called Privacy Preservation Average Consensus (PPAC) to solve the problem of average consensus while protecting the privacy of each person. Table 1 gives the comparison of data aggregation approaches published prior to this date.

Table 1: Comparison of data aggregation approaches

Reference	Issues	Methodology	Pro's	Con's
[24]	Affirmation of data fusion	polling and witness-based techniques to verify the data hub	Public expenditures for the recommended technique are negligible, and the number of predicted surveys is fewer than the number of witnesses in a hostile environment.	not providing secrecy and freshness
[27]	reducing overhead associated with communication and power use.	Secure Data Aggregation	decreases the time and effort required for communication	Poor resilience to node and connection failures
[31]	Power usage and reliability	order- and duplicate insensitive	As it employs ring topology, it is robust in the face of connectivity and linking failures	fails to address the issue of misleading sub-aggregate values
[34]	concealing data	privacy homomorphism	Data privacy and usability are no longer mutually exclusive	networks cannot run ad-hoc
[36]	Energy usage	Cluster based	Improved performance, especially in terms of accurate data aggregation, and enhanced privacy and efficacy in communication	not employ methods that protect confidentiality
[37]	distributed denial-of-service	consensus blockchain technique	efficient in terms of time consumption and problems associated with memory utilization	A misstep or a tweak that has to be made is difficult to undo.
[38]	data integrity	Slice-Based SDA	check the integrity of each SN separately	Increased number of hops
[39]	DoS attack	Authenticated Encryption with Associated Data	energy efficient	Network delay

4. Data Aggregation Optimization

Several practical optimisation issues fall under the category of NP-hard problems because they are notoriously difficult to solve optimally using algorithms in polynomial time. For NP-hard tasks, we have both precise algorithms and approximation algorithms to choose from. Appropriate algorithms for NP-hard issues aim to produce good approximations of the ideal solution in less time than required by exact algorithms. WSN efficiency is determined by how well the hardware is built and optimised. Strong network connection and high data transmission rates can only be ensured if lifespan and coverage are maximised while energy demand and the quantity of nodes are minimised. One of the main problems with the standard approaches is that they only look at one possible optimization parameter.

Thus, multi-objective optimization (MOO) approaches have been evolved to deal with such circumstances, where many objectives of the WSN are dealt with correspondingly with a number of additional restrictions [40]. Because of the short battery life of individual SNs, it is essential that they work together to maximize both the longevity of their networks and the breadth of their coverage. WSN is presented in an adaptable, energy-managing, self-organizing, application-focused, energy-preserving, and communication-restricted fashion using a MOO strategy.

4.1. Optimization Techniques

Optimization techniques for WSN usage is discussed below:

a) Adaptive Design Optimization

Several aspects of a network's performance can benefit from the application of genetic algorithms (GAs) in optimization. One of GA's defining features is the ability to monitor SNs health. GA's method for producing the best SN possible in order to meet specialised needs for various applications, power-saving functions, and network connection [41].

The authors of [42] suggest a routing protocol, a hybrid of the LEACH and Micro Genetic algorithms. As compared to previously used protocols, this approach improves cluster head (CH) selection while also decreasing the network's overall energy usage. All the nodes are assumed to be static and homogeneous in the multi-objective GA technique (M2NGA), which uses more energy during data transfer than radio energy [43]. Due to the tradeoff between energy efficiency and precision, the former cannot be prioritised above the latter. In [44], a CS-based approach for efficient data transfer over WSNs is suggested; this algorithm employs multi-objective GAs to find the optimal combination of measurement quantity, transmission distance, and sensing matrix.

b) Bio-inspired Optimization Techniques
It's difficult to balance broad routing needs with security since several optimisation objects must be taken into account. In practise, it is common to have several objectives that all need to be reduced or maximised at the same time in an optimisation issue. For WSN routings, multi-objective optimisation routing algorithms based on ant colony optimisation (ACO) have received much research [45]. To optimise a problem, Particle Swarm Optimization (PSO) is a computationally simple, effectual, and functional approach. It's utilised to fix things like node location, data aggregation, perfect placement, and clustering in wireless sensor networks. As comparison to other algorithms, PSO provides superior results in terms of convergence speed, solution quality, and computational efficiency [46].

b) Coverage and Lifetime Optimization
WSNs keep the necessary sensing coverage up and send the data they collect at regular intervals to a central hub. The lifespan might be anywhere between a week and a few months. Since SNs have limited battery life, WSNs have challenges in maintaining network availability and expanding their coverage area. Better coverage and longer network life are achieved with the help of Gaussian distribution [47]. Despite the importance of minimising energy usage to extend network lifespan, the restricted number of relay nodes is sometimes neglected as a barrier. Optimizing network lifespan and relay node count in three-dimensional terrains was analysed in [48].

The suggested technique has dramatically improved performance, as demonstrated by simulations on 3D datasets. The authors of [49] explored the use of relay nodes to create linked topologies in WSNs. They suggested several cutting-edge heuristics including the ones based on Delaunay triangulation and the least spanning tree. An innovative optimum placement technique for relay nodes that minimises energy consumption is suggested in [50]. They suggested using a bee-inspired algorithm to optimise the network's settings and significantly increase its lifespan.

5. Conclusion

The issues of WSNs, data aggregation in WSN, fundamental data aggregation security standards, and a survey and comparison of security techniques were all covered in this research study. As a starting point, we talked about the most important worries about network security in WSNs and the most common ways to attack them. SNs are often placed in dangerous, inhospitable, or remote areas, so there is a high chance that they will be hacked. This review looks at the many attacks on security and the steps that have been taken to stop them. Existing methods are compared with regards to key aspects of security. Because of their limited resources, SNs cannot achieve optimal efficiency without making certain trade-offs in other areas. One of the main problems with traditional optimization methods is that they only look at a single optimization parameter, whereas MOO can look at all of them at once. Finding proactive mechanisms that provide privacy, scalability, and support for many applications with dynamic querying is becoming a pressing research question in the context of WSNs.

References

[1] H. M. A. Fahmy, “Wireless Sensor Networks Essentials,” in Wireless Sensor Networks, Cham: Springer International Publishing, 2020, pp. 3–39. doi: 10.1007/978-3-030-29700-8_1.
[2] D. K. Sah and T. Amgoth, “Renewable energy harvesting schemes in wireless sensor networks: A Survey,” Information Fusion, vol. 63, pp. 223–247, Nov. 2020, doi: 10.1016/j.inffus.2020.07.005.
[3] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, “A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks,” IEEE Commun. Surv. Tutorials, vol. 19, no. 2, pp. 828–854, 2017, doi: 10.1109/COMST.2017.2650979.
[4] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, “Applications of Wireless Sensor Networks: An Up-to-Date Survey,” ASI, vol. 3, no. 1, p. 14, Feb. 2020, doi: 10.3390/asi3010014.
[5] E. Yousefpoor, H. Barati, and A. Barati, “A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks,” Peer-to-Peer Netw. Appl., vol. 14, no. 4, pp. 1917–1942, Jul. 2021, doi: 10.1007/s12083-021-01116-3.
[6] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, “A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges,” in Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, vol. 846, Springer International Publishing, 2020, pp. 197–209. doi: 10.1007/978-3-030-24513-9_12.
[7] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, “A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network,” IEEE Access, vol. 7, pp. 53079–53090, 2019, doi: 10.1109/ACCESS.2019.2911395.
[8] W. Fang, X. Wen, J. Xu, and J. Zhu, “CSDA: a novel cluster-based secure data aggregation scheme for WSNs,” Cluster Comput, vol. 22, no. S3, pp. 5233–5244, May 2019, doi: 10.1007/s10586-017-1195-7.
[9] M. S. Yousefpoor and H. Barati, “Dynamic key management algorithms in wireless sensor networks: A survey,” Computer Communications, vol. 134, pp. 52–69, Jan. 2019, doi: 10.1016/j.comcom.2018.11.005.

[10] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, Jan. 2019, pp. 0475–0481. doi: 10.1109/CCWC.2019.8666557.

[11] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An Improved IDAF-FIT Clustering Based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network," Mobile Netw Appl, vol. 26, no. 3, pp. 1059–1067, Jun. 2021, doi: 10.1007 /s11036-020-01664-7.

[12] M. Keerthika and D. Shanmugapriya, "Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures," Global Transitions Proceedings, vol. 2, no. 2, pp. 362–367, Nov. 2021, doi: 10.1016/j.gltp. 2021. 08.045.

[13] S. A. Jilani, C. Koner, and S. Nandi, "Security in Wireless Sensor Networks: Attacks and Evasion," in 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, Feb. 2020, pp. 1–5. doi: 10.1109/NCETSTEA48365.2020.9119947.

[14] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 1–13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[15] M. Alotaibi, "Security to wireless sensor networks against malicious attacks using Hamming residue method," J Wireless Com Network, vol. 2019, no. 1, p. 8, Dec. 2019, doi: 10.1186/s13638-018-1337-5.

[16] Z. Chen, M. Xu, M. Wang, and Y. Jia, "Joint Optimization of Data Freshness and Fidelity for Selection Combining-Based Transmissions," Entropy, vol. 24, no. 2, p. 200, Jan. 2022, doi: 10.3390/e24020200.

[17] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," Procedia Computer Science, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.

[18] V. Clupek, V. Zeman, and P. Dzurenda, "Light-weight Mutual Authentication with Non-repudiation," RADIOENGINEERING, vol. 27, no. 1, pp. 143–150, Apr. 2018, doi: 10.13164/re.2018.0143.

[19] M. Wazid and A. K. Das, "A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Networks," Wireless Pers Commun, vol. 94, no. 3, pp. 1165–1191, Jun. 2017, doi: 10.1007/s11277-016-3676-z.

[20] D. C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," Cluster Comput, vol. 22, no. S1, pp. 1313–1328, Jan. 2019, doi: 10.1007/s10586-017-1622-9.

[21] G. W. Kibirige and C. Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network". Networking and Internet Architecture, https://arxiv.org/abs/1505.01941v2

[22] N. Tamilarasi and S. G. Santhi, "Detection of Wormhole Attack and Secure Path Selection in Wireless Sensor Network," Wireless Pers Commun, vol. 114, no. 1, pp. 329–345, Sep. 2020, doi: 10.1007/s11277-020-07365-4.

[23] A. Angappan, T. P. Saravanabava, P. Sakthivel, and K. S. Vishvaksenan, "RETRACTED ARTICLE: Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN," J Ambient Intell Human Comput, vol. 12, no. 6, pp. 6567–6578, Jun. 2021, doi: 10.1007/s12652-020-02276-5.

[24] S. Radhika, K. Anitha, C. Kavitha, W.-C. Lai, and S. R. Srividhya, "Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks," Electronics, vol. 12, no. 1, p. 123, Dec. 2022, doi: 10.3390/electronics12010123.

[25] P. Maratha, K. Gupta, and A. K. Luhach, "Improved fault-tolerant optimal route reconstruction approach for energy consumed areas in wireless sensor networks," IET wirel. sens. syst., vol. 10, no. 3, pp. 112–116, Jun. 2020, doi: 10.1049/iet-wss.2019.0152.

[26] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact," IEEE Trans. Inform. Forensic Secur., vol. 9, no. 4, pp. 681–694, Apr. 2014, doi: 10.1109/TIFS.2014. 2307197.

[27] M. Felemban, A. Daghistani, Y. Javeed, J. Kobes, and A. Ghafoor, "A Security and Performance Driven Architecture for Cloud Data Centers." arXiv, Mar. 27, 2020. Accessed: Mar. 27, 2023. [Online]. Available: http://arxiv.org/abs/2003. 12598

[28] X. Liu, X. Zhang, J. Yu, and C. Fu, "Query Privacy Preserving for Data Aggregation in Wireless Sensor Networks," Wireless Communications and Mobile Computing, vol. 2020, pp. 1–10, Feb. 2020, doi: 10.1155/2020/9754973.

[29] A. Aseeri and R. Zhang, "Secure Data Aggregation in Wireless Sensor Networks: Enumeration Attack and Countermeasure," in ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, May 2019, pp. 1–7. doi: 10.1109/ICC.2019.8761889.

[30] C. Regueiro, I. Seco, S. de Diego, O. Lage, and L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," Information Processing & Management, vol. 58, no. 6, p. 102745, Nov. 2021, doi: 10.1016 /j.ipm.2021.102745.

[31] A. A. Agarkar and H. Agrawal, "LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid," Heliyon, vol. 5, no. 3, p. e01321, Mar. 2019, doi: 10.1016/j.heliyon.2019.e01321.

[32] S. S, Y. H K, D. Yogish, and A. N, "Credence Aware Data Aggregation for Wireless Sensor Networks," Journal of Computer Science, vol. 18, no. 4, pp. 297–305, Apr. 2022, doi: 10.3844/jcssp.2022.297.305.

[33] B. Gao, D. Amagata, T. Maekawa, and T. Hara, "Detecting Energy Depriving Malicious Nodes by Unsupervised Learning in Energy Harvesting Cooperative Wireless Sensor Networks," Journal of Information Processing, vol. 28, no. 0, pp. 689–698, 2020, doi: 10.2197/ipsjjip.28.689.

[34] H. E. D. Kang, D. Kim, S. Kim, D. D. Kim, J. H. Cheon, and B. W. Anthony, "Homomorphic Encryption as a secure PHM outsourcing solution for small and medium manufacturing enterprise," Journal of Manufacturing Systems, vol. 61, pp. 856–865, Oct. 2021, doi: 10.1016 /j.jmsy.2021.06.001.

[35] V. Kumar, N. Malik, G. Dhiman, and T. K. Lohani, "Scalable and Storage Efficient Dynamic Key Management Scheme for Wireless Sensor Network," Wireless Communications and Mobile Computing, vol. 2021, pp. 1–11, Jun. 2021, doi: 10.1155/2021/5512879.

[36] Y. Wang, "Privacy-Preserving Average Consensus via State Decomposition." arXiv, Mar. 02, 2019. Accessed: Mar. 27, 2023. [Online]. Available: http://arxiv.org/abs/1902.09576

[37] G. Subathra, A. Antonidoss, and B. K. Singh, "Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme," Security and Communication Networks, vol. 2022, pp. 1–13, Jul. 2022, doi: 10.1155/2022/3167958.

[38] D. Vinodha and E. A. Mary Anita, "Discrete Integrity Assuring Slice-Based Secured Data Aggregation Scheme for Wireless Sensor Network (DIA-SSDAS)," Wireless Communications and Mobile Computing, vol. 2021, pp. 1–17, Jul. 2021, doi: 10.1155/2021/ 8824220.

[39] M. Dener, "SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks," Electronics, vol. 11, no. 24, p. 4194, Dec. 2022, doi: 10.3390/electronics11244194.

[40] M. E. Migabo, K. Djouani, T. O. Olwal, and A. M. Kurien, "A Survey on Energy Efficient Network Coding for Multi-hop Routing in Wireless Sensor Networks," Procedia Computer Science, vol. 94, pp. 288–294, 2016, doi: 10.1016 /j.procs.2016.08.043.

[41] S. Kr. Jha and E. M. Eyong, "An energy optimization in wireless sensor networks by using genetic algorithm," Telecommun Syst, vol. 67, no. 1, pp. 113–121, Jan. 2018, doi: 10.1007/s11235-017-0324-1.

[42] M. Radhika and P. Sivakumar, "Energy optimized micro genetic algorithm-based LEACH protocol for WSN," Wireless Netw, vol. 27, no. 1, pp. 27–40, Jan. 2021, doi: 10.1007/s11276-020-02435-8.

[43] T. Wang, G. Zhang, X. Yang, and A. Vajdi, "Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks," Journal of Systems and Software, vol. 146, pp. 196–214, Dec. 2018, doi: 10.1016/j.jss.2018.09.067.

[44] M. A. Mazaideh and J. Levendovszky, "A multi-hop routing algorithm for WSNs based on compressive sensing and multiple objective genetic algorithms," J. Commun. Netw., vol. 23, no. 2, pp. 138–147, Apr. 2021, doi: 10.23919/JCN.2021.000003.

[45] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks," Applied Soft Computing, vol. 77, pp. 366–375, Apr. 2019, doi: 10.1016/j.asoc. 2019.01.034.

[46] M. Z. Hasan, H. Al-Rizzo, and M. Günay, "Lifetime maximization by partitioning approach in wireless sensor networks," J Wireless Com Network, vol. 2017, no. 1, p. 15, Dec. 2017, doi: 10.1186/s13638-016-0803-1.

[47] F. H. Awad, "Optimization of relay node deployment for multisource multipath routing in Wireless Multimedia Sensor Networks using Gaussian distribution," Computer Networks, vol. 145, pp. 96–106, Nov. 2018, doi: 10.1016/j.comnet.2018.08.021.

[48] N. T. Tam, T. H. Hung, H. T. T. Binh, and L. T. Vinh, "A decomposition-based multi-objective optimization approach for balancing the energy consumption of wireless sensor networks," Applied Soft Computing, vol. 107, p. 107365, Aug. 2021, doi: 10.1016/j.asoc.2021.107365.

[49] F. Senel and M. Younis, "Novel relay node placement algorithms for establishing connected topologies," Journal of Network and Computer Applications, vol. 70, pp. 114–130, Jul. 2016, doi: 10.1016/j.jnca.2016.04.025.

[50] H. A. Hashim, B. O. Ayinde, and M. A. Abido, "Optimal placement of relay nodes in wireless sensor network using artificial bee colony algorithm," Journal of Network and Computer Applications, vol. 64, pp. 239–248, Apr. 2016, doi: 10.1016/j.jnca.2015.09.013.