Review on secure data aggregation in Wireless Sensor Networks

Mohammed Salah Abood¹, Hua Wang (王华)¹, Hussain Falih Mahdi², Mustafa Maad Hamdi³ and Ahmad S. Abdullah⁴

¹ School of Information and Electronics, Beijing Institute of Technology, Haidian District, Beijing 100081, China
² Computer Engineering Department, Faculty of Engineering, University of Diyala, Baquba, Diyala Province, Iraq.
³ Department of Computer Engineering Techniques, Al-Maarif University College, Al-Anbar, Iraq.
⁴ Department of Communications, College of Engineering, University of Diyala, Baqubah, Iraq.

E-mail: Mohammedsalah81@gmail.com

Abstract. Recent advances in wireless sensor networks (WSNs) have inspired various new applications, including target tracking and monitoring of ecosystems. Nevertheless, a large amount of data energy consumption of WSNs is utilized by data communication. However, data aggregation techniques can eliminate redundant data being transferred back to the base station and thereby lessening the consumption of energy. Security features like data integrity, confidentiality and accumulation of latest data is of great importance if WSN is utilized in extremely hostile or remote settings whereby the sensors are vulnerable to node failure and breach. Currently, there is prospect for securing data aggregation using WSN. In light of this, security features in data aggregation using WSN will be examined in current study. Next, the adversarial model that can be used in any aggregation scheme is then evaluated. Moreover, the latest and most sophisticated secured data aggregation scheme, proposed will be examined and categorized into two groups which are classified according to the number of aggregator nodes and the existence of the verification term. In this paper, created a table that showed the advantages and limitations of each algorithm that was adopted by researchers, shown in Table 3. Last, a computational approach is recommended to build a modern design with minimal protection preconditions against various types of challenges. The conceptual framework aims to provide an advanced understanding and enable the process of evaluation.

Keywords. Data Aggregation (DA), Attack, (WSNs), Sensor Node

1. Introduction

WSNs consist of a large number of small sensor nodes scattered around a specific geographical area. While the growing node is low power for any computer that combines computing and wireless networks in addition to the capabilities of the sensor [1]. After the sensor nodes are deployed in a certain way to build a strong network provide reports to a SINK. WSNs have limited power supplies as well as batteries, which means that the sensor nodes don’t recharge. When put the nodes of sensor in a hostile
environment then the nodes can be made compromised by attacks, where will allow to the Opponents controlling on the deployment area. In multi-hop networks the processing is done in (intermediate/aggregator) node, the data from its child nodes are then aggregated by executing the aggregation function like SUM, MAX, MIN, and etc. Then sends the results to the upper level of node or sends to the SINK [2]. The purpose of data aggregation (DA) and security is essential for WSNs, the main problem for researchers was to find more secure for data aggregation. DA is an important primitive for processing, combining and summarizing data packets from serval sensor nodes before transferring these packets to the upper nodes [3-5]. The data collected will therefore be isolated from all sensor nodes, data collected from all sensor nodes that you did not need or redundant, and will be linked to large sensor networks and data collected from all the sensor nodes you need and will summarize the data at a sensor node [6]. Then send those data to the base station which led to rationalization of energy consumption. So, data aggregation is very suitable to rationalization of energy consumption and provision of valuable information’s to the base station [7, 8]. So, after study and viewing, especially with expansion of Internet and its importance, types and number of other attacks which also grown. Observed presence of a large exhaustion of energy when there are communications between all nodes, which is considered one of the most important challenges facing this study. In other words, low connectivity in the wireless networks is a daunting problem with irregular sensor node densities. Owing to these threats, specific security issues will be addressed at data aggregation (DA). Therefore, energy efficiency is improved and prolong the wireless network lifetime then the secure DA schemes are categorized. Last, put an end to the end of the aggregation, which represents our main goal in this study. In other word, wireless sensor network analysis and data collection and security of major and important data in WSNs through use public and symmetric keys.

In data aggregation for WSN functions, performance measures are explained with security requirements [9]. Data need to be aggregated while it is being transmitted to its final destination (SINK). It forms a network whereby the sensor nodes send values to specific nodes for example, aggregators. Individual aggregator will then consolidate the data before transmitting it as shown in Figure 1. There are two levels in the Data Aggregation methodology used in this study. The first is local aggregation at the nodes level and the second level is at the aggregator's level. At each period p, each node will send its aggregated set of data to its legitimate aggregator which aggregates all data received from various sensor nodes and transmits them to the SINK [10]. Aggregation is defined as "the capacity to summarize information". Lots of energy is consumed during communication between sensor nodes, collector nodes and SINK.

![Figure 1. Data Aggregation Scheme [9].](image-url)
1.1. Functions and Requirements for Data Aggregation
DA function is the process of combining data from multiple sensor nodes in wireless sensor networks using any aggregation functions such as minimum, maximum, aggregation, intermediate and other aggregation nodes [11, 12]. The data security requirements for WSNs are similar to those for classic wired and wireless networks. There are however some unique specifications that can be found only in WSNs. Security requirements for data aggregation are therefore: data integrity, data confidentiality, availability of data, data freshness, non-repudiation, accuracy and authentication [13-16].

1.2. Performance measure of Data Aggregations
- Energy Efficiency: If the network functions are maximized, the DA scheme would be energy efficient.
- Operation time.
- Communications Energy: To assess the performance of the schemes proposed.
- Execution time includes aggregation time and processing time and energy costs include assembly and calculation energy.

Since SINK has a high energy content compared to normal nodes, it do not allow SINK energy depletion to determine energy costs. The assessment of energy costs is based on the energy model identified in [17, 18].

In summary, will show the treatment of data aggregation in wireless sensor network. In WSNs, will discuss expected attacks which threaten secure DA schemes, then sorting and comparison of current Secure DA schemes (DAS), in this study will present and discuss (single/multiple) aggregator scheme with comparison of secure aggregation schemes, in this part will classify the single and multiple aggregator scheme to two type for each (verification and no verification phases). Finally, will explain almost type with strengths and limitations for each from side description of Current Schemes and framework for evaluation new schemes. The conclusion and vision will be presented in the last part of this study.

2. Related work
The problem of data aggregation in wireless sensor network has been tackled by numerous researchers. Many recent review articles were done in this topic. The researchers in [19] considers Witness-based Data fusion node. Ensure (WDA) for one clustering system the validation of data generated from a node aggregated to SINK (base station). In order to validate the data, the aggregation nodes must provide evidence from a number of witness nodes which, in turn, collect the data at the base station but without transmitting the results, where the message authentication code (MAC) for the result is calculated by each node of the above-mentioned witness nodes. Next, the witness node forwards it to the aggregator node which then send the evidence to the base-station. WDA provides integrity features for data aggregation security [20]. It sends many copies of the report to the aggregator point which are close to the aggregate value of the original.

The aggregator point will then transmit these reports together with the aggregator value to the base-station. Some researcher developed problem by [21-23] explains SIA which deliberates the usage of a WSNs when many sensor nodes are located far from a user. The base station is used as an intermediary between the users and the sensor nodes, then the sensor nodes pass their values to the base station (a node grouped in the network) which performs the assembly and redirects the results of the aggregation to the primary server for user. SIA guarantees whether or not the user accepts aggregated results. However, if the reported value differs from the actual value, the user will track the attack and dismiss the reported result. SIA uses sampling mechanisms and interactive evidence to achieve this objective. Aggregate functions for example SUM, Count, Average, Min and Max can be used to compute aggregates. Another researcher used resilient aggregation (RA), this study presented[15].

The limitation of this study, that it does not check how data is collected but only examines the aggregated data received at the base station. Moreover, the connection will be very expensive because as the
network grows or increases in size it will send all sensor readings to the main station. In this study proposed secure data aggregation (SDA).

The algorithm in [15] shows the first SDA which was suggested by [2]. The process of addressing the problem of collecting data just because the node is broken through delaying the assembly and validation at higher levels, as this protocol will provide flexibility against node levelling. Thus, sensor measurements are transmitted without change and assembled in the second hop rather than in the immediate or first hop.

Hence, the sensor must buffer the data so as to authenticate it as soon as the base station disclosed the shared key. The proposed scheme provides authentication, data integrity and freshness. SDA increases the level of confidence based on the readings provided by the sensor. If the parent and child are compromised in the hierarchy, the integrity of the data will be affected. When a compromised node is traced, if no practical action is taken to reduce the harm caused by this compromise, the availability of data in the network will be affected. Once the grandfather's node detects that the node has been hacked, it will not be able to positively detect if the cheating node is the child's node [24]. Some researchers developed by efficient secure aggregation (ESA).

The survey in [25] had improved Data Aggregation by using ESA instead of μTESLA to authenticate the broadcast done by a base station during the process of validation process to reveal the shared key. The researchers used the marital hop keys to encode the first data between the node and its parent key and the second between the node and its grandparent. This improved the secure aggregation scheme by enhancing data confidentiality and decreasing the memory overhead since there is no need to store the data until the key is revealed. However, if two consecutive nodes are hacked into the hierarchy, the system will collapse.

This study proposed in [26] A data-gathering protocol over a safe hop for sensor networks that can penetrate one or more nodes and calculate the average. SDAP typically uses a grouping method that divides nodes into multiple groups or subdivisions of the same size within a tree structure. Within each logical group, the standard hop usage is calculated by the hopping aggregation protocol. The group sum will be sent to the base station by the member of each logical group. It creates an obligation based on the contributions each node in the group makes. It will identify groups that had made false contributions by using an outlier detection algorithm. Participation in the certification process can prove the validity of the group total. The base station will discard the aggregates which failed the attestation procedure from the group. Final aggregation will be calculated based on all groups of groups that have passed through authentication from the remote detection algorithm.

The researchers in [27] suggested a summary publishing algorithm that is a novel within a network aggregation that provides accurate estimates of duplicate sensitive aggregates i.e. meaning the partial result of a node which is a small summary for example of a sample, bit vector, histogram, etc. from the data. Such as generating a summary that takes a tangible value and generates a summary representing that data $SG(\cdot)$ and fusion fusion that generates a new abstract $SF(\cdot, \cdot)$. Finally the evaluation of the summary that the summary evaluation function converts the summary to a final answer $SE(\cdot)$.

The summary publishing algorithm consists of two stages, the first is the distribution stage where the aggregate query is routed across the entire network and the aggregation topology is created. The second is the aggregation stage where the collected results are directed toward the query node.

The study in [28] examined a tree topology utilized in TAG to prevent double-counting sensor readings. The TAG works when users send aggregation requests from a power-packed base station, then by pressing the current custom network protocol the operators conducting the query will be spread across the network and then the sensor nodes will route data at the basestation in the tree routing. The data will be collected based on the segmentation based on the value specified in the query and the aggregation function.

The researcher suggested in [29] the verification algorithm designed for the base station to verify the calculated aggregation and that its main goal is to reduce overheads for communications. This algorithm is used to validate the entire network total and to detect counterfeit sub-attack attacks produced by any compromised node.
Finally, in this study [30] introduces the integrity and confidentiality of the wireless sensor network and to obtain correctness, integrity, and confidentiality of data. Researchers in this algorithm used symmetric encryption (Elliptic curve El Gamal) and message authentication code (MAC).

3. Types of attacks
There are several types of attacks, but will discuss and address in this section on the types that affect data aggregation in wireless sensor networks.

3.1. Denial of Service attack (DoS)
The transmission of radio signals that interfere with the radio frequencies used by WSN networks is a popular form of attack on WSN. This is known as jamming and any increase in the capability of the opponent will affect a larger part of the network [31, 32].

3.2. Replay Attack
Replay attack occurs when an attacker transfers the previous sensing data repeatedly and thereby influencing the freshness of sensor data. Besides, BS is unable to obtain the most recent data from each sensor node. In order to prevent a replay, attack a time specific tag should be attached to each packet transmitted in the network. The researchers had used a related chain of keys while changing its keys values in accordance to different prerequisites [33].

3.3. Sybil Attack
An attacker can conceal itself as a correct or valid sensor node inside a network. During Data Aggregation process a node which is invalid can play many roles and attack a network greatly without being detected. The effect of Sybil attack can be reduced by using a "Beta reputation" system [21].

3.4. Data Integrity Attack
Software integrity attacks can circumvent the bad data detection mechanism and cause the system operator to get device cases that are inaccurate, resulting in significant economic losses [34].

3.5. Stealthy Attack
A hidden attack in the aggregation of data may trigger a security problem as it provides incorrect data which leads to a total change in the final decision on the basetation [10].

| Attacks         | Causes                              | Solutions                      |
|-----------------|-------------------------------------|--------------------------------|
| A Denial of service attack | Interference with radio frequency | Using MAC algorithm             |
| B Replay Attack | Transmitting same data without data freshness | Use time stamp                |
| C Sybil attack  | Making multiple identities         | Use authentication             |
| D Data Integrity Attack | Inserting false data | Use MAC and digital signature |
| E Stealthy Attack | Incorrect data entry caused, resulting security issue in data aggregation | Using consensus algorithm |

In this part, have clarified five types of attacks, as shown in Table 1 above, with an explanation of the causes and solutions of each type. Through our review and study of them, it was noted that the best type is Stealthy Attack Because it is a more general process and can work remarkably to reduce the losses caused by the attack [35].
4. **Classify and compare current safe data charts**

The proposed secured Data Aggregation scheme is classified into two models namely:

4.1. **Single aggregator model.**

In a single aggregation scheme, data communication occurs between base station of SINK and normal sensor nodes. The aggregator node performs the expected communication and high computation as show in Figure 2. This model is utilized in a small network to determine whether there is Verification Phase and No Verification.

4.2. **Multiple aggregator model**

In the multi-cluster diagram, data collected in the network will be collected more than once before it reaches SINK. Consequently, this process resulted in a reduction in the number of bits transmitted from the sensor node to the base-station. Figure 2, show in this model is utilized if the network is large to determine whether there is Verification Phase and No Verification Phase.

![Figure 2. Single aggregator and Multi aggregator Model](image)

**Table 2.** Comparison of Existing Schemes[30].

| Algorithm | Based on | Aggregate Considered | No. of compromised nodes | Integrity | Authentication | Verification |
|-----------|----------|-----------------------|--------------------------|-----------|----------------|--------------|
| SIA       | single   | Median, Min, Max, Average | ≥1                       | yes       | yes            | yes          |
| WDA       | Single   | General Aggregation.   | ≥1                       | yes       | yes            | yes          |
| TAG       | Hierarchical | Count, Sum          | 0                        | No        | No             | No           |
| SDA       | Hierarchical | Count, Sum           | 1                        | yes       | yes            | yes          |
| SD        | Hierarchical | Count, Sum           | 0                        | No        | No             | No           |
| SDAP      | Hierarchical | Count, Sum           | ≥1                       | yes       | yes            | yes          |
5. Adversarial model

Now in adversarial model, various capabilities which an opponent may have against the WSNs will be discussed. And it can be classified into two kinds, the first one is adversary types and other is network access. In adversary types can secured DA schemes are threaten by two types of Opponents such as [17].

- Passive Adversary: influence the confidentiality of the data.
- Active Adversary: influence the integrity of the data.

But in network access, WSN is made up of three different elements namely sensor, aggregator, and base station which serves diverse functions and possesses different capabilities. Next, how these three elements are compromised by the adversaries will be discussed. The conceptual framework would allow researchers to devise new schemes to improve their proposed scheme against the adversarial model, based on the analyzes in the previous sections. This study is the first attempt to create a framework which can propose minimum security prerequisites which should be available in any scheme according to its specifications. The network size helps the researchers to choose a proper aggregation model. The minimum prerequisites for a proposed secured scheme to resist against light adversaries namely data confidentiality and freshness is as in Figure 3. These prerequisites should be offered in a single aggregator model if the network size is small. Likewise, a multiple aggregator mode [17, 36] should be used if the network size is big.

Figure 3. Framework for Evaluation New Schemes.

There are many studies of researchers on data aggregation in WSN for reducing energy consumption. In Table 3 below provide a summary and analysis of the most important challenges of data aggregation in the wireless sensor network.
Table 3. List of existing data aggregation algorithm schemes in wireless sensor network.

| Author | Problem                          | Method                                      | Advantages                                                                 | Limitations                                    |
|--------|----------------------------------|---------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------|
| [21]   | Data fusion assurance            | WDA and polling systems to ensure the data consolidation node | The number of expected surveys is less than the number of witnesses in a harsh environment, also public expenditures are very low for the proposed mechanism | Doesn’t offer freshness and confidentiality  |
| [27]   | Reducing communication overhead and power expense for sensor nodes while collecting data in the sensor network | a Secure Data Aggregation Protocol (SDAP) | Reduces communications overhead                                              | Non robust against node and communications failure |
| [28]   | Energy consumption and reliable order- and duplicate-insensitive (ODI) | Solid against connections and linking failure, since it uses ring topology | Solid against connections and linking failure, since it uses ring topology | Doesn’t solve problem of false sub aggregate values |
| [29]   | Energy consumption              | Examined a tree topology utilized in TAG to prevent double-counting sensor readings | Avoid all “double account sensor” readings                                 | Because it uses a tree topology, it is not strong against node and communication failures |
| [30]   | Data aggregation schemes based on privacy homomorphism encryption | Homomorphic encryption and Message Authentication Codes (MAC) | To Reduces computation and communication overhead                           | This does not use confidential data aggregation schemes for homogeneous and heterogeneous WSN networks for the purposes of optimizing the implementation of a particular process. |
| [9]    | Energy consumption              | Symmetric Signature Syndication (HES) and Homomorphic encryption technology | To save energy, restore original sensor data and filter false data           | The recoverable approach to sensor data is not effective about large messages |
6. Conclusion and our vision

This analysis paper addressed the network of wireless sensors, data aggregation in WSN, basic data aggregation security specifications and an overview of and comparison of security protocols. The DA schemes are classified into single and multiple pools. Individual aggregation networks implement individual aggregation systems where the only aggregation is the base station. WAN uses many grouping systems. Hierarchical integration makes it easy for many aggregators to design the model from individual aggregator. Generally, message authentication code is used to secure the security of most DA schemes. Moreover, the usage of symmetric and public keys can achieve end to end encryptions. These charts are divided into two groups: the first is the complex of one model and the other is the complex of multiple models. Future research should evaluate more secured schemes and extend the framework. In this study, our vision of building a modern architecture with minimum pre-protection conditions against different types of challenges is recommended with use a computational approach.
References

[1] D. Y. Fong. 2017 Wireless Sensor Networks. Internet of Things and Data Analytics Handbook, pp. 197-213.

[2] L. Hu and D. Evans. 2003 "Secure aggregation for wireless networks," in 2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings., pp. 384-391: IEEE.

[3] H. Chan, A. Perrig, B. Przydatek, and D. Song. 2007 "SIA: Secure information aggregation in sensor networks," Journal of Computer Security, vol. 15, no. 1, pp. 69-102.

[4] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. 2003 "A witness-based approach for data fusion assurance in wireless sensor networks," in GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489), vol. 3, pp. 1435-1439: IEEE.

[5] M. M. Hamdi, L. Audah, S. A. Rashid, S. Alani, M. A. Al-Mashhadani, and A. S. Mustafa. 2020 "Green Communication Networks Challenges, Opportunities and Future Role," JCM, vol. 15, no. 3, pp. 256-262.

[6] K. Wu, D. Dreef, B. Sun, and Y. Xiao. 2007 "Secure data aggregation without persistent cryptographic operations in wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 100-111.

[7] S. Brown. 2017 "An analysis of loss-free data aggregation for high data reliability in wireless sensor networks," in 2017 28th Irish Signals and Systems Conference (ISSC), pp. 1-6: IEEE.

[8] S. Misra and S. Chatterjee. 2014 "Social choice considerations in cloud-assisted WBAN architecture for post-disaster healthcare: Data aggregation and channelization," Information Sciences, vol. 284, pp. 95-117.

[9] H. Zhong, L. Shao, J. Cui, and Y. Xu. 2018 "An efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks," Journal of Parallel and Distributed Computing, vol. 111, pp. 1-12.

[10] P. B. Gaikwad and M. R. Dhage. 2015 "Survey on secure data aggregation in wireless sensor networks," in 2015 International Conference on computing communication Control and Automation, pp. 242-246: IEEE.

[11] J. J. Palop, L. Mucke, and E. D. Roberson. 2010 "Quantifying biomarkers of cognitive dysfunction and neuronal network hyperexcitability in mouse models of Alzheimer's disease: depletion of calcium-dependent proteins and inhibitory hippocampal remodeling," in Alzheimer's Disease and Frontotemporal Dementia: Springer, pp. 245-262.

[12] P. Jesus, C. Baquero, and P. S. Almeida. 2014 "A survey of distributed data aggregation algorithms," IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 381-404.

[13] J. Domingo-Ferrer. 2002 "A provably secure additive and multiplicative privacy homomorphism," in International Conference on Information Security, pp. 471-483: Springer.

[14] S. Balin. 2011 "Non-identical parallel machine scheduling using genetic algorithm," Expert Systems with Applications, vol. 38, no. 6, pp. 6814-6821.

[15] D. Westhoff, J. Girao, and M. Acharya. 2006 "Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation," IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1417-1431.

[16] C. Kumar and H. F. Mahdi. 2017 "A real time algorithm for the machine to machine communication-smart warrior system," in 2017 IEEE 13th Malaysia International Conference on Communications (MICC), pp. 213-217: IEEE.

[17] H. Modares, R. Salleh, and A. Moravejesharieh. 2011 "Overview of security issues in wireless sensor networks," in 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 308-311: IEEE.

[18] H. Alzaid, E. Foo, and J. M. Gonzalez Nieto. 2008 "Secure data aggregation in wireless sensor networks: a survey," in Proceedings of the Sixth Australasian Information Security Conference (AISC 2008), vol. 81, pp. 93-105: Australian Computer Society.
[19] J. Guo and X. Chen. 2011 "Survey on secure data aggregation for wireless sensor networks," in Proceedings of 2011 IEEE International Conference on Service Operations, Logistics and Informatics, pp. 138-143: IEEE.

[20] M. Felemban, A. Daghistani, Y. Javeed, J. Kobes, and A. Ghafoor. 2020 "A Security and Performance Driven Architecture for Cloud Data Centers," arXiv preprint arXiv:2003.12598.

[21] G. Saurabh, K. Laura, and B. Mani. 2008 "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Networks, vol. 4, no. 3, pp. 1-37.

[22] S. Randhawa and S. Jain. 2017 "Data aggregation in wireless sensor networks: Previous research, current status and future directions," Wireless Personal Communications, vol. 97, no. 3, pp. 3355-3425.

[23] A. Sarkar and T. S. Murugan. 2019 "Cluster head selection for energy efficient and delay-less routing in wireless sensor network," Wireless Networks, vol. 25, no. 1, pp. 303-320.

[24] H. Alzaid, E. Foo, J. G. Neito, and D. Park. 2011 "Secure data aggregation in wireless sensor networks," Emerging Communications for Wireless Sensor Networks, p. 183.

[25] Y. Yang, X. Wang, S. Zhu, and G. Cao. 2008 "SDAP: A secure hop-by-hop data aggregation protocol for sensor networks," ACM Transactions on Information System Security (TISSEC), vol. 11, no. 4, pp. 1-43.

[26] S. Roy, M. Conti, S. Setia, and S. Jajodia. 2012 "Secure data aggregation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052.

[27] S. Nath, P. Gibbons, S. Seshan, and Z. Anderson. 2008 "Synopsis diffusion for robust aggregation in sensor networks. TOSN 4 (2), 71–740 (2008)," ed.

[28] S. Madden, "Michael j. Franklin, Joseph M Hellerstein. 2002" TAG: a Tiny Aggregation service for adhoc networks," in 5th Annual Symposium on Operating Systems Design and Implementation (OSDI).

[29] D. R. Anggraini, I. Petrus, and R. Inderawati. 2019 "Theoretic Analysis of Implicatures in Pride and Prejudice and Its Pedagogical Implications," Script Journal: Journal of Linguistics and English Teaching, vol. 4, no. 2, pp. 75-87.

[30] S. B. Othman, A. Trad, H. Youssef, and H. Alzaid. 2013 "Secure data aggregation with MAC authentication in wireless sensor networks," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 188-195: IEEE.

[31] A. Shi-Nash and D. R. Hardoon. 2017 "Data analytics and predictive analytics in the era of big data," Internet of things and data analytics handbook, pp. 329-345.

[32] D. Vinodha and E. M. Anita. 2019 "Secure data aggregation techniques for wireless sensor networks: a review," Archives of Computational Methods in Engineering, vol. 26, no. 4, pp. 1007-1027.

[33] G. Dhand and S. Tyagi. 2016 "Data aggregation techniques in WSN: Survey," Procedia Computer Science, vol. 92, pp. 378-384.

[34] D. An, Q. Yang, W. Liu, and Y. Zhang. 2019 "Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach," IEEE Access, vol. 7, pp. 110835-110845.

[35] W. Zhang and X. He. 2018 "Stealthy attack detection and solution strategy for consensus-based distributed economic dispatch problem," International Journal of Electrical Power & Energy Systems, vol. 103, pp. 233-246.

[36] A. Nazarloo, M. R. Feyzi, M. Sabahi, and M. B. Banna Sharifian. 2018 "Energy management of electric vehicles aggregator using a new multi-objective algorithm," Journal of Energy Management and Technology, vol. 2, no. 2, pp. 20-30.

[37] W. Y. Alghamdi, H. Wu, and S. S. Kanhere. 2017 "Reliable and secure end-to-end data aggregation using secret sharing in wsns," in 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6: IEEE.

[38] H. Hayouni and M. Hamdi. 2017 "A Data Aggregation Security Enhancing Scheme in WSNs Using Homomorphic Encryption," Intelligent Automation & Soft Computing, pp. 1-9.
[39] P. Zhang, J. Wang, K. Guo, F. Wu, and G. Min. 2018 "Multi-functional secure data aggregation schemes for WSNs," Ad Hoc Networks, vol. 69, pp. 86-99.

[40] A. Ullah, G. Said, M. Sher, and H. Ning. 2020 "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," Peer-to-Peer Networking and Applications, vol. 13, no. 1, pp. 163-174.

[41] W. Fang, X. Wen, J. Xu, and J. Zhu. 2019 "CSDA: a novel cluster-based secure data aggregation scheme for WSNs," Cluster Computing, vol. 22, no. 3, pp. 5233-5244.