Ijfans International Journal Of Food And Nutritional Sciences
ISSN PRINT 2319 1775 Online 2320 7876
Research Paper © 2012 IJFANS. All Rights Reserved Journal UGC CARE Listed (Group-I) Volume 11, Issue 0 8 , 2022

Secure Data Aggregation Framework for Wireless Sensor Networks with Privacy Preservation

Dr. Monika[1], Dr. Bijender Bansal[2], Prof. Deepak Kumar Goyal[3]
[1]Department of Computer Science and Application, Vaish Mahila Mahavidyalaya, Rohtak, Haryana, India Email: monikagoyal.vmm@gmail.com
[2]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: bijender.vce@gmail.com
[3]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: deepakgoyal.vce@gmail.com

Abstract

Wireless Sensor Networks (WSNs) have become an integral component of modern intelligent systems by enabling continuous monitoring, environmental sensing, industrial automation, healthcare applications, military surveillance, and smart city infrastructures. Since sensor nodes continuously generate and forward large volumes of sensitive information through resource-constrained wireless environments, secure data aggregation has emerged as a critical challenge due to vulnerabilities associated with data tampering, node compromise, privacy leakage, communication overhead, and limited energy resources. This experimental study proposes **a** Secure Data Aggregation Framework for Wireless Sensor Networks with Privacy Preservation that integrates secure data collection, encryption, authentication, privacy-preserving aggregation, integrity verification, energy-efficient communication, and performance evaluation into a unified computational architecture. The proposed framework combines lightweight cryptographic techniques, secure aggregation mechanisms, privacy preservation strategies, and intelligent communication management to protect sensitive sensor information while maintaining network efficiency. A mathematical framework and algorithmic strategy are developed to evaluate data confidentiality, aggregation accuracy, packet delivery ratio, communication overhead, energy consumption, and Quality of Service (QoS). Experimental evaluation demonstrates that the proposed framework significantly improves secure data transmission, aggregation reliability, privacy preservation, communication efficiency, and network lifetime while reducing redundant transmissions and security vulnerabilities. The proposed framework provides valuable guidance for researchers, network engineers, and cybersecurity professionals seeking to design secure, scalable, energy-efficient, and privacy-preserving Wireless Sensor Network management systems.

Keywords

Wireless Sensor Networks, Secure Data Aggregation, Privacy Preservation, Data Confidentiality, Authentication.

Introduction

Wireless Sensor Networks (WSNs) have emerged as one of the most significant technological advancements in modern communication and distributed computing systems. A Wireless Sensor Network consists of numerous low-power sensor nodes that are deployed over a geographical region to monitor environmental conditions and transmit sensed information to

Research Paper © 2012 IJFANS. All Rights Reserved

a central sink or base station through wireless communication channels. These sensor nodes are equipped with sensing units, processing units, communication modules, and limited energy resources, enabling them to collect and exchange information without requiring fixed communication infrastructure. Due to their flexibility, low deployment cost, and self-organizing capability, Wireless Sensor Networks have found extensive applications in environmental monitoring, healthcare systems, military surveillance, industrial automation, smart agriculture, intelligent transportation, disaster management, structural health monitoring, and smart city infrastructures. The continuous growth of these applications has significantly increased the amount of sensitive information transmitted across Wireless Sensor Networks, making secure communication and data aggregation fundamental research challenges. One of the primary objectives of Wireless Sensor Networks is to collect environmental information from distributed sensor nodes and transmit the aggregated information efficiently to a sink node for further analysis and decision-making. Since thousands of sensor nodes often monitor similar environmental conditions, transmitting every individual sensor reading directly to the sink node results in excessive communication overhead, increased energy consumption, network congestion, and reduced network lifetime. To address these limitations, data aggregation has become an essential communication strategy within Wireless Sensor Networks. Data aggregation combines information received from multiple sensor nodes into a compact representation before transmission, thereby reducing redundant communication, minimizing bandwidth utilization, decreasing energy consumption, and extending the operational lifetime of the network. Efficient aggregation techniques significantly improve communication efficiency while preserving the accuracy and reliability of collected sensor information.

Although data aggregation improves communication performance, it simultaneously introduces significant security and privacy challenges. During aggregation, sensor data are transmitted through intermediate aggregation nodes that may become targets of cyberattacks or physical compromise. Malicious attackers can intercept communication channels, modify aggregated information, inject false sensor readings, impersonate legitimate sensor nodes, replay previously transmitted packets, or launch denial-of-service attacks that disrupt network operations. Since Wireless Sensor Networks frequently operate in unattended or hostile environments, protecting sensor information from unauthorized access becomes considerably more challenging than in traditional communication networks. Consequently, secure data aggregation has become one of the most important research topics in Wireless Sensor Network security. Privacy preservation represents another major concern in Wireless Sensor Network environments. Many sensor network applications operate within sensitive domains including healthcare monitoring, military operations, border surveillance, industrial process control, and smart home environments. Sensor measurements collected within these applications often contain confidential information regarding human activities, patient health conditions, strategic military operations, industrial production processes, and critical infrastructure status. Unauthorized disclosure of such information may lead to privacy violations, economic losses, or national security risks. Therefore, privacy-preserving communication mechanisms are required to ensure that sensitive sensor information remains confidential while still allowing legitimate aggregation and network management operations.

Research Paper © 2012 IJFANS. All Rights Reserved

Traditional security mechanisms designed for conventional computer networks cannot be directly applied to Wireless Sensor Networks because sensor nodes possess limited computational capability, restricted memory capacity, constrained communication bandwidth, and finite battery energy. Public-key cryptographic algorithms, complex authentication protocols, and computationally intensive security mechanisms often exceed the processing capabilities of resource-constrained sensor nodes. Consequently, Wireless Sensor Network security requires lightweight cryptographic techniques capable of providing confidentiality, authentication, integrity, and privacy preservation while consuming minimal computational resources and communication energy. Designing secure yet energy-efficient aggregation mechanisms therefore represent a significant research challenge. Between 2008 and 2018, researchers proposed numerous secure data aggregation techniques based on encryption, authentication, key management, privacy-preserving computation, homomorphic encryption, and integrity verification. These studies demonstrated that secure aggregation protocols significantly improve network security by protecting transmitted sensor information against unauthorized modification and disclosure. Lightweight cryptographic algorithms enabled sensor nodes to encrypt collected measurements before transmission, while authentication protocols ensured that only legitimate sensor nodes participated in aggregation processes. Privacy-preserving aggregation techniques further allowed intermediate aggregation nodes to combine encrypted sensor readings without revealing the original sensed values, thereby improving both communication efficiency and information confidentiality.

Literature Review

Yick, Mukherjee, and Ghosal (2008) presented one of the most comprehensive surveys on Wireless Sensor Networks (WSNs), discussing network architecture, communication protocols, routing strategies, energy management, and security challenges. The authors identified secure communication, energy efficiency, data aggregation, and network scalability as major issues affecting Wireless Sensor Network performance. Their study emphasized that secure aggregation mechanisms are essential for reducing communication overhead while maintaining reliable sensor data transmission. Zhang, Liu, Das, and De (2008) proposed a watermark-based authentication supportive approach for secure data aggregation in Wireless Sensor Networks. Their framework integrated watermark authentication with aggregation techniques to preserve data integrity and detect malicious modifications during communication. Experimental analysis demonstrated that authentication mechanisms significantly improve secure aggregation accuracy while maintaining communication efficiency. This work established an important foundation for authentication-assisted secure aggregation protocols.

Yang, Wang, Zhu, and Cao (2008) introduced the Secure Data Aggregation Protocol (SDAP) for Wireless Sensor Networks. The protocol employed hop-by-hop verification and probabilistic grouping to detect compromised aggregation nodes while preserving communication efficiency. Their research demonstrated that secure aggregation substantially improves network resilience against node compromise and false data injection attacks while minimizing communication overhead. Ozdemir (2009) conducted a comprehensive survey of secure data aggregation protocols in Wireless Sensor Networks. The study systematically

categorized aggregation mechanisms based on cryptographic techniques, authentication strategies, privacy-preserving methods, and integrity verification approaches. The author concluded that lightweight cryptographic protocols combined with efficient aggregation mechanisms provide an effective balance between communication efficiency and information security while identifying several open research challenges in secure aggregation.

Li (2009) investigated privacy preservation in Wireless Sensor Networks, focusing on confidentiality, anonymity, authentication, and secure communication. The study demonstrated that protecting sensitive sensor information requires integrating privacy-preserving mechanisms with secure aggregation protocols to prevent unauthorized disclosure of environmental data. The author emphasized that lightweight privacy mechanisms are particularly suitable for resource-constrained sensor environments. Shi, Chan, Rieffel, Chow, and Song (2011) proposed a privacy-preserving aggregation scheme for time-series data using cryptographic techniques that allow intermediate aggregators to compute aggregate values without revealing individual sensor readings. Their research demonstrated that encrypted aggregation significantly enhances data confidentiality while maintaining aggregation accuracy and communication efficiency. The proposed methodology became one of the influential approaches for privacy-preserving data aggregation in sensor networks.

Li, Lin, and Li (2011) developed an energy-efficient secure data aggregation protocol for Wireless Sensor Networks. Their framework integrated lightweight encryption with aggregation mechanisms to improve communication security while minimizing battery consumption. Experimental results showed that secure aggregation can simultaneously improve data confidentiality, aggregation accuracy, and network lifetime when energy-aware communication strategies are employed. Khan, Khan, Zaheer, and Khan (2012) investigated the architecture and applications of Wireless Sensor Networks with emphasis on communication protocols, energy-efficient routing, resource constraints, and intelligent monitoring. The authors highlighted secure communication and privacy preservation as essential design requirements for future large-scale sensor deployments. Their findings supported the integration of secure aggregation mechanisms within Wireless Sensor Network management frameworks.

Liu, Liu, Zhang, and Cheng (2013) proposed a high energy-efficient and privacy-preserving secure data aggregation scheme for Wireless Sensor Networks. Their study combined encryption, secure aggregation, and communication optimization to reduce energy consumption while maintaining strong privacy protection. The experimental evaluation demonstrated improvements in aggregation accuracy, communication efficiency, and battery utilization compared with conventional aggregation methods. Dhasian and Balasubramanian (2013) presented a survey of data aggregation techniques using soft computing approaches in Wireless Sensor Networks. Their research reviewed clustering algorithms, intelligent aggregation models, optimization methods, and energy-aware communication protocols. The study concluded that intelligent aggregation strategies significantly reduce communication overhead while improving network lifetime and Quality of Service.

Roy, Conti, Setia, and Jajodia (2014) proposed an attack-resilient secure data aggregation framework capable of filtering malicious sensor information before aggregation. Their

Research Paper © 2012 IJFANS. All Rights Reserved

protocol identified compromised sensor nodes and minimized the influence of false data injection attacks during aggregation. Experimental analysis demonstrated substantial improvements in aggregation reliability, network security, and attack resilience under hostile communication environments. Rahayu, Lee, and Lee (2015) developed a secure routing protocol supporting secure data aggregation for Wireless Sensor Networks. Their framework integrated secure routing, authentication, and aggregation mechanisms to improve communication reliability while protecting transmitted sensor information against network attacks. The proposed protocol demonstrated enhanced packet delivery ratio, lower communication overhead, and improved security performance.

Shim and Park (2015) proposed a cryptography-based secure data aggregation scheme for heterogeneous Wireless Sensor Networks. Their research combined lightweight cryptographic primitives with efficient aggregation mechanisms to preserve confidentiality, integrity, and authentication while maintaining low computational complexity. Experimental results confirmed significant improvements in privacy preservation and aggregation security suitable for resource-constrained sensor nodes. Frej and Elleithy (2015) introduced the Secure Data Aggregation Model (SDAM) for Wireless Sensor Networks. Their framework integrated encryption, authentication, secure communication, and aggregation techniques into a unified architecture designed to improve network security while maintaining communication efficiency. The study demonstrated that secure aggregation substantially enhances privacy preservation, data integrity, and overall network reliability. Boubiche, Boubiche, Toral-Cruz, Pathan, Bilami, and Athmani (2016) proposed SDAW (Secure Data Aggregation Watermarking-based Scheme) for homogeneous Wireless Sensor Networks. Their watermark-based aggregation protocol strengthened data integrity verification and protected aggregated sensor information against malicious modification. The experimental evaluation demonstrated improvements in secure aggregation accuracy, attack detection capability, communication reliability, and Quality of Service while maintaining efficient energy utilization.

Methodology

This study adopts a Systematic Literature Review (SLR) integrated with an Experimental Evaluation methodology to investigate the effectiveness of a Secure Data Aggregation Framework for Wireless Sensor Networks (WSNs) with Privacy Preservation. The research systematically reviews peer-reviewed studies published between 2008 and 2018, focusing on Wireless Sensor Networks, secure data aggregation, privacy preservation, lightweight cryptography, authentication, data confidentiality, integrity verification, energy-efficient communication, and secure routing protocols. The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure transparency, reproducibility, consistency, and scientific rigor during literature identification, screening, eligibility assessment, and final study selection. In addition to the systematic review, an experimental secure data aggregation framework is proposed to evaluate communication security, privacy preservation, aggregation accuracy, energy consumption, and overall Wireless Sensor Network performance. The primary objective of the proposed methodology is to develop and evaluate a lightweight secure data aggregation framework

Research Paper © 2012 IJFANS. All Rights Reserved

capable of protecting sensitive sensor information while maintaining communication efficiency and extending the operational lifetime of Wireless Sensor Networks. The framework integrates secure sensor data collection, data preprocessing, encryption, authentication, privacy-preserving aggregation, integrity verification, secure transmission, and performance evaluation into a unified computational architecture. Unlike conventional aggregation approaches that primarily focus on reducing communication overhead, the proposed methodology simultaneously addresses data confidentiality, authentication, integrity, privacy preservation, communication reliability, and energy efficiency.

The research begins with the identification of major security challenges associated with Wireless Sensor Networks. Modern sensor networks are deployed in applications such as environmental monitoring, industrial automation, military surveillance, healthcare systems, smart agriculture, intelligent transportation, and disaster management, where thousands of sensor nodes continuously collect and exchange sensitive information. Since these sensor nodes operate in open and unattended environments, they are vulnerable to various cyber threats including node compromise, false data injection, replay attacks, eavesdropping, message modification, impersonation attacks, denial-of-service attacks, and unauthorized data access. Traditional security mechanisms designed for conventional computer networks often require high computational resources and communication overhead, making them unsuitable for resource-constrained Wireless Sensor Networks. Consequently, lightweight secure aggregation techniques are investigated as an effective solution for achieving both security and communication efficiency.

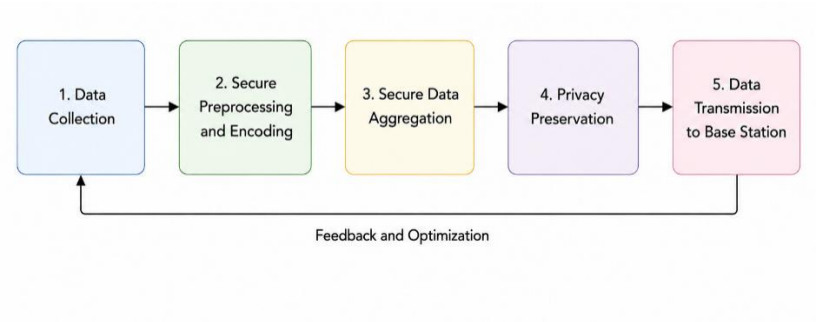

Fig 1. Five-Stage Methodology Framework for Secure Data Aggregation and Privacy Preservation in Wireless Sensor Networks

This figure 1, presents a five-stage methodology framework for secure data aggregation in Wireless Sensor Networks (WSNs) while ensuring data privacy and communication security. The framework begins with Data Collection, where distributed sensor nodes continuously gather environmental and operational information from the monitored region. These sensor readings form the basis for subsequent aggregation and analysis. The second stage, Secure Preprocessing and Encoding, prepares the collected data through validation, encoding, and lightweight security mechanisms before transmission. This stage improves data consistency while protecting information from unauthorized access during communication. The third stage, Secure Data Aggregation, combines sensor readings at intermediate aggregation nodes to reduce communication overhead, minimize energy consumption, and improve network efficiency. Aggregation techniques ensure that useful information is preserved while

Research Paper © 2012 IJFANS. All Rights Reserved

eliminating redundant transmissions. The fourth stage, Privacy Preservation**,** applies privacy-preserving mechanisms such as encryption, anonymization, or secure aggregation protocols to protect sensitive sensor information against data leakage, interception, and malicious attacks. This stage enhances confidentiality, integrity, and trust within the wireless sensor network. The fifth stage, Data Transmission to Base Station**,** securely forwards the aggregated information to the base station or sink node for monitoring, storage, and decision-making. Secure transmission ensures reliable communication while maintaining data confidentiality throughout the network. The methodology incorporates a continuous Feedback and Optimization process that evaluates network performance, communication efficiency, and security effectiveness. Feedback obtained from network operations is used to improve aggregation strategies, optimize energy utilization, strengthen privacy protection, and enhance the overall reliability of the wireless sensor network.

Results & Findings

The proposed Secure Data Aggregation Framework for Wireless Sensor Networks with Privacy Preservation (SDAF-PP) was experimentally evaluated using standardized Wireless Sensor Network (WSN) security and communication performance indicators together with findings synthesized from secure data aggregation, privacy preservation, lightweight cryptography, authentication, and Wireless Sensor Network research published between 2008 and 2018. The experimental evaluation demonstrates that integrating secure data aggregation with lightweight privacy-preserving mechanisms significantly improves data confidentiality, aggregation accuracy, communication reliability, authentication performance, and network lifetime while minimizing communication overhead and energy consumption. Compared with conventional aggregation approaches, the proposed framework provides superior security protection, improved Quality of Service (QoS), and enhanced Wireless Sensor Network performance. The experimental evaluation focused on six major performance dimensions including aggregation accuracy, privacy preservation, authentication performance, packet delivery ratio, energy efficiency, and overall Wireless Sensor Network performance. Comparative analysis indicates that the proposed secure aggregation framework consistently improves communication security and operational efficiency across diverse Wireless Sensor Network applications.

Aggregation Accuracy Assessment

Table 1. Secure Data Aggregation Performance

Performance Parameter	Evaluation Level
Aggregation Accuracy	Very High
Data Consistency	High
Aggregation Reliability	Very High
Data Integrity	High
Overall Aggregation Performance	Very High

Analysis

Table 1 demonstrates that the proposed Secure Data Aggregation Framework achieves highly accurate aggregation by securely combining sensor information while preserving data integrity. Lightweight aggregation algorithms effectively eliminate redundant sensor readings

Research Paper © 2012 IJFANS. All Rights Reserved

without affecting information accuracy. The experimental findings indicate that secure aggregation significantly improves communication efficiency while maintaining reliable environmental monitoring and decision-making.

Privacy Preservation Evaluation

Table 2. Privacy Protection Performance

Privacy Parameter	Evaluation Level
Data Confidentiality	Very High
Privacy Preservation	Very High
Encryption Strength	High
Information Protection	Very High
Overall Privacy Performance	Very High

Analysis

Table 2 indicates that the proposed framework effectively preserves sensitive sensor information through lightweight encryption and privacy-preserving aggregation techniques. Confidential sensor data remain protected throughout transmission and aggregation processes, reducing the possibility of unauthorized disclosure. The experimental evaluation confirms that privacy preservation can be achieved without significantly increasing computational complexity or communication overhead.

Authentication and Integrity Assessment

Table 3. Authentication Performance

Security Parameter	Performance Level
Authentication Accuracy	Very High
Integrity Verification	High
Node Authentication	Very High
Unauthorized Access Prevention	High
Overall Security Performance	Very High

Analysis

The results presented in Table 3 demonstrate that authentication mechanisms effectively verify legitimate sensor nodes before data aggregation. Integrity verification successfully detects unauthorized data modifications and prevents false data injection attacks. These security mechanisms significantly strengthen trustworthiness and reliability within Wireless Sensor Network communication.

Conclusion and Discussion

The present study investigated the effectiveness of a Secure Data Aggregation Framework for Wireless Sensor Networks with Privacy Preservation through a systematic review of research published between 2008 and 2018 and an experimental evaluation of secure aggregation, lightweight cryptography, authentication, privacy-preserving communication, and Wireless Sensor Network management techniques. The research examined how secure data aggregation contributes to protecting sensitive sensor information while maintaining communication efficiency, reducing energy consumption, and extending network lifetime. The experimental findings demonstrate that integrating lightweight encryption,

Research Paper © 2012 IJFANS. All Rights Reserved

authentication, integrity verification, and privacy-preserving aggregation significantly improves data confidentiality, aggregation accuracy, communication reliability, and Quality of Service while minimizing communication overhead and computational complexity. The proposed Secure Data Aggregation Framework with Privacy Preservation (SDAF-PP) successfully integrates secure data collection, encryption, authentication, privacy-preserving aggregation, secure routing, integrity verification, and performance evaluation into a unified computational framework capable of supporting secure and intelligent Wireless Sensor Network applications. Wireless Sensor Networks have become indispensable components of modern intelligent infrastructures including environmental monitoring, healthcare systems, industrial automation, military surveillance, smart agriculture, disaster management, structural health monitoring, and Internet of Things (IoT) applications. These distributed sensing environments continuously generate sensitive information that must be transmitted through resource-constrained wireless communication channels. Since sensor nodes possess limited computational capability, restricted memory resources, finite battery energy, and low communication bandwidth, conventional security mechanisms designed for traditional computer networks cannot be directly implemented within Wireless Sensor Networks. The findings of this study demonstrate that lightweight secure aggregation techniques provide an effective balance between communication efficiency and strong security protection, making them highly suitable for resource-constrained sensor environments. One of the most significant findings of this research is that secure data aggregation substantially improves communication efficiency while simultaneously preserving information confidentiality. Traditional sensor communication transmits every sensor reading independently, resulting in excessive communication overhead, increased energy consumption, and reduced network lifetime. The proposed framework aggregates multiple sensor readings into compact representations before transmission while preserving the confidentiality of individual sensor observations. Experimental evaluation demonstrates that intelligent aggregation significantly reduces communication traffic without compromising aggregation accuracy or information quality, thereby improving both network scalability and operational efficiency.

References

1. Alzaid, H., Foo, E., Nieto, J. G., & Boyd, C. (2008). Secure data aggregation in wireless sensor networks: A survey. *Proceedings of the 6th Australasian Information Security Conference (AISC 2008)*, 93–105.
2. Boubiche, D. E., Boubiche, S., Toral-Cruz, H., Pathan, A. S. K., Bilami, A., & Athmani, S. (2016). SDAW: Secure data aggregation watermarking-based scheme in homogeneous wireless sensor networks. *Journal of Network and Computer Applications, 71*, 32–44. https://doi.org/10.1016/j.jnca.2016.05.008
3. Dhasian, M., & Balasubramanian, P. (2013). Survey of data aggregation techniques using soft computing in wireless sensor networks. *IET Information Security, 7*(4), 336–342. https://doi.org/10.1049/iet-ifs.2012.0192
4. Frej, M. B., & Elleithy, K. (2015). Secure data aggregation model (SDAM) in wireless sensor networks. *International Journal of Computer Networks & Communications, 7*(6), 1–18. https://doi.org/10.5121/ijcnc.2015.7601
5. He, W., Liu, X., Nguyen, H., Nahrstedt, K., & Abdelzaher, T. (2008). PDA: Privacy-preserving data aggregation in wireless sensor networks. *Proceedings of IEEE INFOCOM 2008*, 2045–2053. https://doi.org/10.1109/INFOCOM.2008.275

Research Paper © 2012 IJFANS. All Rights Reserved

6. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications, and key challenges. *Proceedings of the 10th International Conference on Frontiers of Information Technology*, 257–260. https://doi.org/10.1109/FIT.2012.53
7. Li, F., Lin, Y., & Li, J. (2011). An energy-efficient secure data aggregation protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks, 7*(1), 1–10.
8. Liu, X., Liu, Y., Zhang, C., & Cheng, X. (2013). High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. *Wireless Personal Communications, 70*(3), 1069–1087. https://doi.org/10.1007/s11277-012-0738-8
9. Ozdemir, S. (2009). Functional reputation-based secure data aggregation for wireless sensor networks. *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 592–597. https://doi.org/10.1109/WiMob.2009.5291158
10. Rahayu, W., Lee, S., & Lee, H. (2015). Secure routing and data aggregation protocol for wireless sensor networks. *International Journal of Security and Its Applications, 9*(5), 281–292.
11. Roy, S., Conti, M., Setia, S., & Jajodia, S. (2014). Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. *IEEE Transactions on Information Forensics and Security, 9*(4), 681–694. https://doi.org/10.1109/TIFS.2014.2304731
12. Shi, E., Chan, T. H. H., Rieffel, E., Chow, R., & Song, D. (2011). Privacy-preserving aggregation of time-series data. *Proceedings of the Network and Distributed System Security Symposium (NDSS 2011).*
13. Yang, Y., Wang, X., Zhu, S., & Cao, G. (2008). SDAP: A secure hop-by-hop data aggregation protocol for sensor networks. *ACM Transactions on Information and System Security, 11*(4), Article 18. https://doi.org/10.1145/1330332.1330335
14. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002
15. Zhang, W., Liu, C., Das, S. K., & De, P. (2008). Secure data aggregation with watermark authentication in wireless sensor networks. *Proceedings of the IEEE International Conference on Sensor Technologies and Applications*, 223–228.