Journal of Namibian Studies, 34 S2(2023): 1165-1178 ISSN: 2197-5523 (online)

Secure Data Transmission Using Caesar Cipher Encryption in Wireless Sensor Networks

Manjunatha A S[1], Dr. Venkatramana Bhat P[2]

[1] Assistant Professor, Department of Computer and Communication Engineering, NMAM, Institute of Technology (NMAMIT), Nitte (Deemed to be University), Karnataka, India
E-mail: manjunatha.as@nitte.edu.in

[2] Professor, Department of Computer Science and Engineering, NMAM Institute of Technology (NMAMIT), Nitte (Deemed to be University), Karnataka, India
E-mail: pv.bhat@nitte.edu.in

Abstract

In the Wireless Sensor Network, sensor nodes sense the data and send it to the cluster head. Since multiple sensor nodes sense similar data, there is a need to control the data redundancy at the cluster head node to reduce the energy consumption in the sensor network. Another challenge is the confidentiality and the integrity of the aggregated data sent to the base station.

Keywords: Wireless Sensor Networks, Confidentiality

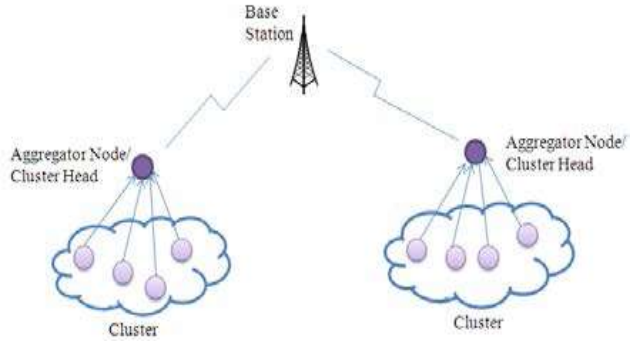
Introduction

Wireless Sensor Network (WSN) is one of the important areas of research in Computer Science. WSN is used in many of the current applications like automation, agriculture areas, military applications, medical and home applications, etc. The WSNs may be used to detect and track the intrusion of enemies, forest fires and floods, monitoring environmental pollution and also the traffic flows in the networks. Wireless Sensor Network consists of a number of sensor nodes which will read the environmental data. Each sensor node contains a sensing unit, micro controller, RF module and provided with a limited battery power. The sensor nodes are programmed in such a way that the sensed data will be sent to the base station.

WSNs are like Ad Hoc networks that contains a huge number of sensor nodes. There is no fixed infrastructure for Wireless sensor networks and the sensor nodes may be deployed and managed in an Ad Hoc manner. The sensor nodes used for monitoring transmission of real-time data uses few precise software in the intermediate collection nodes called cluster

head. The back-end data center will receive the sensed data from the cluster head for further process and analysis. Fig 1.1 shows the basic architecture of a typical wireless sensor network with cluster head.

Fig 1.1 Architecture of Wireless Sensor Network with Cluster Heads



Security is one of the fundamental constraints in the WSNs. As the WSNs normally deployed in remote environments and work in an unattended manner, prevention of attack and protection of privacy of data collected at each node is an important issue. The security countermeasure schemes and their classification for the sensed data is the matter of interest.

Literature Survey

In recent years, there are several security issues have been identified. The security attacks may be categorized into two categories [1]:

1. Active attacks: Active attacks are the attacks in which the attacker modifies the contents of the sensed data. Examples for active attacks are node replication attacks, wormhole attacks, compromised node attacks, etc.

2. Passive attacks: Passive attacks are the attacks in which the attacker monitors the network to check the data communication. An Example of the passive attack can be considered as eavesdropping.

Since nodes will join and leave the network frequently in wireless sensor networks, it is dynamic in nature [2]. Also, the authors have discussed the various kinds of attacks that are possible on sensor networks. They have discussed the low-level security in mobile sensor networks.

The authors in their paper [3] have discussed the attacks against broadcast services in wireless sensor networks. These attacks will have the most catastrophic effects on power and other resource constraints. As the duplicate packets are propagated through the sensor nodes without being filtered out, the sensor nodes will simply waste their energy and memory on transmitting and buffering those false packets. They proposed a new secure broadcast authentication for sensor networks. According to their research, this authentication scheme may be used to detect invalid packets and to isolate links that are from the compromised

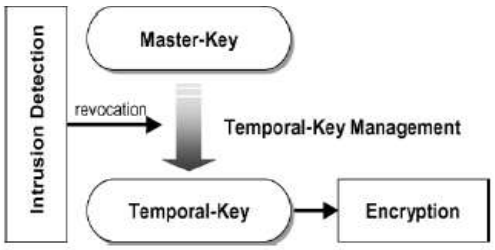
nodes, which results in enhanced resistance to various security attacks including DoS attacks. Their research contains two components: Lightweight Neighbor Authentication Protocol (LNAP) and Predictive Hash-Based Broadcast Protocol (PHBBP). LNAP is used for authenticating the received packet that whether the packet is really from a neighbor or not. This protocol allows each sensor node to authenticate whether a received packet is really from a neighbor or not. The PHBBP protocol is based on PH technique and size selecting the forwarding technique.

The authors in their paper [4] had mentioned the 3-factor authentication scheme for WSN using Elliptic Curve Cryptography (ECC). The fundamental steps to be followed in ECC are, System setup and sensor node registration phase, user registration phase, login phase, authentication phase, post-deployment phase, password change phase, gateway impersonation attack, sensor node impersonation attack, session key disclosure attack, and new smart card issue attack. After the implementation, they compared the result with respect to security features, computational cost, communication cost, and storage cost. They showed that it is resistant to various known attacks. Also, they evaluated the performance of their scheme along with that of existing systems. They also showed that their method is more secure than other schemes and has less communication costs.

The safety framework for preserving privacy in data aggregation in wireless sensor networks have been discussed in [5] in which solution for the safety of Concealed Data Aggregation (CDA) and general Private Data Aggregation (PDA) have suggested by the authors. According to the authors, the security model covers both private-key and public-key based CDA/PDA constructions. But for end-to-end communication proper security mechanism is required to avoid active attacks.

A light-weight security protocol (LiSP) is proposed in [6] that is equipped with key renewability and makes a tradeoff between security and resource consumption. The authors also proposed a joint authentication and recovery algorithm for rekeying, in which the key server periodically broadcasts a new key well before its use for encryption/decryption, and a client node will authenticate the received key and then recovers the previously missed out keys. The key hierarchy which was used in LiSP is show in Fig 2.1.

Fig 2.1 The key hierarchy used LiSP



The wormhole-based attacks are the major problems in wireless sensor networks [7]. As per the authors, in wormhole attacks, attackers create a low latency link between two points in the network. Once the link is created, the attacker collects the data packets, sends the data packets using the low-latency link, and replays them at the other end. Wormhole attack results in a modification in the network data flow and then deceiving the base station. The authors discussed wormhole attacks and illustrated the state-of-art in wormhole attack detection in wireless sensor networks. The authors discussed various kinds of wormhole attacks such as wormhole using encapsulation, wormhole using high-quality/out of band channel, wormhole using high power transmission capability, wormhole using protocol distortion. They also discussed the wormhole attack detection mechanisms such as distance-bounding/consistency-based approaches, synchronized clock-based solutions, and multi-dimensional scaling-visualization based solutions, trust-based solutions, localization-based solutions, secure neighbor discovery solutions, connectivity-based approaches, and radio fingerprinting approaches.

In [8], the authors discuss the integrated privacy, security, and trust solution for WSNs was presented that is needed for achieving completeness in the security solution. They also described the integration details of the privacy, security, and trust components that are helpful in understanding the interactions between various components. They have done the theoretical analysis and evaluation on memory consumption, communication overhead, etc. The Fig 2.2 shows their result with respect to memory consumption.

Fig 2.2 Memory consumption

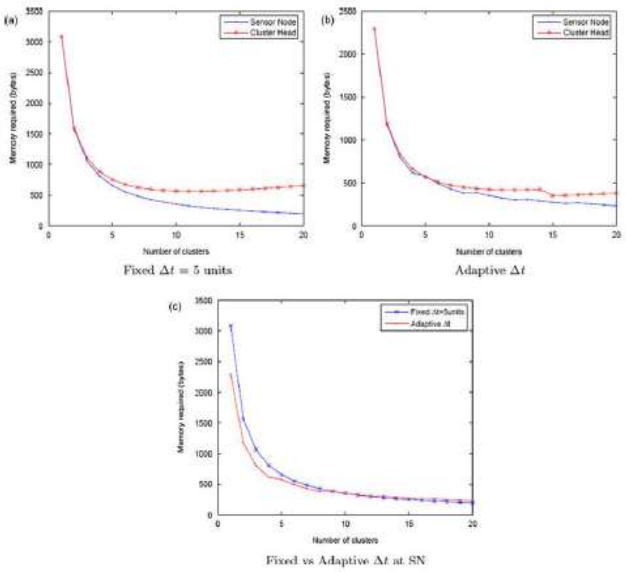
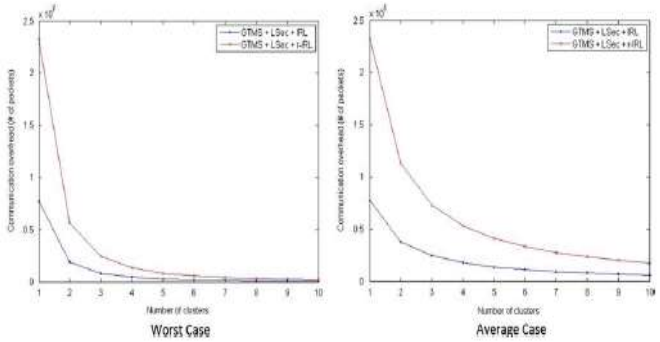


Fig 2.3 shows the result with respect to communication overhead when transferring the data from the cluster head node to the base station.

Fig 2.3 Communication overhead



The inspiration given by the authors combines the advantages of both symmetric and asymmetric encryption algorithms [9], by the way of using AES, DES, and m-RSA algorithms. In the encryption system, the plain text is divided into three components after which the AES encryption approach has been applied in the first part, DES on the second part, and m-RSA on the third part. These are applied in parallel by the usage of parallel Computing Toolbox feature in MATLAB 2017a. The ciphertext is the combination of three cipher texts, is dispatched to the receiver.

The authors have mentioned the encryption and decryption system using the symmetric method in wireless sensor networks [10]. They also have mentioned data transmission in wireless sensor networks. According to the authors, the security of the data transmission of wireless sensor networks can be considerably progressed by using the symmetric key algorithm. Based on this, the transmission performance of the wireless sensor networks is further analyzed to improve the overall transmission performance of the wireless sensor networks.

In [12], the authors have listed the various security issues that may cause harm to the flow of data in wireless sensor networks and also the feasible countermeasure for these issues. They also list various limitations in wireless sensor networks such as node, network, and physical limitations.

There are two key management schemes [13], namely centralized and distributed schemes. The centralized scheme relies on a trusted third-party key distribution center (KDC) to distribute and manage keys. Whereas the distributed scheme there are no key distribution centers, rather the generation and updating of keys is done completely in a distributed manner.

The authors in [14] discuss the confidentiality and integrity for data aggregation in WSN using homomorphic encryption. The scheme adopts a symmetric-key homomorphic encryption to protect data privacy and combines it with homomorphic signature to check the aggregation data

integrity. They showed that their mechanism requires less communication and computation overheads than previously known methods.

The authors of [15] proposed a security framework for cluster based WSN against the selfishness problem. They showed that the selfishness attack (passive attack or insider attack), in cluster based WSNs can cause serious performance disaster, particularly when a cluster head node becomes selfish. They proposed a security framework that involves a novel clustering technique as well as a reputation system at nodes for controlling selfishness, making them cooperative and honest.

In [16], the authors discuss the selection of cluster heads. A fuzzy multiple attribute decision making approach was used them for the selection of cluster heads. They included the parameters like residual energy, number of neighbors and the distance from the base station to the nodes for the selection of cluster heads.

The basic security of data transmission is typically achieved using the symmetric encryption methods since they use little energy [17]. If the energy input and usage is not balanced, nodes may black out. The authors of [17] proposed a scheme in which switching between symmetric-key and public-key encryption, based on an energy threshold, the level of security can be traded off against the urgency of energy-saving.

In [18], the author proposed a convolutional technique that generates security bits using convolutional codes to prevent malicious node attack on WSNs. Different security codes were generated at different hops and results were shown to reduce computational complexity compared to existing approaches.

The authors in [19] proposed a practical-ID based encryption for WSN. It splits the encryption process into two parts, the offline part, and the online part. In the offline part, all the heavy computations are done without the knowledge of the receiver's identity. In the online stage, only light computations such as modular operation and symmetric-key encryption are required, together with the receiver's identity and the plaintext message.

The authors in [20] talk about the blockchain mechanism and symmetric encryption in the WSN. They proposed a methodology that helps to protect data integrity and availability based on the security advantages provided by blockchain and the use of cryptographic tools. Their results proved that their method is less susceptible to many of the major attacks.

The authors in [21], made a survey on secure data transmission using some cryptographic techniques in WSNs. They found that for sending data in wireless sensor network, there is a requirement for cryptographic algorithms.

The authors in [22] discuss the secure and lightweight mutual authentication protocol for wireless sensor networks. According to the authors, the secure and lightweight mutual authentication protocol for WSNs has resistance from various security drawbacks and provides perfect forward secrecy and mutual authentication.

The authors in [23] performed a review on privacy preserving sensor based continuous authentication and user profiling. They summarize the privacy preservation methods employed to protect the security of sensor-based data used to conduct user authentication.

The authors of [24] discuss the technique for data encryption using quaternions for WSN. They used IEEE standard half-precision number system in the arrangement of quaternions and secret keys.

In [25], the authors discuss security and privacy as well as emerging applications of wireless sensor networks. They discuss the tradeoff between security and performance such as QoS, dependability and scalability.

The authors in [26] discuss the encryption and key exchange mechanism in wireless sensor networks. They discussed various symmetric-key mechanisms and the key distribution mechanisms.

The authors in [27] made a survey on cryptography mechanisms in wireless sensor networks. They also discussed the usual resource constraints of processing, memory and the energy of multimedia-based sensors.

The author in [28], discusses the issues in wireless sensor network in security. They also discussed the issues in data integrity.

The authors in [29] discuss the user authentication schemes for wireless sensor networks. They conducted a survey on the user authentication schemes and discussed twenty-two user authentication schemes. In each of the schemes, they mentioned the advantages and disadvantages.

Since the sensor nodes in wireless sensor networks consume more energy during the computation, a simple and secure authentication scheme is proposed by the authors in [30]. They use the digital certificate for authentication with other nodes to start their communication process.

Objectives

The main objective of the proposed work is to provide efficient encryption algorithms.

Energy efficient encryption algorithm

The data collected at the cluster head needs to be transferred to the base station. During this transmission, the data may get corrupted due to the transmission errors and other kinds of attacks. This issue needs to be addressed and can be achieved through the encryption algorithms. The

main challenge needs to be considered is the energy consumption at the cluster node. So, there is a need to propose a secure algorithm which is energy efficient.

Results and Discussions

The basic model for the wireless sensor network is carried out. The Caesar cipher algorithm is implemented at the cluster head node and the results show that the algorithm works well at the cluster head node.

6.1 Data Aggregation

MATLAB has been used to create a wireless sensor network. Fig. 6.1 shows a model of a wireless sensor network with 6 sensor nodes, 2 cluster heads and one base station. The LEACH algorithm has been implemented successfully and the same is illustrated below.

Fig 6.1 Basic Configuration of WSN with cluster head and base station

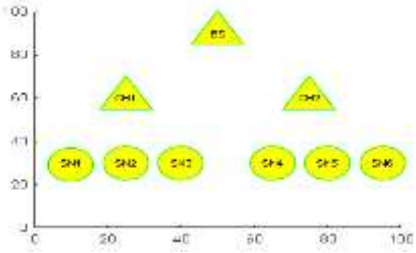
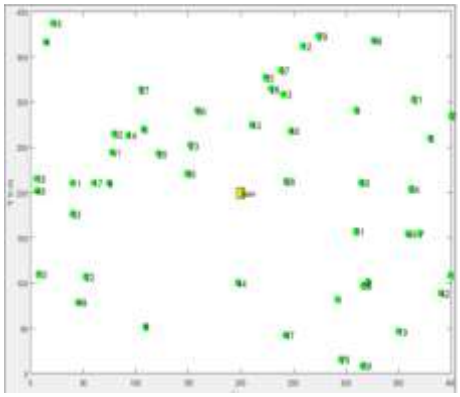


Fig 6.2 Creation of WSN with 50 nodes with Base Station

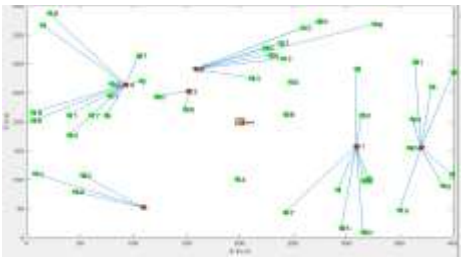


While creating the wireless sensor network, initial energy is as 10 units measured in Joules. The energy required to run the circuitry for both transmitter and receiver is taken as $50*10^{-9}$ units in Joules per bit. The

WSN is configured with the required number of sensor nodes. For the demonstration, we have taken the number of nodes as 50 nodes as illustrated in Fig 6.2. Once the number of required sensor nodes is selected, the zone division is carried out. In the current implementation, we have considered the zone size as 400x400. The sink node can be placed

anywhere in the zone. We need to specify the location for the sink node. In this implementation, we have placed the sink node at the location 200x200. The simulation is carried out for 100 rounds and the result is taken out for three routing methods. Fig 6.3 shows how the simulation is carried out.

Fig 6.3 Simulation Results



The average energy consumption by the node for each round is shown in Fig 6.4. The simulation is run for 100 rounds and the graph plotted to show the energy consumption.

Fig 6.4 Energy Consumption by the node comparison

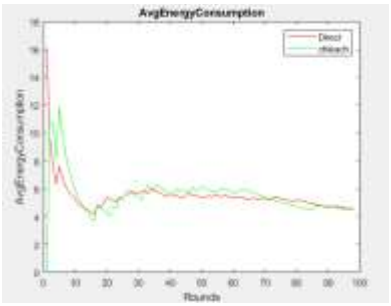
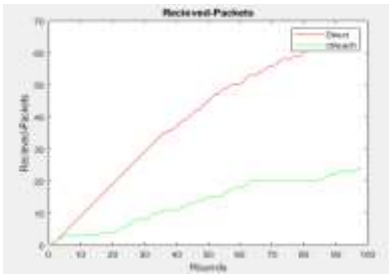


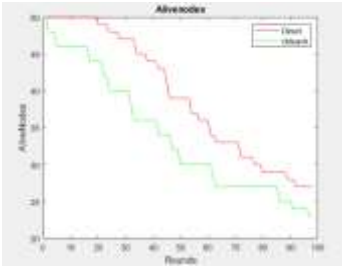
Fig 6.5 shows the received packets in the three algorithms implemented. The Direct method received the greatest number of packets at the base station.

Fig 6.5 Packets received at the base station using the direct method and the LEACH algorithm comparison.



The total number of alive nodes after simulating the complete round is shown in Fig 6.6. All the three algorithms are compared in the simulation.

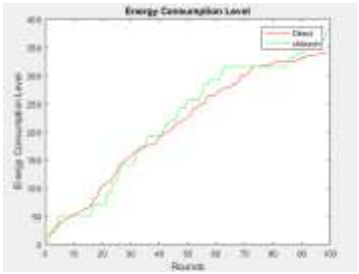
Fig 6.6 The total number of alive after simulating into 100 rounds.



Most of the nodes in the direct method is out of coverage area and they not involved in any of the transmission. Hence, they are alive even after the completion of 100 rounds.

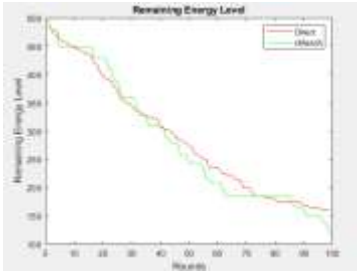
The energy consumption level is compared among the three algorithms. Since many of the nodes in the direct method was not involved in the transmission, less energy is consumed whereas LEACH algorithm has the high energy consumption level. Fig 6.7 shows the energy consumption level of the three algorithms.

Fig 6.7 Energy consumption level comparison



In each algorithm some of the energy will remain in the nodes. Fig 6.8 shows the comparison between the two algorithms for remaining energy level.

Fig 6.8 Comparison of Remaining Energy Level



6.2 Working with the Sensor Nodes

Sensor nodes are created using MATLAB and the three algorithms are implemented namely, the direct method, multihop algorithm for Leach

protocol has been implemented. Comparisons on various factors have been plotted in the graph.

6.3 Encryption

The basic cipher algorithm and the AES algorithm is implemented at the cluster head node. The basic cipher method takes less energy in the cluster head and the AES algorithm takes more energy for the encryption process. This is because each sensor node will have very less energy and power. The AES algorithm takes much time for the encryption process since 128-bit is required to encrypt the data. The energy consumption at the cluster head node is calculated. This energy consumption, the basic cipher method is compared against the AES algorithm. Hence it might be difficult to implement the AES algorithm at the cluster head node since it consumes more energy.

Future Work

The following works are planned for future course of action.

1. Currently the basic encryption algorithm and the AES algorithm are implemented. The energy consumed by the algorithms is compared. This needs to be further improvised so that the energy consumed at the cluster head node is minimal. Creating an energy efficient encryption algorithm for the data to send from cluster head to the base station.

There is a need to create an energy efficient algorithm for authentication.

Bibliography

1. Chun-Ta Li, Department of Information Management, Tainan University of Technology, Taiwan, “Security of Wireless Sensor Networks: Current Status and Key Issues”, DOI: 10.5772/13158
2. Kashif Kifayat, Madjid Merabti, Qi Shi, David Llewellyn-Jones, “Security in Mobile Wireless Sensor Networks”, https://www.researchgate.net/publication/225933532.
3. Seonho Choi, Hyeonsang Eom, and Edward Jung, “Securing Wireless Sensor Networks Against Broadcast Service Attacks”, International Journal of Computers and Applications, ISSN: 1206-212X (Print) 1925-7074 (Online).
4. Devender Kumar, Harsh Kumar Singh & Chhahat Ahlawat, “A secure three-factor authentication scheme for wireless sensor networks using ECC”, Journal of Discrete Mathematical Sciences and Cryptography, SSN: 0972-0529 (Print) 2169-0065 (Online).
5. Aldar C-F. Chan, Claude Castelluccia, “A Security Framework for Privacy-Preserving Data Aggregation in Wireless Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 7, No. 4, Article 29, Publication Date: February 2011.

6. Taejoon Park And Kang G. Shin, “LiSP: A Lightweight Security Protocol for Wireless Sensor Networks”, ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004, Pages 634–660.
7. Majid Meghdadi, Suat Ozdemir & Inan Güler, “A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”, IETE Technical Review, ISSN: 0256-4602 (Print) 0974-5971 (Online)
8. Riaz Ahmed Shaikh, Sungyoung Lee & Aiiad Albeshri, “Security Completeness Problem in Wireless Sensor Networks”, ISSN: 1079-8587 (Print) 2326-005X (Online)
9. Pooja & R. K. Chauhan, “Triple phase hybrid cryptography technique in a wireless sensor network”, ISSN: 1206-212X (Print) 1925-7074 (Online)
10. WeiZhou, PingLi, QinJuWang, Narjes Nabipour, “Research on data transmission of wireless sensor networks based on symmetric key algorithm”, https://doi.org/10.1016/j.measurement.2019.10745 40263-2241/_ 2019 Elsevier Ltd.
11. Shadi Nashwan, “AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment”, https://doi.org/10.1016/j.eij.2020.02.005 1110-8665/_ 2020 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.
12. Tanveer Zia, Albert Zomaya, “Security Issues in Wireless Sensor Networks”, DOI: 10.1109/ICSNC.2006.66
13. Weiping Wang1, Shigeng Zhang, Guihua Duan, and Hong Song, “Security in Wireless Sensor Networks”, Higher Education Press, Beijing and Springer-Verlag Berlin Heidelberg 2013.
14. Soufiene Ben Othman, Abdullah Ali Bahattab, Abdelbasset Trad & Habib Youssef, “Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption”, Wireless Personal Communications, ISSN 0929-6212, DOI 10.1007/s11277-014-2061-z
15. Zeba Ishaq, Seongjin Park, and Younghwan Yoo, “A Security Framework for Cluster-Based Wireless Sensor Networks against the Selfishness Problem”, 10 Jul 2018, https://doi.org/10.1155/2018/8961239
16. Puneet Azad and Vidushi Sharma, “Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment”, 24 Feb 2013, https://doi.org/10.1155/2013/909086
17. Jong Min Kim, Hong Sub Lee, Junmin Yi, and Minho Park “Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks”, 16 Mar 2016, https://doi.org/10.1155/2016/2678269
18. Turki Ali Alghamd, “Convolutional technique for enhancing security in wireless sensor networks against malicious nodes”, 22 October 2019, Human-centric Computing and Information Sciences volume 9, Article number: 38 (2019)

19. Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao, Robert H. Deng, “Practical ID-based Encryption for Wireless Sensor Network”, 4 Jan 2010, International Association for Cryptologic Research
20. Alma E. Guerrero-Sanchez, Edgar A. Rivas-Araiza, Jose Luis Gonzalez-Cordoba, Manuel Toledano-Ayala, and Andras Takacs, Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network, Sensors (Basel). 2020 May; 20(10): 2798, doi: 10.3390/s20102798
21. Heena Dogra and Jyoti Kohli, “Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey”, Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106883, December 2016.
22. Deok Kyu Kwon, Sung Jin Yu, Joon Young Lee, Seung Hwan Son and Young Ho Park, “WSN-SLAP: Secure and Lightweight Mutual Authentication Protocol for Wireless Sensor Networks”, 30 January 2021, Sensors 2021, 21, 936. https://doi.org/10.3390/s21030936.
23. Luis Hernández-Álvarez, José María de Fuentes, Lorena González-Manzano and Luis Hernández Encinas, “Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review”, 25 December 2020, Sensors 2021, 21, 92. https://dx.doi.org/10.3390/s21010092.
24. Monjul Saikia & Md. Anwar Hussain (2020) “Efficient data encryption technique using quaternions for wireless sensor network”, Cryptologia, 44:5, 451-471, DOI: 10.1080/01611194.2020.1755745.
25. Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, and Jose Maria de Fuentes, “Recent Advances in Security and Privacy for Wireless Sensor Networks”, Hindawi Journal of Sensors Volume 2017, Article ID 3057534, 3 pages https://doi.org/10.1155/2017/3057534.
26. Erwin, “Encryption and Key Exchange in Wireless Sensor Networks”, January 15, 2013.
27. Daniel G. Costa, Solenir Figuerêdo and Gledson Oliveira, “Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions”, 5 January 2017, Cryptography 2017, 1, 4; doi:10.3390/cryptography1010004.
28. Shafiqul Abidin, “Wireless Sensor Network and Security Mechanism by Encryption”, International Journal of Research in Advent Technology, Vol.7, No.6, June 2019 E-ISSN: 2321-9637.
29. Saru Kumari, Muhammad Khurram Khan, Mohammed Atiquzzaman, “User authentication schemes for wireless sensor networks: A review”, 5 December 2014, http://dx.doi.org/10.1016/j.adhoc.2014.11.018.
30. G. Bhanu Chander, Dr. G. Kumaravelan, “Simple and Secure Authentication in Wireless Sensor Network Using Digital Certification”, International Journal of Pure and Applied Mathematics Volume 119 No. 16 2018, 137-143.