JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SURVEY LIGHT WEIGHT CRYPTOGRPAHY ALGORITHM FOR SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

R. Nesamalar[1] *Dr.K.Ravikumar*[2]
[1] Research Scholar, Department of Computer Science, Tamil University
[2] Associate Professor , Department of Computer Science, Tamil University

Abstract : Due to the availability of inexpensive, short-range, and easily deployed sensors, wireless sensor networks (WSNs) have developed during the past few decades. WSN systems collect and deliver real-time sense data from a particular monitoring environment so the back-end system can process and analyze it further. Security is one of the most crucial challenges in WSN. This paper examines the security vulnerabilities and requirements of WSNs. Designing effective and lightweight cryptographic algorithms to secure shared data is essential. Cryptographic algorithms are typically used to address security issues to prevent communication data from being intercepted, manipulated, or falsified by unauthorized nodes. Lightweight cryptographic algorithms are created to offer sufficient security and performance without requiring a lot of computational power. The level of security, efficiency, and lifetime of the sensor node can all be considerably increased by cryptographic techniques. This paper reviews symmetric and asymmetric cryptography methods used for providing data security. This paper also reviews secure data transmission in WSN.

Keywords: WSN, Security, Cryptography, Data Transmission

1. Introduction

WSNs have many sensor nodes that share information with the sink node. The purpose of sensor nodes is to sense and gather environmental data. These nodes are powered by a tiny battery that, in most situations, cannot be recharged [1]. These networks are used in various industries, including monitoring the environment [2], detecting forest fires, and monitoring and controlling industrial processes for military purposes and civilian usage [3]. Figure 1 shows the WSN architecture.

The sensor nodes are linked to the gateway nodes connected to a base station or central processing units. The sensor nodes also have constrained resources, such as processing power, communication bandwidth, and storage space. Despite having many advantages, these networks have faced significant security issues due to the deployment of open sensor nodes, which encourages and provides a gateway for various physical security attacks. WSNs are susceptible to various security issues due to their numerous changes and certain limits. To address these security issues, secure and protected protocols must be developed to protect the data communication in WSNs [4].

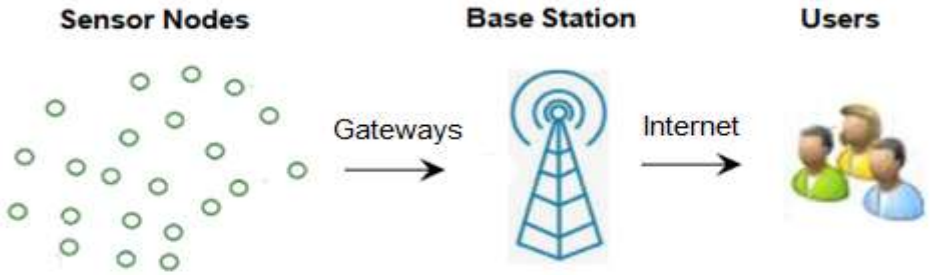

Figure 1 WSN Architecture

According to Hari and Singh [5], there are four basic categories of security: data confidentiality, authentication, data availability, and data integrity. To secure the data communication channels in the network, confidentiality and the authenticity of the data on every node are required [6]. When creating a security protocol for WSNs, key considerations include non-repudiation, freshness, integrity, confidentiality, authenticity, availability, freshness, forward secrecy, and backward secrecy. WSNs are subject to attacks, including Denial of Service (DoS), Sybil, Selective Forwarding, Sink Hole, Hello Flood, and Node Capture assaults.

Sensor nodes collect data in real-time straight from the environment; there is a possibility that attack individuals could access the data and utilize it inappropriately. It is crucial to address this issue to secure sensitive data from misuse and illegal access. The secrecy, integrity, and validity of sensor data and nodes can be protected with the help of cryptography [7]. Cryptography methods transform unprotected data into secure data unreadable by anyone but the intended receiver. Security keys are frequently used in cryptography for data encryption, which offers flexibility in the encryption and decryption process but also raises issues with key management.

This study provides an extensive review and comparative analysis of several cryptographic algorithms for secure data transmission in WSN. The remaining part of the paper is organized as follows: Section 2 describes the security vulnerabilities and requirements of WSN. Section 3 explains cryptography in WSN, and section 4 reviews the secure data transmission in WSN. Finally, Section 5 concludes the paper.

2. WSN Security Vulnerabilities and Requirements

The sensor nodes in a WSN are spread out over a large area rather than being deployed in a small area, making it difficult to control and monitor them individually in a network. This makes it possible for unauthorized users to report security flaws without access to the sensor nodes. There are three primary types of WSNs:

- Attack on Authentication and Confidentiality: Attacking these security parameters results in modifications like packet repetition or alteration.
- Network accessibility Attack/DoS assaults/denial of service: These attacks give the impression that the networks are unavailable when they are available for use.
- Integrity attacks prevent a network from transmitting accurate data packets and make it possible for attackers to communicate in the network while also preventing the network from transmitting useful information.

The fundamental idea behind WSNs operation is similar to how a traditional computer network functions. Data communication security in WSNs, as compared to computer networks during a working network life cycle, is essentially an additional need. The additional element of WSNs that includes specific and significant terms like secrecy, integrity, availability, authenticity, and quality of service is security requirements.

The following are some of the security criteria in WSN:

Confidentiality: An unauthorized user may access no information on a network.

Authentication: To enable secure data communication in a network and ensure reliable data transmission from source to destination, a secret authentication code known as MAC is communicated between the nodes communicating in a network.

Integrity: In a communicative network, an unauthorized user does not have permission to change the data that is being transferred.

Availability: In WSNs, some services are required on demand while others are fixed, such as node connectivity, which may be required on demand or as a fixed service. The availability parameter in a network is utilized to meet these demands at any time.

3. Cryptography in WSN

In wireless sensor networks, cryptographic algorithms can satisfy various security needs, including data authentication, confidentiality, and integrity [8]. Authentication is the process of guarding against unauthorized access to data. Data confidentiality is the process of preventing unauthorized parties from accessing the information. It is accomplished to prevent an opponent from alternating the data while it is in transit. Data must be encoded so that it cannot be read by an adversary to achieve the various security goals, and this encoding process is known as encryption.

Public and private key cryptography are the two main subcategories of cryptography, depending on how many keys are required to encrypt data. Symmetric key cryptography requires extra memory to hold the secret key because keys must be disseminated beforehand. Asymmetric key cryptography necessitates the use of extra resources for calculation.

A shared key is used for data encryption and decryption in symmetric cryptography. Before the deployment, keys must first be distributed to perform symmetric encryption. As mentioned above, there are various key pre-distribution schemes. The AES, RC4, RC5, and Blowfish symmetric key algorithms are widely used.

Table 1 summarizes the various symmetric key algorithms and their characteristics, including type (block cipher or stream cipher), plaintext size, key length, and the number of rounds. AES, RC5, DES, and Blowfish are block cipher algorithms, while RC4 is a stream cipher method. While RC4 only performs one round of operation and the input sizes for the various algorithms are typically 64 bits and 128 bits, DES, AES, RC5, and Blowfish all perform 16, 12, 20, and 16 rounds of operation, respectively, RC5 accepts input of 32 bits that is suitable for sensor networks but requires more time for encryption as it requires 20 rounds of operation. RC4 uses considerably less time because there are fewer rounds to complete.

Table 3.1 Symmetric key Cryptography algorithm

Algorithm	Cipher Type	Keys Length in bits	Plain Text Size in bits	No of Round
AES	Block	128, 192, 256	128	12, 14, 16
Blowfish	Block	32 to 448	64	16
DES	Block	56	64	16
RC4	Stream	40 to 2048	-	1
RC5	Block	0 - 2040	32, 64, 128	0 to 255

Two keys are essentially used in asymmetric key cryptography: a public key for encryption and a private key for decryption. While the user keeps private keys secret, public keys are available to the general public. Regarding security, asymmetric algorithms have an advantage because their keys are longer than those used by symmetric algorithms and are employed differently for encryption and decryption procedures. While the asymmetric algorithm's vulnerability caused the overhead on the data packet to increase as key length increased, lowering operating speed. Asymmetric algorithms include RSA, DSA, Diffie Hellman, and ECC. Table 2 shows the comparison of the Asymmetric key algorithm.

Table 3.2 Asymmetric key algorithm

Algorithm	Key Size in bits	Advantage	Disadvantage
DSA	512, 1024	Data integrity, non-repudiation, and authentication	The random signature value's entropy, secrecy, and uniqueness are crucial.
Diffie-Hellman	2048	Extremely difficult discrete logarithm.	Extremely costly exponential operation and authentication issues.
ECC	256, 384, 512	Smaller key sizes use less energy and require less storage and transmission time.	Increases the amount of the encrypted text and depends on extremely complex equations, which makes the method more complex.
RSA	1024, 2048, 4096	shorter computing times.	The same key is used for encryption and signing.

With the development of Lightweight Cryptography (LWC) procedures, which are simple to use on restricted devices, getting more satisfactory security with less equipment use and better-improved results is possible [9]. For platforms like WSN, lightweight cryptographic algorithms are the most effective. On both the hardware and software levels, lightweight cryptography is possible. The amount of optimization accomplished by using LWC is measured by factors like chip size, energy consumption, and RAM complexity at the hardware level. Large keys and several rounds are used to construct traditional cryptographic methods as defences against malicious attacks. The issue with utilizing traditional cryptographic techniques to protect WSN systems is that they use much computing power. Therefore, effective security-ensuring methods that use less power and function well are needed for WSNs. AES, Noekeon, LED 128, Present, Prince, Picolo, TWINE, Simon64/94, and KATAN64 are examples of LWC algorithms. Table 3 shows the LWC algorithms.

Table 1 LWC algorithms comparison [10]

Method	Block Size	Key Size	Type	Rounds	No of Cycles
AES	128	128	SPN	1	11
Prince	64	128	SPN	1	13
Simon64/94	64	96	Feistel	2	22
Present	64	80	SPN	2	17
KATAN64	64	80	Shift register	16	17
Picolo	64	128	Feistel	1	26
TWINE	64	128	Feistel	2	19
LED 128	64	128	SPN	1	50
Noekeon	128	128	SPN	1	18

4. Secure Data Transmission in WSN

Data transmission and security are constant concerns because of the significance of wireless sensor networks. The majority of current research efforts are concentrated on enhancing transmission and security. Transmitting encrypted data is necessary to preserve data integrity between the sender and the recipient. Data transmission via a wireless network must be protected from unauthorized users. This section reviews the different techniques for secure data transmission in WSN.

To enable secure data transfer and extend the lifespan of the WSNs, Prakash et al. [8] created an improved algorithm. A hybrid method is designed for data encryption and decryption in WSN. The key is created using the asymmetric key algorithm (ECC), while data is encrypted and decrypted using the symmetric key algorithm (AES). To guarantee energy efficiency and dependable forwarding via secure intermediary nodes against data threats, Haseeb et al. [9] propose an energy-aware and secure multi-hop routing protocol that uses an XOR-based secret sharing method. Based on the node's position, the network field is divided into inner and outer zones. Numerous clusters are produced in each zone based on the proximity of the node neighbourhood. The secret sharing mechanism secures the data transfer from cluster heads in each zone to the sink node. This method is dependable, energy-efficient, and reduces retransmissions and routing disturbance.

Fotohi et al. [10] suggested the abnormal sensor detection accuracy approach, which prevents DoS attacks and saves energy. A clustering approach is suggested based on energy, and distance is used to select the proper cluster head. The RSA cryptographic technique, interlock protocol, and an authentication method are utilized to prevent DoS attacks. Ali et al. [6] proposed a data security method with faster computation and response times using a modified version of Diffie- Hellman. The Diffie-Hellman has been enhanced to make it more resistant to attacks by creating a hash of each value broadcast over the network. The technique has undergone safety testing against numerous hazards. It has also been examined for different data volumes in terms of encryption/decryption time, computation time, and key generation time.

Mohindru et al. [5] suggest a hybrid cryptography scheme to protect WSNs from node-clone attacks. The algorithm uses symmetric (AES) and asymmetric (ECC) cryptographic methods along with the hash function. Communication in the sensor network verifies the message's integrity. To address the energy and security issues associated with intra-cluster data transmission, Wang et al. [7] present a new energy-efficient intra-cluster data communication method (EEICS) for WSNs. To maintain the privacy of nodes on the communication line, a secure data transfer technique is created to safeguard the source data.

Babaeer et al. [9] present a simple, safe method based on the Threshold Sensitive, Energy Efficient Sensor Network protocol and watermarking techniques to guarantee data integrity during transmission. This approach uses homomorphic

encryption for sinkhole detection and prevention, which is quick, effective, and uses less energy while identifying sensor nodes. A Paillier Cryptosystem and Compressive Sensing based Routing protocol is suggested by Ifzarne et al.[7]. Each device receives paillier security keys for data authentication. Within the intra-cluster, the spatio-temporal measurement matrix design significantly lowers computation and transmission costs. The base station can identify and isolate malicious network behaviour with the help of the integration of zero noise factors with all sent data.

A new cryptosystem based on matrix translation and elliptic curve cryptography is proposed by Pradeep et al. [8] to create a secure routing algorithm that would enable energy-efficient and secure data transmission in wireless sensor networks. The author also suggests two new algorithms: an encryption/decryption algorithm based on ASCII and prime numbers and a secure routing algorithm called Matrix Translation and Elliptic Curve based Cryptosystem Secure Routing Algorithm that uses cipher text conversion and distance vectors to perform cluster-based and energy-efficient secure routing.

A continuous hybrid and energy-efficient secure data aggregation algorithm is proposed by Hajian et al. [4] that weighs the trade-offs between preserving privacy, data integrity, communication overload, delay, and accuracy before selecting the optimum scenario based on the use and significance of the parameters. The slice-mixing technique is used to keep privacy protected in this case. Each subtree's optimal slicing is selected using fuzzy logic, and the key authentication mechanism is verified using GNY logic. Table 4 shows the comparison of different algorithms with merits and demerits.

Table 2.1 Comparison of Algorithms with Results

Algorithm / Protocol	Result (Merits and demerits)
Hybrid cryptography ECC and AES	The minimal usage of system resources allows it to maintain data integrity and confidentiality.
Energy-aware and secure multi-hop routing	Increases network lifetime, throughput and reduces energy consumption and delay
ASDA-RSA	Provides a high level of security and average throughput, and packet delivery ratio. Decrease network lifetime.
Modified Diffie- Hellman	Less computational time
Hybrid cryptography	It offers an effective and safe solution for energy sensor networks.
EEICS	Reduce energy consumption and increase packet delivery ratio with high security.
Homomorphic encryption and watermarking	Minimizes energy usage and guarantees the reliability and legitimacy of the sensed data.
Paillier Cryptosystem	Reduce communication costs and increase network lifetime.
Matrix translation and Elliptic curve cryptography	Reduce energy use and latency while improving security, packet delivery ratio, and network performance.
Continuous hybrid and energy-efficient secure data aggregation.	With little communication overhead, it uses less energy and is extremely secure.

5. Conclusion

The networks are insecure because sensor nodes are placed in an unsupervised setting. Military, environmental, medical, and commercial applications increasingly use wireless sensor networks. Traditional wired networks and wireless ad-hoc networks have fundamental differences from sensor networks. Wireless sensor network deployment requires a strong focus on security. This paper first analyzes the security vulnerabilities and issues of WSN and explains cryptography in WSN. Different approaches for secure data transmission in WSN are reviewed.

References

[11] Prakash, S., & Rajput, A. (2018). Hybrid cryptography for secure data communication in wireless sensor networks. In Ambient Communications and Computer Systems: RACCCS 2017 (pp. 589-599). Springer Singapore.

[12] Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 7, 79980-79988.

[13] Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4), e4234.

[14] Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., ... & Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International journal of distributed sensor networks, 16(6), 1550147720925772.

[15] Mohindru, V., Singh, Y., & Bhatt, R. (2020). Hybrid cryptography algorithm for securing wireless sensor networks from Node Clone Attack. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering), 13(2), 251-259.

[16] Wang, A., Shen, J., Vijayakumar, P., Zhu, Y., & Tian, L. (2019). Secure big data communication for energy efficient intra-cluster in WSNs. Information Sciences, 505, 586-599.

[17] Babaeer, H. A., & Al-Ahmadi, S. A. (2020). Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. IEEE Access, 8, 92098-92109.

[18] Ifzarne, S., Hafidi, I., & Idrissi, N. (2023). Compressive sensing and paillier cryptosystem based secure data collection in WSN. Journal of Ambient Intelligence and Humanized Computing, 14(5), 6243-6250.

[19] Pradeep, S., Muthurajkumar, S., Ganapathy, S., & Kannan, A. (2021). A matrix translation and elliptic curve based cryptosystem for secured data communications in WSNs. Wireless Personal Communications, 119, 489-508.

[20] Hajian, R., & Erfani, S. H. (2021). CHESDA: continuous hybrid and energy-efficient secure data aggregation for WSN. The Journal of Supercomputing, 77(5), 5045-5075.