Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

A NOVEL SECURE FRAMEWORK BASED ON TRUST BASED ROUTING AND LIGHTWEIGHT CRYPTOGRAPHIC SCHEME TO ENSURE SECURE COMMUNICATION IN WSN

Mrs.K.HimaBindu Research Scholar, Department of CSE, GIET University, Gunupur- 765022.
Dr.MD.Sirajuddin Associate Professor, Department of I.T, Kallam Haranadhareddy Institute of Technology, Guntur-522019 **kmaryjasmine@gmail.com ; siraj538@gmail.com**

Abstract: -
Wireless Sensor Network (WSN) is a wireless network which comprises sensor nodes that are dispersedspatially to work together to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion and pollutants at different locations [1]. A WSN doesn't require any fixed infrastructure to setup and it is dynamic in nature. Due to these features, WSNs are employed in wide range of applications irrespective of domains. WSNs are susceptible to various security threats. Ensuring secure communication in WSN is one of the challenging issues. To ensure secure communication many cryptographic algorithms have been proposed. Cryptographic algorithms should use light weight computations to provide security and to optimize the battery consumption. The main objective of this work is to propose a novel secure framework to ensure secure communication by using trust based routing along with lightweight cryptographic scheme. The proposed framework improves the QoS of the WSN.

Keywords: -Wireless Sensor Network**,** Lightweight Cryptography, Trust based Routing, Power Optimization, QoS.

Introduction: -

A wireless sensor network (WSN) is an infrastructure-free wireless network that is deployed on a large number of wireless sensors on an ad hoc basis to monitor system and physical or environmental conditions.
It monitors physical or environmental conditions such as temperature, pressure, motion, sound, vibration, and pollutants and passes that data and information directly over the network to a sink (also known as the main site) where the information is frequently observed and will be analyzed.
The base station or sink appears to be the interface between the user and the network. By inserting some queries and collecting the results from the sink, you can transform the information you want back from the network.
Symmetric and Asymmetric key distribution [12] is used to secure the information broadcasted through the network. The given information is converted into Cipher text[3,16] which can be decrypted by the authenticate user by using the key An elliptical curve [3] is used for the key distribution which inturn uses a secure hash function for the computation.
Wireless sensor networks typically include thousands of sensor nodes.Sensory nodes can communicate with each other via wireless signals. Wireless sensor nodes are equipped with sensors and radio transceivers, computing devices, and power components.

Components of WSN:

Sensors:

Sensors in WSN are used to seize the environmental variables and which is used for information acquisition. Sensor alerts are transformed into electrical signals.

Radio Nodes:

It is used to get hold of the statistics produced with the aid of the Sensors and sends it to the WLAN get right of entry to point. It consists of a microcontroller, transceiver, exterior memory, and strength source.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

Sink Node:-

It receives the information which is despatched by using the Radio nodes wirelessly, typically through the internet.

Evaluation Software:

The statistics acquired by way of the WLAN Access Point is processed through a software program referred to as Evaluation Software for providing the document to the users for similarly processing of the information which can be used for processing, analysis, storage, and mining of the data.

Architecture of Wireless Sensor Networks:-

The components of wireless sensor network and its architecture is depicted in figure 1.

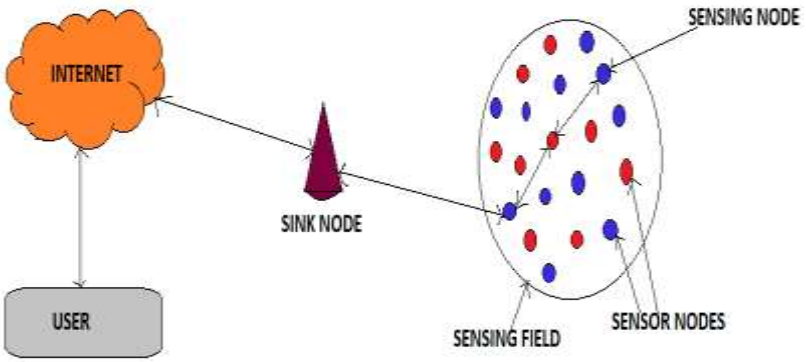

Figure 1: Architecture of Wireless Sensor Networks

Advantages:

- **Scalability: Wireless sensor Network architecture is used to scale numerous nodes, which enables comprehensive data collection which monitors across a variety of applications**
- **Flexibility: Wireless Sensor Network architecture is designed as a flexible architecture considering simple variations for various conditions and applications.**
- **Energy efficiency: Wireless Sensor Networks are energy-efficient networks which means that it consumes very less energy increasing the battery life.**
- **Distributed processing: Wireless Sensor Networks are designed to incorporate distributed processing which enables effective data handling and analysis at hub level.**

Disadvantages:

- **Complexity:Wireles Sensor Network has a complex architecture requiring specific knowledge and expertise.**
- **Security vulnerabilities: Wireless Sensor Network is exposure to security threats such as eaves dropping, message alteration and node impersonation which puts the data integrity and confidentiality at risk.**
- **Cost:** Wireless Sensor Network architecture implementation is expensive and requires expensive software and hardware components.

Applications of WSN:-

Wireless Sensor Networks are widely used in many applications.

1. **Military Applications:-** Wireless Sensor Networks are used in Military Applications like Combat Monitoring, Battlefield Surveillance and intruder detectionas it doesnot requires any wires to setup and is an instant network.

2. **Health Applications:-** Wireless Sensor Networks are used to monitor patients in healthcare facilities using advanced medical sensors
3. **Environmental Applicatons:-**Wireless Sensor Networks are used in Environmental applications as they require nonstop checking of surrounding conditions in hazardous and remote areas
4. **Home Control Applications:-** Wireless Sensor Network Applications empower the establishment, updating administer the system of a home control framework without wires.

Related Work: -

A Wireless Sensor Network can be installed without any infrastructure.

EzhilRoja P. et. al. [1] proposed a new lightweight key distribution mechanism for secure and resource-efficient communication in WSNs proposed a modern lightweight key disseminationcomponent for secure and resource-efficient communication in WSNs.In the first phase, CUBA-LSS was used to achieve optimal clustering by selecting appropriate CHs. The selection was based on energy, distance, delay, and RSSI. The second phase introduced automatic encryption using improved ECC for secure data transmission. In the final phase, a simplified key management scheme was established to protect the cryptographic keys through session key generation. According to the results, the KPA attack value of CUBA-LSS was low (0.001084), and the KPA attack value of AOA, ARCHOA, BES, BOA, CA, DHO, and ECDSA was high[6]

CS Kumar et. al. [2] proposed that wireless sensor networks can be employed in a wide range of operations. WSN data security and energy operation are major disquisition motifs. The primary thing in this study is to produce a revolutionary algorithm for icing data security while using lower energy. This proposaldiscusses the disquisition results, the significance of the disquisition donation, a summary of the disquisition exertion, and the eventuality for future exploration. The computing time of security styles is nearly related to network energy operation. As a result, the suggested security approaches focus on delivering security attributes analogous as data integrity, closeness, and authenticity while taking minimal computation time. The Intel lab dataset is used to produce the combination of algorithms for temperature measures. A homomorphic cryptosystem's disbenefit is that it isn't recoverable and isn't suited for a block of different data kinds. Decryption time is also long for homomorphic cryptosystems. Because the decryption is performed atthe BS, the decryption cost is neglected in the operation. One of the primary uses of WSN is the remote case covering system. Abuse or detention of health data might complicate matters for cases. The covered health data must reach medical magazines and clinicians swiftlyandsecurely.Decrypting medical data of various data kinds takes a long time using homomorphic cryptosystems. As a result, disquisition is conducted to identify the swish symmetric algorithm and access control approaches. Blowfish and CP- ABE are chosen as the swish and tested on gender, body temperature, and cardiac rate parameters. Feathery symmetric algorithms are intensively studied in order to minimize computing time for low- powered bias. Speck and CP- ABE are subsequently linked tobeing an applicable mix and carried out on health data. The bulk of current intrusion discovery systems(IDS) are designed to descry network caste assaults rather than cross-subcaste assaults. Following also, the study has concentrated on furnishing IDS for cross-subcaste risks. To execute this assignment, disquisition of assaults, the goods of assaults, and criteria to identify assaults is conducted.

Shabana Urooj ,et. al. [3] explored the community related to the area of wireless and mobile computing, during the once decade, wireless detector networks(WSNs) have gained a lot of interest. There are innumerous growing operations of WSN, ranging from home and office inner deployment situations to out-of-door deployment in the adversary's home in a military battleground. These networks, still, are vulnerable to security pitfalls, because of their deployment in remote areas. This may negatively affect their performance. In this composition we've delved WSN security issues and security pitfalls along with LEACH clustering[9] for energy effective routing. In addition, they

employed a series of effective countermeasures that can be used to apply their proposed guidelines. In this respect, the use of technology called cryptography is used to break similar security problems has been demonstrated and their failings have been reduced for making it more usable for WSNs.

P. Ramadevi , et. al. [4] utilised Wireless Sensor Networks in pivotal operations like monitoring, shadowing, and controlling, among others, WSNs' security characteristics are pivotal. When using a low- powered detector to convey pivotal information duly and on time, secure and reliable communication is pivotal. The thing of this work trouble was to ameliorate security in WSNs. Grounded on network size, bumps are grouped in this work, and cluster chiefs are chosen using CSO. Data encryption and decryption are fulfilled via IKEC. Based on the results, the proposed model outperforms other current models with 73 seconds to encrypt 100 MB of raw material. To assess the proposed work in real time, this work doesn't apply, but unborn work will be in these directions. The suggested system cannot effectively cipher images and other types of data due to its experimental setting and lack of exploration moxie, and as a result, there are some limits.

HalaTawalbeh et. al. [5] suggested that Traditional cryptography isn't the applicable system to insure security in WSNs as these systems are thick, complex, and consume too important power. Therefore, Lightweight Cryptography is used rather of traditional cryptography. Research in this field is getting emotional as experimenters realize the felicity of LWC to Wireless Sensor Network Systems and Bedded Systems. The authors anatomized several lightweight cryptographic mechanisms in a analogous pattern. They also describe the reasons behind the need for further development sweats in LWC because it's the most suitable result for surroundings with special conditions, similar as WSN. The author also surveys several symmetric and asymmetric LWC ciphers that are designed specifically for surroundings with tackle and software conditions. They elect tackle and software that had the rearmost executions of several LWC ciphers and discusses both executions for each cipher independently because specific characteristics can affect the tackle perpetration but not the software perpetration and vice versa. The authors also give several approaches to develop lightweight designs of traditional algorithms; they also punctuate the main features that should be enforced in the algorithms and the main limitations that the algorithms should consider.

Description of Existing Approaches	**Secure Routing**	**Lightweight computation**	**Power Optimization Considered**
Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model	CUBA-LSS	Yes	No
A Sophisticated and Light weight Cryptographic Protocols for Data Security in Wireless Sensor Networks	Blowfish and CP- ABE	Yes	No
Description of Existing Approaches	**Secure Routing**	**Lightweight computation**	**Power Optimization Considered**
Cryptographic Data Security for Reliable Wireless Sensor Network	LEACH clustering	No	No

Security for wireless sensor networks using cryptography	IKEC	No	No
Security in Wireless Sensor Networks Using Lightweight Cryptography	symmetric and asymmetric ciphers	No	No

Table 1: Summary of Existing Approaches

Summary of existing approaches are mentioned in Table 1**.**

Research Gaps:

- Many researchers emphasized on only few factors to improve the security in WSN.
- Existing algorithms not considered Power optimization in WSN.
- Existing algorithms require more computational power.
- Secure routing protocol implementation not considered.

Proposed Work: -

The above stated research gaps are addresses in our proposed framework. In this work, we proposed a novel secure framework based on trust based routing and lightweight cryptographic scheme to enhance the security in WSN.

This framework has three parts:

- Wireless network formulation: We simulate WSN formulation by using energy and mobility modelsof NS2.
- Trust based routing: In this protocol, only trusted nodes are allowed to participate in communication. Routing is performed by evaluating the trust values of nodes.
- Lightweight cryptography algorithm: We propose a secure cryptographic scheme that uses lightweight computations to provide confusion and diffusion features. This proposed algorithm provides better security with simple computations.

The steps involved in the proposed framework is depicted in Figure 2.

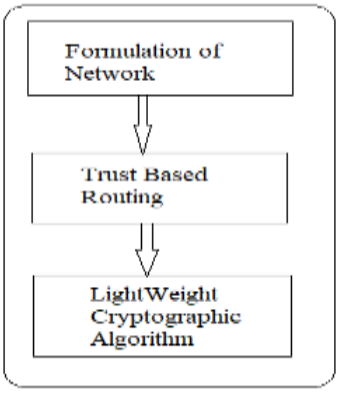

Figure 2: Proposed Framework

Conclusion and Future Work: -

In this work, we proposed a secure framework to enhance the security of WSN. We proposed trust based routing and cryptographic scheme to ensure secure communication in the network. The proposed framework provides better security than the existing approaches. In future we simulate above stated proposed algorithms using NS2 and assess their performance by comparing with the existing approaches.

References: -

[0] Misbha, D. S. "Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model." *High-Confidence Computing* 3.2 (2023): 100126.

[1]. Kumar, C. Srinivasa, et al. "A Sophisticated and Light Weight Cryptographic Protocols for Data Security in Wireless Sensor Networks." Journal of Algebraic Statistics 13.3 (2022): 3806-3821.
[2]. Urooj, Shabana, et al. "Cryptographic data security for reliable wireless sensor network." Alexandria Engineering Journal 72 (2023): 37-50.
[3]. Urooj, Shabana, et al. "Cryptographic data security for reliable wireless sensor network." Alexandria Engineering Journal 72 (2023): 37-50.
[4]. Tawalbeh, Hala, et al. "Security in Wireless Sensor Networks Using Lightweight Cryptography." Journal of Information Assurance & Security 12.4 (2017).
[5]. Pöpper, Christina. Applied Cryptography and Network Security: 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part I. Springer Nature, 2024.
[6]. Sivasangari, A., et al. "Security and privacy in wireless body sensor networks using lightweight cryptography scheme." Security and privacy issues in IoT devices and sensor networks. Academic Press, 2021. 43-59..
[7]. Hassan, Alaa. "State-of-the-Art Lightweight Cryptographic Protocols for IoT Networks." Proceedings of the Future Technologies Conference. Cham: Springer International Publishing, 2022.
[8]. Urooj, Shabana, et al. "Cryptographic data security for reliable wireless sensor network." Alexandria Engineering Journal 72 (2023): 37-50.
[9]. Sarkar, Anindita, Swagata Roy Chatterjee, and Mohuya Chakraborty. "Role of cryptography in network security." The" essence" of network security: an end-to-end panorama (2021): 103-143.
[10]. Arogundade, Oluwasanmi Richard. "Network security concepts, dangers, and defense best practical." Computer Engineering and Intelligent Systems 14.2 (2023).
[11]. Tiwari, Devisha, et al. "Lightweight encryption for privacy protection of data transmission in cyber physical systems." Cluster Computing 26.4 (2023): 2351-2365.
[12]. Alshehri, Jawaher, and AlmahaAlhamed. "A review paper for the role of cryptography in network security." 2022 4th International Conference on Electrical, Control and Instrumentation Engineering (ICECIE). IEEE, 2022.
[13]. Mulder, Valentin, et al. Trends in Data Protection and Encryption Technologies. Springer Nature, 2023.
[14]. Sahay, Rajeev Ranjan. "Information Security and Cryptography-Encryption in Journalism." Indian Journal of Mass Communication and Journalism 3.1 (2023): 1-16.
[15]. Bhagat, Vijesh, et al. "Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications." Concurrency and Computation: Practice and Experience 35.1 (2023): e7425.
[16]. Nithya, B., et al. "An Analysis on Cryptographic Algorithms for Handling Network Security Threats." 2022 IEEE Delhi Section Conference (DELCON). IEEE, 2022.
[17]. Uzunov, I., and S. Lyubomirov. "analysis and research of cryptographic models to ensure information security in engineering education." INTED2023 Proceedings. IATED, 2023..
[18]. Yamparala, Rajesh, and T. Kamaleshwar. "Lightweight Cryptography Model for Overhead and Delay Reduction in the Network." International Conference on Cognitive Computing and Cyber Physical Systems. Cham: Springer Nature Switzerland, 2023..
[19]. AL_AZZAWI, RuahMouadAlyas, and Sufyan Salim Mahmood AL-DABBAGH. "A Lightweight Encryption Algorithm To Secure IoT Devices", International Journal of Applied Sciences and Technology, 2023, http://dx.doi.org/10.47832/2717-8234.16.3