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

Investigation of sensor security and Routing Techniques For SEWN

[1] Mr. Kamesh Bhardwaj, [2] Mr. Nitin Kumar, [3] Dr. Rakesh Joon, [4] Dr. Rishu Bhatia
[1] M. Tech. Scholar, [2] Assistant Professor, [3] Associate Professor, [4] Associate Professor
[1,2,3,4] Ganga Institute of Technology & Management, Kablana, Jhajjar

Abstract- Sensor networks are quickly becoming the most important research topic for data collection at base stations. A sensor enhanced wireless network is how the sensor network is described (SEWN). The network of this method has the ability to improve network coverage and connection. The degree of existence on the left decreases as the degree of existence on the right increases. In high-density grids, a compact grid is advantageous because it reduces coverage gaps and thus improves overall network infrastructure dependability. In sparse networks, a large grid size may be desirable to minimize network coverage duplication and ensure that each node's sensory capacity is fully utilized. Examining sensor security and employing encryption to gain access to the network's root route If the security is strong and the data packets are broadcast, it may work. Sensors are in use. Sensor-enabled wireless networks (SEWNs) are networks comprised of hundreds or thousands of small sensors capable of detecting, analyzing, and transmitting data. Three major factors were discovered in the study: delivery time, energy consumption, and data packet loss. The analytical result of each communication configuration was saved and retrieved after each communication configuration. As a result, the three most important variables are delivered time, energy, and data packet loss. Following each communication setup, the outcome was analyzed.

Key Word: Sensor Network, Energy Usage, Delivery Time, Loss of Data Packets

I. INTRODUCTION

The WSN is essentially a small network that gathers data about its surroundings. This thesis proposes the term Sensor enabled Wireless networks (SEWN) [1,7,14], which refers to networks made up of hundreds or even thousands of tiny sensors that can monitor the real-world environment, each with sensing, processing, and transmission capabilities, and can communicate with one another. Traditional high overhead security techniques are not feasible for sensor nodes with limited resources due to resource constraints. SEWN security experts have proposed a variety of security solutions, each of which is optimal for these resource-constrained networks. A number of SEWN security researchers have proposed a variety of safe and efficient routing methods [2 - 5], secure data aggregation techniques [6 - 11], and other approaches to prevent data leakage and theft. Because of the network's decentralized nature and lack of infrastructure, security techniques in SEWNs must include node cooperation in addition to traditional security issues such as safe routing and secure data aggregation. It is not reasonable to assume that the nodes in real-world SEWNs are trustworthy. As a result, researchers concentrated their efforts on developing a sensor confidence model in order to solve problems that were beyond the scope of traditional cryptographic methods [12-19].

1.1 Security of Sensor

Intrusion detection is one of the most difficult and most important jobs in the area of cyber security. As the network uses more security sensors to monitor and identify threats, these sensors produce a great deal of warnings with various event granularities and semanticity's [1]. Such large numbers of warnings make a correlation procedure for a network assault very complicated and unpredictable. Attack correlations, on the other hand, have become an important component of most IDS systems, because they may improve the detection rate and provide more accurate attack strategies [2]. A better method is thus essential to improve existing network security for attack analysis and correlation. We suggest that relevant assaults be identified and predicted by utilizing memantine networks. Each node represents an assault and the edges link corresponding attacks when building a semantic network.

II. LITERATURE REVIEW

Khashan, O. A., Khafajah, N. & Ahmad, R. (2021), Security, efficiency and energy consumption remain important in Wireless networks (WSNs), owing to their open, large-scale and resource restricted nature. The findings show that, life, the suggested regime offers a substantial delaying and encrypting time compared with existing cypheres using set encryption parameters. It may increase network life respectively, in comparison safety study shows is able to withstand several assaults including. **Li, Z., Peng, C., Klötter, M., & Li, L. (2021),** With mobile communication network growth, particularly today's 5G and future 6G, pictures in cloud apps response to the requirements, an efficient and secure plaintext-related chaotic picture encoding method based on. In the proposed system, the internal keys for managing the whole compression and encryption process are created initially using a single picture and

the starting key. **Li, M. Li, M. (2021),** this article offers a symmetric algorithm-based automated encryption technique for network sensor capture data. The analysis of the SEWN architecture and the structure of the sensor nodes is used to design symmetric flow encryption algorithms, set up a network attack model, analyze multi-path transmission safety using the symmetrical algorithm, estimate the probability of successful eavesdropping and encrypt the sensor network collection data accordingly. **Bonavolontá, F., & Cioffi, A. (2020),** This article discusses a new area of electronic measurement in extremely low signal-to-noise circumstances relating to the experimental investigation of cyber security transducer networks. The weakness of the Internet's most frequently used encryption method, Advanced Encryption Standard (AES), has been proven experimentally. **Gonzalez-Cordoba, et.al., (2020),** The most essential needs in IoT Systems are security, privacy, dependability and autonomy. If these problems are not addressed, the IoT system may be used maliciously and maliciously by malevolent individuals. The findings collected show that the concept meets the key criteria of. **Kumaresan, J., & Ramasamy, J. S. (2020),** Wireless sensors are used to collect the video, transform the video into frames of pictures and send them to the sink node for analysis for many real-life applications like traffic surveillance. Safety is a significant problem in the case of wireless imaging owing to the existence of attackers on the wireless channel in such a situation. Most attackers here are passively trying to read the data sent to the network in order to abuse the data for personal advantages. The proposed algorithm and architectural framework established in these works was experimentally evaluated and showed that the proposed safe routing method is better when utilized in wireless applications that follow the framework suggested in the work. **Ge, C., Yin, C., Liu, Z., Fang, L. & H. (2020),** Big data and artificial intelligence are quickly developing. Big data analyzes were used in various areas of intelligent healthcare. Once this data is released or changed during transmission, it will not only affect patient privacy, but will also put their lives at risk. Many researchers have been working on encrypted health records (PHR). They propose in this article a system for the prediction of diseases and prompt warnings by gathering data from sensors and by applying deep education to evaluate patient health data and monitor them. To safeguard the privacy of health data, we use a safe data deletion method, which allows the data owner to cancel the access of certain users to their health information. Extensive. **Wang, Z., et.al., (2019),** For the fundamental safety of Sensor enabled Wireless networks (SEWNs) a block encryption method is suggested based on the chaotic replacement box (S-box). In this work, they produced a novel S-box, based on the messy map, the chaotic sinusoid map, the Baker map and the generator of a linear congruence. In addition, this study also takes into account the restricted processing power and communication capacity of SEWN. The technique for generating round subkey and F is based on the S-box. The thorough safety and performance experiments indicate that the suggested encryption method is safe and resource-free, which is appropriate for SEWN. **Zhang, W., et.al., (2019),** A chaotic compressive sensing cryptosystem is intended for simultaneous compression - encryption. Compressive sensing needs a measurement matrix to sample a sparse signal compressively and ensure its recovery at the receiver. This article offers a novel one-dimensional chaotic map used to build the chaotic measuring matrix. **Perazzo, P., et.al., (2019),** The Internet of Things (IoT) offers a new generation of innovative services that integrate smart devices with information systems in a seamless way. Such IoT devices produce a continuous information flow which may be sent through a distrustful network and kept on an unconfident infrastructure. The performance assessment indicates that the implementation of ABE on restricted devices is possible, but the costs rise with the number of characteristics. The study shows in particular how ABE has a major effect on battery powered device life that is substantially affected characteristics. **Ghehioueche, A. A., Hubert, N., & Mezrag, F. (2019),** technology Internet's significant technologies. It is used successfully in many applications in the current world, including healthcare, environmental monitoring, tracking, etc. Small sensor nodes with low resources consist of SEWNs. However, the connection between the SEWN components is uncertain. Therefore, it is essential to develop efficient and lightweight cryptographic systems protect the transferred performance of several cryptosystems for SEWNs is evaluated. Our research contains a comparative analysis of the encryption methods examined with respect to power consumption, space memory and computer time. **Gracy, P. L., & Josef, S. (2018),** The security of the Wireless Sensor Network (SEWN) is a significant problem in the present age. The data must be transferred securely between two nodes to encrypt each node information. Therefore, the algorithm Honey Encryption (HE) is employed in SEWN. Seeds are utilized here, containing different words. When attackers encrypt the data using the incorrect encryption key, HE returns a sweet message (i.e., fake plain-text). This content may appear genuine, but it is not. An attacker may thus end up with an incorrect message. In contrast to other methods, our experimental findings indicate that Honey Encryption provides superior performance.

III. ANALYSIS OF SENSOR SECURITY AND ENGAGING THE ROOT PATH OF THE NETWORK THROUGH ENCRYPTION

The physical layer encryption (PLE) offers a strong safety measure, which is significantly different from high layer encryption methods, as a solution to severe security transmission issues in wireless communication. PLE may benefit from fundamentally distinct from conventional Boolean algebra cryptography. A broad cipher signal space and key area are provided in the proposed PLE architecture, offering more design freedom and. Transmission safety has become a highly significant problem with the fast growth of wireless communication technologies. Because of the wireless broadcasting characteristics, the to the private communication issue and linked secrecy and dependability closely. However, the recent development of sophisticated contemporary theories of cryptography is divorced from the basis of wireless communication [14,15].

Modern cryptography investigates, on the one hand, encryption via error-free transmission. We merely assess the dependability and efficiency of communications networks, on the other hand. There are separately constructed and few overlaps with a communication and security layer of a real. Moreover, current PLE publications lack accurate extremely essential for the construction of provide the appropriate criteria to evaluate PLE safety. One of the primary purposes of this article is to create rudimentary PLE cryptographic and to describe the fundamental design principles. This paper's major contributions are:

1) Here this research is to split broad mathematical models are developed and the blocks are defined.

2) The design framework and fundamental principles of be proposed.

3) isometry and stochastic processes in PLE block will be defined. We will demonstrate that both KPA and CPA can comply with the proposed PLE frameworks. The remainder of this paper is structured accordingly.

3.1 PLE System Model and Cryptographic Primitive

The conventional safety method is presumed to provide an error-free equivalent route for encryption and decryption blocks. We presume that the. PLE will take this issue into consideration and integrate encryption and communication components.

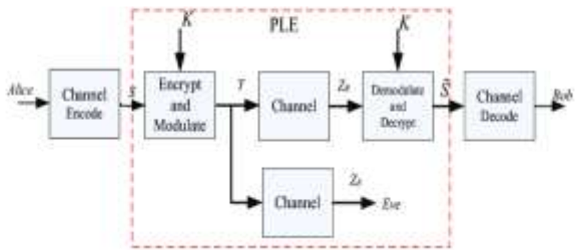

Figure 1 PLE Communication system model

The key still has to be disseminated since it is faced with a realistic the following communication module will then be processed and transmitted over the channel. PLE really requires encryption to be taken into account but must also address problems of transmission efficiency and dependability. PLE may be seen as a novel cryptography extension on complicated fields and non-error-free channels [10-15].

3.2 SEWN or WSN integration module presented scenario of intruders

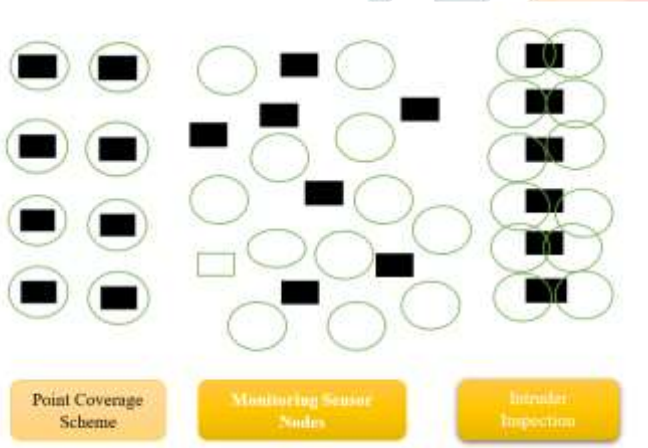

Figure 2 SEWN or WSN integration module presented scenario of intruders

senses since uncertainties are not taken into consideration in the node monitoring and physical signals. When the node sensing radius is inside the sensor, a monitoring point is covered or detected.

$$P_{cov}(s_i, m_j) = \begin{cases} 0 \; if \; d(s_i, m_j) \le r^p \\ 1, \quad otherwise \end{cases}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Then the Euclidean distance between two nodes can be expressed as

$$d((s_i, m_j) = \sqrt{(x_i - x_j)^3 + (y_i - y_j)^3 + (z_i - z_j)^3}, \ldots\ldots\ldots\ldots(2)$$

$$p_{co}(s_i, m_j) = \begin{cases} 0, & d(s_i, m_j) \le r_1, \\ e^{-p(d((s_i,m_j)-r_j^{ij}, r_1 < d(s_i,m_j) \le r^p}, & \\ 1, & d(s_i, m_j) \ge r^p \end{cases} \ldots\ldots\ldots\ldots(3)$$

Clustering of sensor nodes is an efficient topology control technique that optimizes network use of energy. In different SEWN applications, many clustering methods were employed. To that effect, presents an energy consumption model that is widely employed, specifically equations (4) and (5).

$$E_{TX}(K_1, d) = \begin{cases} E_{ele} + \varepsilon_{fs} \times d^3) \times k_1, d \le d_0 \\ E_{ele} + \varepsilon_{fs} \times d^5) \times k_1, \; d > d_0 \end{cases} \ldots\ldots\ldots\ldots(4)$$

$$E_{TX}(k) = E_{ele}^3 \times k_1 \ldots\ldots\ldots\ldots(5)$$

The previous equation and does not take energy usage into account. The Wireless Data Sheet energy consumption model may be used as a means of making.

$$E_i = \sum_{state\ j} P_{state\ j} \times k_{1+} \sum E_{state\ j} \ldots\ldots\ldots\ldots(6)$$

The grid technique is often utilized in preset deployment methods for accurate placement of the sensor nodes at the given grid locations. The network used by this technique may to some degree enhance network coverage and connection. The Kano model is based on analyzes of the user satisfaction effect and represents the non-linear relationships between user happiness and user satisfaction. The ordinate is the pleasure of the user [7-9]. The higher the greater the fulfilled, the lower the unhappier; the abscissa indicates how far there is a certain need., therefore the grid size must be chosen according to the SEWN density [3-5]. A compact grid helps to reduce coverage gaps for high-density grids, which increases network stability. However, a in sparse networks since it may minimize duplicated network coverage, thereby ensuring full use of the node's sensory capacity. For the SEWN life cycle, energy use control is extremely important. In the same situation, the less, the current security scenario includes a new energy consumption model in accordance with reality. Three components are considered as the consumption of energy: firstly, the energy consumption in order to perform the sensing task; secondly, during wireless communication; and thirdly, energy consumed by nodes after optimized use to move distance [11-17].

$$E_{\propto} = n.\sum_{i=1}^{m} (r_i^p)^2 \ldots\ldots\ldots\ldots (7)$$

The higher the deployment. However, because node batteries cannot be replenished, the network's life cycle energy consumption and the lower area, the more effective it is to reduce the network voids and simplify second network implementation.

$$\begin{cases} f_1(I) = \min(C_r(I)) \\ s.t. \; A(s_i) \quad \epsilon \quad H_2 \end{cases} \ldots\ldots\ldots\ldots (8)$$

A high-precision technique has been utilized to compute the exact three-dimensional position of the target using the signal reach angle and finally with the mathematical triangulation process. The cost of this measurement technique is extremely costly and involves very specialized many of which have no such scope or placement in small features, and others may have high-end equipment [16-17].

IV. RESULT AND SIMULATION

Various SEWN applications need various degrees of monitoring coverage. The coverage needs thus vary depending on the application situation and this important aspect must first be addressed in designing the deployment strategy.

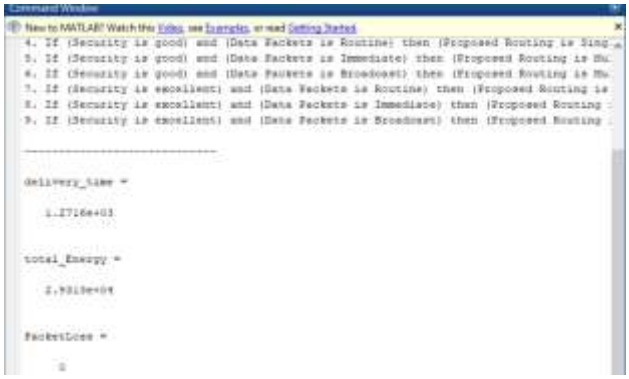

Figure 3. Screen layout of the Code

Point coverage aims to monitor such that fixed places are covered efficiently (target points). Point coverage may generally be considered to be a special area coverage situation, if sensor node numbers are not considered.

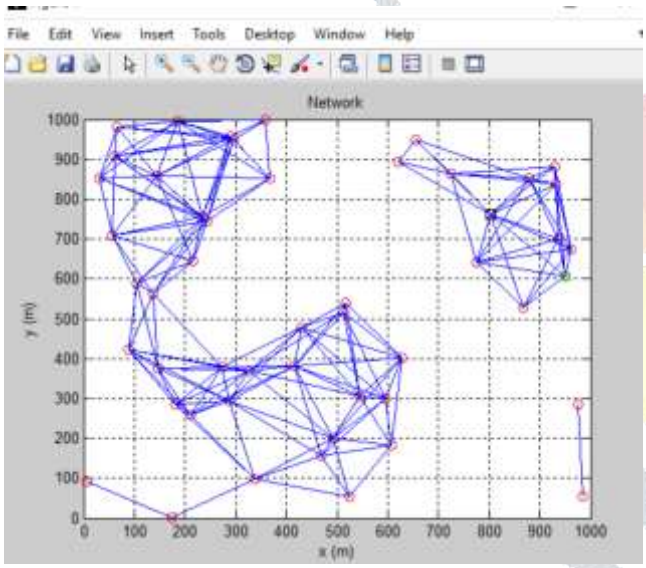

Figure 4 SEWN initialize with Fence coverage having whole surveillance

Fence coverage refers to the monitoring of sensor nodes and the surveillance of. that breach the border or enter a protected region. The fundamental need is to construct a sensor fence in order to continuously insulate the region covered by sensors in the fence from intrusion sensing, as shown in Figure as presented above. In the case of fence coverage, the interferer typically enters the fence sensing network with the lowest chance that it is not detected. The primary objective in the area coverage is to cover the whole surveillance locations there as illustrated in Figure above. The SEWN be changed in real time and the areas coverage is frequently complete; the whole area is covered by the SEWN.

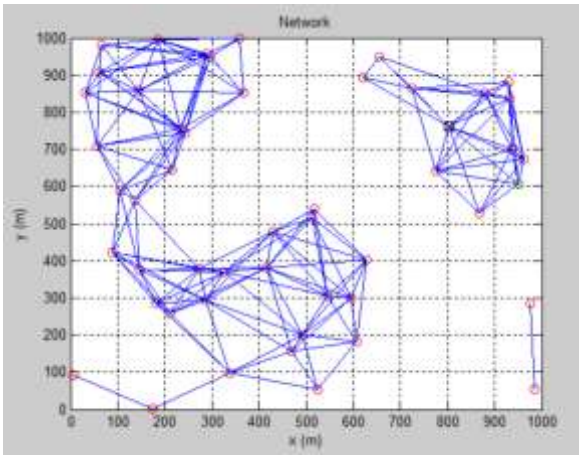

Figure 5 SEWN initialize monitoring region further continue

Full coverage means that at least one sensor node is identified everywhere in the area and helps to optimize the usage. This kind of network employs a high number of sensor nodes in order to monitor a wide region in which the operation circumstances are often severe, if not hostile to the sensor nodes themselves. In contrast, the SEWN nodes are severely resource constrained because to their low processing capabilities, limited memory capacity, and restricted energy supplies. Because these networks are often installed remotely and unsupervised, they need security to protect themselves against attacks such as node capture, physical disruption, eavesdropping, service denial, and other forms of denial of service. As the above figure illustrated that the SEWN communication running and the route has been established.

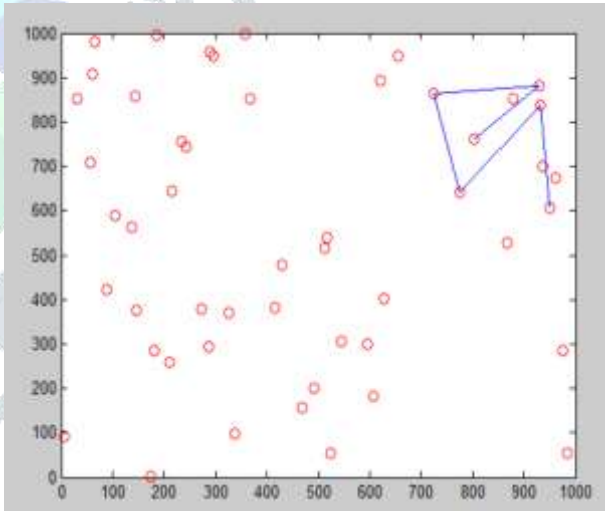

Figure 6. SEWN initialize monitoring region in last stage

As a result of the decentralized nature of SEWNs and the lack of accessible infrastructure, security techniques in SEWNs. In real-world SEWNs, it is not reasonable to assume the nodes to be trustworthy. As the above figure presented that the nodes are communication at in very last stage.

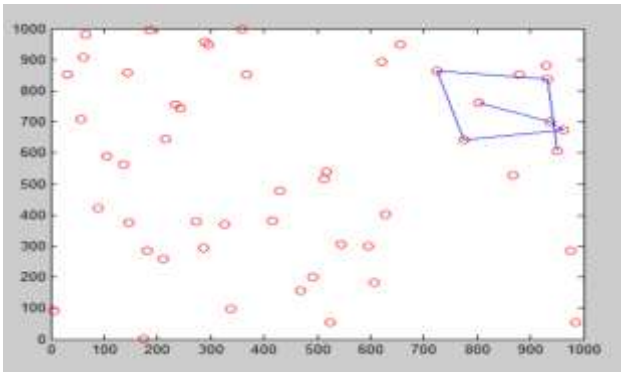

Figure 7. SEWN initialize monitoring region in last stage Done

As in figure above presenting the last communication has been running. The path has been largely been defined as gathered all the necessary data to the central unit of the SEWN network.

4.1 Result Drawn as follow

Proposed Scenario:

Ans =

Routing Case 1: If (Security is poor) and (Data Packets is Routine) then (Proposed Routing is Discard)

Routing Case 2: If (Security is poor) and (Data Packets is Immediate) then (Proposed Routing is Multiple)

Routing Case 3: If (Security is poor) and (Data Packets is Broadcast) then (Proposed Routing is flood)

Routing Case 4: If (Security is good) and (Data Packets is Routine) then (Proposed Routing is Single)

Routing Case 5: If (Security is good) and (Data Packets is Immediate) then (Proposed Routing is Multiple)

Routing Case 6: If (Security is good) and (Data Packets is Broadcast) then (Proposed Routing is Multiple)

Routing Case 7: If (Security is excellent) and (Data Packets is Routine) then (Proposed Routing is Single)

Routing Case 8: If (Security is excellent) and (Data Packets is Immediate) then (Proposed Routing is Single)

Routing Case 9: If (Security is excellent) and (Data Packets is Broadcast) then (Proposed Routing is Multiple)

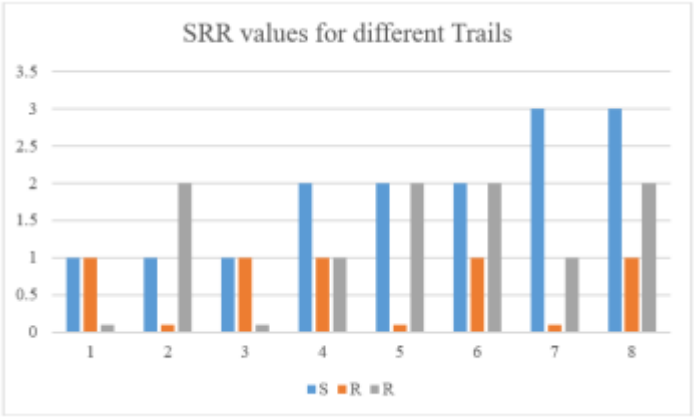

Figure 8. SRR values for different trails (where Security is poor=1, Security is good=2, Security is excellent =3, Data Packets is Routine=1, Data Packets is Immediate=0.1, Data Packets is Broadcast=1, Routing is Multiple=2, Routing is Single=1, Routing is flood=0.1)

The level of SSR (Security (S), Data packet Routing (R) and Packet Flow Routing (R) has been illustrated in above example in logical manner to investigation the security check for SEWN proposed network.

Delivery time = 1.4137e+03 = 1412.7 mili second

Total Energy = 3.4571e+04= 34571.04 mili joule

Packet_Loss = 0

As the result has been drawn the three key factors has been extracted after the end of communication as deliver time, energy and loss of data packets. The result has been analytical and extracted after each communication set up.

Table 1. Comparison Table

Authors	Title of Research	Technique	Discussion
C. Karlof and D. Wagner	Secure Routing in wireless sensor networks attacks and countermeasures	This article describes the security objectives that network routing settings must satisfy in sensor networks. It shows the best approach to include these assaults in the fight against ad hoc and peer-to-peer networks.	This article shows that existing routing methods for sensor networks are vulnerable and identifies an open issue for the future to solve.
C. Schurgers and M.B. Srivastava	Energy efficient routing in wireless sensor networks	In conventional routing protocols, a node only has a certain amount of energy and thus a routing protocol designed around previous routing protocols would not consider how to utilize that energy most efficiently.	Two localized algorithm strategies are proposed for extended sensor network lifespan in this study. Reducing the amount of energy used during transmissions by aggregating packet streams. Completing the task of obtaining more consistent resource usage by using the multi-hop nature of the network connections.
G. Kaur	Review paper on reliability of wireless sensor networks	Here, the different energy-saving methods have been covered in this article. This helps the reader to get an understanding of the different methods that are now known for reliably transporting data in sensor networks and reducing energy usage.	WSN application requires unique reliability positions. To minimize the management and retransmission overhead, communication protocols for WSN should be reliable and energy-efficient. WSN dependability research is examined in this article.

Proposed	Sensor security and Routing Techniques For SEWN	This research proposed three key factors has been extracted after the end of communication as deliver time, energy and loss of data packets.	As a result of this study, three important variables have been identified and retrieved at the conclusion of the communication: delivery time, energy consumption, and data packet loss. Every communication setup has produced an analytical result, which has been retrieved after each communication setup.

V. CONCLUSION AND FUTURE SCOPE

The coverage optimization issue for SEWNs is analyzing sensor security and encrypting the network's root route. The grid technique is widely used in both preset and real-time deployment processes to ensure that sensor nodes are correctly placed on the grid. This technique's network may improve network coverage and connectivity. The higher the right, the lower the left. Compact grids assist minimize coverage gaps and therefore improve network stability in high density grids. Many studies have proposed safe and efficient routing algorithms, secure data aggregation techniques, and so on. Because SEWNs are decentralized and have no access to network infrastructure, security solutions must include inter-node cooperation in addition to secure routing and data aggregation. In real-world SEWNs, nodes are not trustworthy information providers. Their goal is to create a sensor confidence model that can handle problems that traditional cryptography can't handle. Physical attack vulnerability is a significant problem in SEWNs due to unsupervised and unsecured sensor nodes.

References

1. Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in Sensor enabled Wireless networks. *Ad Hoc Networks*, *115*, 102448.
2. Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, *176*, 102917.
3. Li, Z., Peng, C., Tan, W., & Li, L. (2021). An efficient plaintext-related chaotic image encryption scheme based on compressive sensing. *Sensors*, *21*(3), 758.
4. Li, M. (2021). Automatic Encryption Method of Sensor Network Capture Data Based on Symmetric Algorithm. *Wireless Personal Communications*, 1-15.
5. Arpaia, P., Bonavolontá, F., & Cioffi, A. (2020). Problems of the advanced encryption standard in protecting Internet of Things sensor networks. *Measurement*, *161*, 107853.
6. Guerrero-Sanchez, A. E., Rivas-Araiza, E. A., Gonzalez-Cordoba, J. L., Toledano-Ayala, M., & Takacs, A. (2020). Blockchain mechanism and symmetric encryption in a wireless sensor network. *Sensors*, *20*(10), 2798.
7. Ramasamy, J., & Kumaresan, J. S. (2020). Image encryption and cluster-based framework for secured image transmission in Sensor enabled Wireless networks. *Wireless Personal Communications*, 1-14.
8. Ge, C., Yin, C., Liu, Z., Fang, L., Zhu, J., & Ling, H. (2020). A privacy preserves big data analysis system for wearable wireless sensor network. *Computers & Security*, *96*, 101887.
9. Tanveer, M., Abbas, G., Abbas, Z. H., Waqas, M., Muhammad, F., & Kim, S. (2020). S6AE: Securing 6LoWPAN using authenticated encryption scheme. *Sensors*, *20*(9), 2707.
10. Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A novel block encryption algorithm based on chaotic S-box for wireless sensor network. *IEEE Access*, *7*, 53079-53090.
11. Fang, W., Zhang, W., Zhao, Q., Ji, X., Chen, W., & Assefa, B. (2019). Comprehensive analysis of secure data aggregation scheme for industrial wireless sensor network. *Computers, Materials and Continua*, *61*(2), 583-599.
12. Girgenti, B., Perazzo, P., Vallati, C., Righetti, F., Dini, G., & Anastasi, G. (2019, June). On the feasibility of attribute-based encryption on constrained IoT devices for smart systems. In *2019 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 225-232). IEEE.
13. Ghehioueche, A. A., Chikouche, N., & Mezrag, F. (2019, November). Performance Evaluation and Analysis of Encryption Schemes for Sensor enabled Wireless networks. In *2019 International Conference on Digitization (ICD)* (pp. 187-191). IEEE.
14. Gracy, P. L., & Venkatesan, D. (2018). A honey encryption based efficient security mechanism for Sensor enabled Wireless networks. *International Journal of Pure and Applied Mathematics*, *118*(20), 3157-3164.
15. Khoury, E., Medlej, M., Abou Jaoude, C., & Guyeux, C. (2018, April). Novel order preserving encryption scheme for Sensor enabled Wireless networks. In *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* (pp. 1-6). IEEE.
16. Cha, H. J., Yang, H. K., & Song, Y. J. (2018). A study on the design of fog computing architecture using sensor networks. *Sensors*, *18*(11), 3633.
17. Sivamani, S., Choi, J., Bae, K., Ko, H., & Cho, Y. (2018). A smart service model in greenhouse environment using event-based security based on wireless sensor network. *Concurrency and Computation: Practice and Experience*, *30*(2), e4240.