Research Article

Study Of Energy Efficient And Secure Routing Mechanisms In Wireless Sensor Network

[1]C. Nithya Praba, [2]Dr. D. Kalaivani.

[1]Research Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
[2]Assistant Professor, Department of Computer Technology, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract - Wireless Sensor Network (WSN) is a group of Sensor Nodes (SN) correspond with each other and sharing the information between the networks. SN are low power and low cost devices are used to construct the network. Sensor based networks are used in various integrated applications. One of the most benefited sensor based application is Healthcare applications. In Healthcare applications, the physical components are data sources and collected information's are transmitted through the network in the mode of intermediate node access. All the physical components or sensors are battery powered in nature, so the energy was play a vital role in Healthcare-WSN (HWSN) applications. Nodes energy will decide the utilisation of the network and accurate data transmission between the nodes. The future of WSN is purely dependent on the Energy saving mechanism and now it is create a new dimension of research constraint. Now, the researchers focusing on the Energy efficient and secure techniques for improve the lifetime of the network and safest data transmission between the nodes and the server. In this paper, various energy efficient mechanisms are analyzed for prolong the network and also review the various secure mechanisms to improve the security of the HWSN applications.

Keywords: - WSN, Sensor nodes, IoT Applications, Energy Consumption, Energy Harvesting, Encryption, Fuzzy Logic.

1. INTRODUCTION

WSN includes SN that have the capability of self-configuration and are so clean of their deployment in the target region. WSNs have a few boundaries in provisions of battery capacity, data transmission, storage and processing.

Energy performance is one of the most critical factors in the design of the WSN. Since WSN is applied in many adversarial and harsh situations, supplying energy supplies or recharging facilities is not always feasible. The entire network must face the challenge posed by the built-in batteries. If a few nodes die due to low battery power, this can cause a complete network failure known as network partitioning, so one of the most important components is to extend the WSN's existence. [15]. WSNs have a number of energy-saving methods, and built-in energy technology and batteries are continually improving. WSN's clustering mechanism can be used to achieve energy efficiency. Clustering is a method of grouping together multiple SN to complete a task. The cluster head is in charge of all the nodes of its own cluster. When compared to non-cluster WSN, the routing process in cluster-based WSN is extremely simple and fast. The CH helps the routing protocol to efficiently send data across the network. [14].

Energy-efficient routing is applicable to multi-hop wireless networks in general, including WSN. Multi-hop wireless networks, as opposed to individual wireless networks, exchange information among nodes. The explanation is that without a centralized system, the maximum number of wireless multihop networks is distributed. It is difficult to design the proper growth of the network life, which is primarily dependent on WSN routing. In terms of energy consumption, the necessary routing protocol in WSN should be efficient.

Developing a wireless healthcare application brings with it a slew of different experiences, such as efficient transmission of data, node mobility support, and rapid event identification, timely data distribution, power management, node computing, and middleware. [21-22]. However, the introduction of emerging technology in healthcare applications without taking into account protection also leaves the privacy of patients vulnerable. Analysis of: I the potential risks to a wireless healthcare application without adequate security; and (ii) privacy concerns. Before addressing security concerns in wireless healthcare applications, it is worth assuming the size of deployment of health care applications using WMSNs. Wireless healthcare capabilities include emergency response, access to clinical data, electronic health records, and other features that are not restricted to patient mental and physical data monitoring. Individuals also share their data with physicians (in a doctor-patient relationship), insurance companies (for insurance protraction), exercise coaches (as sports team trainers), and families (as family support for recovery). There is also value in addressing privacy issues that are ethical from a social perspective.

The electronic medical record system (EMR) [1] is responsible for gathering information during diagnosis and care, such as text, icons, charts, graphics, photographs, etc. Such details will later be used to support the decision-making of physicians and nurses. EMR should be safe from forgery, tampering and repudiation [2]. The patient's EMRs can be considered as a collection of static medical records. The digital signature of each person medical record will protect the confidentiality of the information in identity verification, authorization management and the allocation of responsibility. As a result, how to adequately save computing and storage overhead digital signatures for batch medical records has now become a fascinating topic. At nearly the same time, the criteria for safe EMR storage and access are met.

This paper is structured as follows. Section 2 reviews the various methodologies for energy efficiency and secures the patient's electronic records and also summarizes the literature review. In section 3, the research is identified and overview the proposed solution for the problem definition. Section 4 describes the performance evaluation parameters and metrics for HWSN. Section 5 concludes the paper and analyzes the essential boundaries at the same time as designing a mechanism for WSN.

2. RELATED WORK

The problem of energy efficiency is a key concern for HWSN. The power usage of the node is spread over its various operations. Most SN are deployed with batteries and have a short lifespan, thus prolonging lifespan is of crucial importance [13]. The purpose of this work is to improve the life of the network. And security is another major challenge to WSN healthcare. Due to the computationally intensive nature of security algorithms, most WSN applications do not even consider security [20]. However, when the network monitors and transmits confidential data, security becomes a crucial issue that must be tackled. Even if the data being transmitted is not sensitive, it is important to ensure the authenticity of the neighbor to whom the data is being passed and that the recipient is assured that the data is not being changed (data integrity). A wireless network's security requirements include confidentiality, data integrity, authentication, non-repudiation, and availability.

Shen, L., et al. (2016) proposed the usage of WSNs in a number of healthcare based monitoring systems, potentially reducing the need for healthcare professionals [3]. Sensors on or in patients generate scientific statistics that may be effortlessly manipulated via a huge range of scientific gadget assaults. While signature schemes can ensure the accuracy and credibility of records, as the number of users in the clinical device grows, bandwidth and garage costs may additionally skyrocket, rendering present day signature schemes useless for WSNs. Based on an improved protection model, the proposed work gear an efficient mixture signature template for healthcare WSNs that could combine several signatures into a single combination signature. The length of such a combination signature can be as long as that of an man or woman, doubtlessly decreasing the fee of bandwidth and community device considerably.

Gautam, S., et al. (2017) The proposed protocol established a reference point for the absorption of communication energy, the cultivation of productive chunks and the calm promotion of network resources such as bandwidth, etc [4]. This paper confers on EERA the data aggregation foundation of the wireless sensor network. Structure efforts as a middleware to combine information that is compatible with a total of nodes within a network. The core goal of information gathering algorithms is to bring together and strengthen the quality of corporate information in such a way that the network duration is extended. The aim of the planned output is to analyze the act of TAG in terms of energy capability in analogy with data aggregation in WSN and to fix the accuracy of the protocol in an environment where the storage is finite.

Hamzah, A., et al. (2020) proposed a fuzzy logic based cluster head selection. The proposed model employs a node may become a CH [5]. In the proposed fuzzy logic model a Fuzzy Logic-based Energy-Efficient Cluster for WSN based on a minimum separation distance between CHs (FL-EEC/D) was introduced and furthermore, the Gini Index is used to measure the energy efficiency of clustering algorithms in based on its ability to balance the energy distribution across WSN sensor nodes. Contrast the suggested FL-EEC/D technique with a fuzzy logic-based CH election approach, k-means clustering, and LEACH. The results show a rise in the number of first nodes and half nodes that are dead.

Zaman, N., et al. (2015) describes a very resource-intensive network class in which one of the key concerns is energy consumption In this research, a cross-stage design technique called "Location Sensitive Routing Protocol" was used to construct an energy-efficient routing protocol (PRRP) [6]. PRRP is meant to decrease electricity intake in every node by means of (1) lowering the time the sensor node is idle listening and (2) lowering the average verbal exchange distance across the community. The proposed PRRP's performance was significantly evaluated in terms of network life, throughput, and electricity consumption of the community on a character and records packet basis. The findings of the look at had been analyzed and compared with the famous LEACH and CELRP protocols.

Nguyen, T. D., et al. (2017) introduce energy-harvesting-aware routing protocols for heterogeneous WSN-based IoT applications in the context of ambient energy sources [7]. The proposed work incorporates a new Energy Harvesting Aware Routing Algorithm that is enhanced by incorporating a new approach known as 'extra backoff.' Under variable traffic load and energy availability conditions, the proposed algorithm extends the life of the SN and improves the quality of service (QoS). In terms of network life, simulation results show that our algorithm outperforms the existing Randomized Minimum Path Recovery Time (R-MPRT) algorithm by about 50%.

Abdullah, K. M., et al. (2018) WSNs has urbanized quickly in modern years. They have been based on a variety of leading technologies [10]. They have been major players in a variety of fields, including emergency services, the military, traffic monitoring, environmental protection and medical services, among a wide range of fields. However, with the quick growth of WSN tools, the threat of tools implementation without the necessary protection has been a major challenge faced by a large number of facilities; hence the need to strengthen the WSN safety systems. The proposed work is aimed at proposing a hybrid safety protocol for WSN.

Pritchard, S. W., et al. (2018) Proposed, because of the point of interest on architecture, addressing the safety element of SDWSN has received little attention [11]. Since this paradigm is an aggregate of WSN and

SDN, positive strategies from each paradigm may be modified to account for SDWSN. One of the main demanding situations with imposing safety inside WSN is the inherent problems, which include useful resource constraints. However, most of those troubles had been resolved as a result of the SDN paradigm's centralized management, leaving room for the implementation of WSN protection. To analyze using WSN cryptography within SDWSN, cryptography methods have been carried out within an SDWSN network if you want to confirm whether the SDWSN paradigm does permit for aid extreme WSN security implementations.

Tawalbeh, H., et al. (2017) Describing the relationship that includes the transmission of vital information in many cases requires the defense of such data against potential attacks [12]. But secure communication in Wireless Sensor Networks comes at a high cost of efficiency, as components in WSNs typically have limited computing and power capabilities. Securing information in this restricted setting involves light encryption algorithms, as existing public-key and private-key encryption algorithms involve large computations. In this paper, present and analyze lightweight cryptographic approaches because they are believed to be among the most adequate solutions for the security/performance trade-off in WSNs.

3. PROBLEM DEFINITION

Sensors, which are used in a range of medical instruments used in hospitals, clinics, and households, provide patients and their healthcare providers with insights into physiological and physical health situations that are crucial to the detection, diagnosis, treatment, and management of illnesses. Recent advancements in wireless sensor networks have created a platform for a variety of healthcare applications. It has become an active research field due to its large-scale capability. Sensor networks have the ability to have a major outcome on a lot of areas of health care. By equipping patients with wireless, wearable vital sign monitors, the collection of accurate real-time physiological status data can be greatly simplified. There is, however, a major difference between the current sensor network networks and the needs for medical treatment. Medical sensor networks, in particular, must promote multicast routing topologies, node mobility, a broad range of data rates and high levels of reliability and safety. This research includes the application of WSNs specifically in the field of healthcare. [19].

For wireless sensor networks, energy efficiency is a major concern (WSN). Since SN are usually powered by a battery, energy consumption must be carefully regulated in order to prolong the device's life. However, the volatility and variability in energy supply necessitate a sophisticated energy management system, i.e. the energy demand of each sensor node at any time does not surpass its available energy. Security is an integral component of every kind of structure. Defense has been represented in a number of ways by different people. It is a common fact that protection is always of great importance, regardless of how it is thought or described. [16] Formal paraphrase Numerous security threats may emerge as a result of the wireless nature of communications in healthcare sensor networks applications. These threats and attacks may have a significant impact on a person's social life if they use wireless sensor devices. Certain cases, such as the subject's status, may have drastic implications if it is jeopardized. Security concerns in sensor network-based healthcare applications have long been a source of concern. In recent years, security issues in wireless sensor networks in general have been a major focus of research.

4. PROPOSED METHODOLOGY

Medical sensor networks, when absolutely carried out, can decorate healthcare facilities starting from pressing scenario reply to in-health facility verbal exchange, out-affected person surveillance, and environmental monitoring. Sensor node gadgets are defined as having limited to be had assets, reminiscence, bandwidth, and computational energy. These sensor-node-particular influences impose many constraints on the security architecture. Since cryptographic algorithms can most effectively use a fraction of total memory, the safety structure wishes them to be very lightweight and execute in an affordable quantity of time. Because of the machine's constrained bandwidth, the accelerated overhead vital to offer the safety facility must not have an extensive impact on the device's typical overall performance. [17].

WSN based networks are greater vulnerable to cyber attacks compare with conventional networks. Risk identification is primarily based on distinct varieties of lively and passive attacks which can arise in routing and packet forwarding. Routing attacks are advertising routing changes that don't observe routing protocol specifications, even as packet forwarding attacks purpose information packets to be transmitted in a manner this is deliberately incompatible with routing states. Energy quality (EE) and energy supply are important concerns for WSNs. In contrast to energy-efficient MAC protocols, efficient routing protocols are critical for the creation of energy-efficient multi-hop WSNs [18]. The most important aim of routing protocols is to not only transfer data from source to destination, but also to do so in an energy-efficient manner to ensure to prolong the life of WSNs.

The proposed energy-efficient and reliable wireless communication in WSN offers authenticity, honesty and confidentiality in order to rule out the possibility of false data transmission. The proposed work addresses the issues of limited resources, anonymity, message credibility and validity in the Healthcare Wireless Sensor Network (HWSN). In the proposed work, the Public Key Certificate, also known as the Digital Certificate or Identity Certificate, is an electronic document used to show ownership of the public key. The certificate shall contain information on the key, the identity of its owner and the digital signature of the body that has validated the content of the certificate. The updated ECDSA certificate is a public key certificate where the public key and

both the certificate signature keys are extracted from the elliptical cryptography of the curve. The proposed work consists of the following steps,

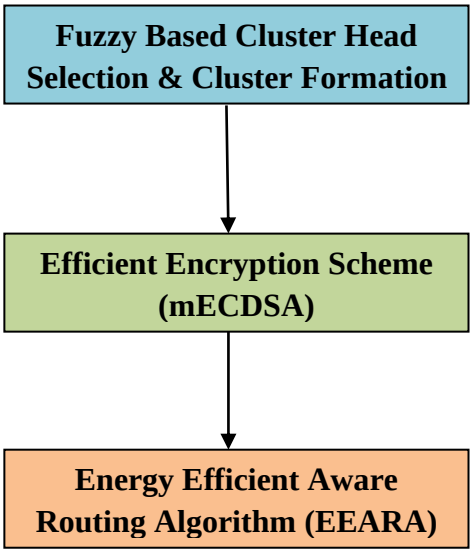

Fig. 1: - Workflow of Proposed Work

However, the costs of increased protection include ever-increasing overheads for computing, communications, and management. There are questions about network effects in popular of scalability, provider performance, and robustness as a result of the usage of security improvements in a functional resource-constrained sensor community. It definitely has to be found that safety and network reliability are similarly important, and a nicely-designed give-up-to-cease protection structure is the main precedence for reaching WSN usability in healthcare packages.

5. PERFORMANCE ANALYSIS

The evaluation of the proposed new energy-efficient and reliable wireless communication for WSN has been carried out for a number of parameters [19, 20].

- **Packet Delivery Ratio (PDR)**

The ratio of the number of data packets received to the total number of data packets sent by the source.

$$\textbf{PDR} = \frac{\textbf{Number of packet received}}{\textbf{Number of packets send}} \textbf{ X 100}$$

- **End -To-End Delay**

The average time elapsed for delivering a data packet within a successful transmission from source to destination.

$$\textbf{Delay} = \frac{\textbf{Inter arrival of 1st packet \& } 2nd\ packet}{\textbf{Total no. of packets received by all destination nodes}}$$

- **Packet Lost**

When a router is overwhelmed and cannot accept any incoming data at a given time, data packets are discarded in a network.

$$\textbf{Packet Lost} = \textbf{Total No. of packet received} - \textbf{Total No. of packet send}$$

- **Energy Consumption**

The total network energy consumption includes transmission and processing energy consumption for both data and control packets.

$$\textbf{Energy Consumption} = \frac{\textbf{Energy Consumed in ideal, sleep, transmit and receive}}{\textbf{Total energy consumed}}$$

5. CONCLUSION

It is known that WSN is a resource-constrained network in which energy constraint is frequently the primary subject, since WSN operation is a great deal dependent on the duration of the node sensor battery. The WSN places a priority on energy conservation and stability. This paper also analyzes many energy efficient mechanisms and security problems. The proposed work incorporates a new energy efficient and stable mechanism for WSN. The problem definition is clearly addressed and proposed the solution called Energy

Efficient Aware Routing Algorithm to resolve the heterogeneity of functions in heterogeneous WSN-based healthcare applications.

6. REFERENCES

[1] Zuckerman, A.E.: Restructuring the electronic medical record to incorporate full digital signature capability. Proc. Amia. Symp. 8(1), 791–795 (2000).

[2] Yu, Y.C.: Dual function seal: visualized digital signature for electronic medical record systems. J. Med. Syst. 36(5), 3115–3121 (2012).

[3] Shen, L., Ma, J., Liu, X., & Miao, M. (2016). A provably secure aggregate signature scheme for healthcare wireless sensor networks. Journal of medical systems, 40(11), 1-10..

[4] Gautam, S., Kumar, A., & Kaur, S. (2017, August). Energy efficient routing algorithm with multihop data aggregation. In 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) (pp. 1-6). IEEE.

[5] Hamzah, A., Shurman, M., Al-Jarrah, O., & Taqieddin, E. (2019). Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks. Sensors, 19(3), 561.

[6] Zaman, N., Tang Jung, L., & Yasin, M. M. (2016). Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol. Journal of Sensors, 2016.

[7] Nguyen, T. D., Khan, J. Y., & Ngo, D. T. (2017, May). An effective energy-harvesting-aware routing algorithm for WSN-based IoT applications. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[8] Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), 262-275.

[9] Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2020). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-20.

[10] Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2018, June). Cryptography methods for software-defined wireless sensor networks. In 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE) (pp. 1257-1262). IEEE.

[11] Tawalbeh, H., Hashish, S., Tawalbeh, L., & Aldairi, A. (2017). Security in Wireless Sensor Networks Using Lightweight Cryptography. Journal of Information Assurance & Security, 12(4).

[12] Dattatraya, K. N., & Rao, K. R. (2019). Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. Journal of King Saud University-Computer and Information Sciences.

[13] Agarwal, A., Gupta, K., & Yadav, K. P. (2016, March). A novel energy efficiency protocol for WSN based on optimal chain routing. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 368-373). IEEE.

[14] Chidean, M. I., Morgado, E., Sanromán-Junquera, M., Ramiro-Bargueno, J., Ramos, J., & Caamano, A. J. (2016). Energy efficiency and quality of data reconstruction through data-coupled clustering for self-organized large-scale WSNs. IEEE sensors journal, 16(12), 5010-5020.

[15] Wang, Z., Qin, X., & Liu, B. (2018, April). An energy-efficient clustering routing algorithm for WSN-assisted IoT. In 2018 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[16] Roy, N. R., & Chandra, P. (2019, April). EEDAC-WSN: Energy Efficient Data Aggregation in Clustered WSN. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 586-592). IEEE.

[17] Louw, J., Niezen, G., Ramotsoela, T. D., & Abu-Mahfouz, A. M. (2016, July). A key distribution scheme using elliptic curve cryptography in wireless sensor networks. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN) (pp. 1166-1170). IEEE.

[18] Harbi, Y., Aliouat, Z., Harous, S., & Bentaleb, A. (2018, December). Secure data transmission scheme based on elliptic curve cryptography for internet of things. In International Symposium on Modelling and Implementation of Complex Systems (pp. 34-46). Springer, Cham.

[19] Chen, T. M., Blasco, J., & Patil, H. K. (2019). Cryptography in WSNs. In Mission-Oriented Sensor Networks and Systems: Art and Science (pp. 783-820). Springer, Cham.

[20] Koch, S.; Hagglund, M. Health Informatics and the Delivery of Care to Older People. Maturitas 2009, 63, 195-199.

[21] Chung, W. Y., Yau, C. L., Shin, K. S., & Myllyla, R. (2007, August). A cell phone based health monitoring system with self analysis processor using wireless sensor network technology. In 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 3705-3708). IEEE.

[22] Omeni, O., Wong, A. C. W., Burdett, A. J., & Toumazou, C. (2008). Energy efficient medium access protocol for wireless medical body area sensor networks. IEEE Transactions on biomedical circuits and systems, 2(4), 251-259.