IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Energy-Efficient and Secure Routing Protocols for WSN Architectures, Strategies, and Performance.

M Fatima, S Krishnan, K Nayanam
Department of Electrical and Electronics Engineering,
Sunrise University, Alwar, Rajasthan, India
mfat01@gmail.com, snan40@gmail.com, knayanam@gmail.com

Abstract: *Recent developments in low-power communication and signal processing technologies have led to the extensive implementation of wireless sensor networks (WSNs). In a WSN environment, cluster formation and cluster head (CH) selection consume significant energy. the widespread adoption of wireless sensor networks (WSN) has resulted in the growing integration of the internet of things (IoT). However, WSN encounters limitations related to energy and sensor node lifespan, making the development of an efficient routing protocol a critical concern. Cluster technology offers a promising solution to this challenge. This study introduces a novel cluster routing protocol for WSN. A novel energy-saving cluster routing model is designed, which can accurately reflect the real situation of WSN and significantly improve the network performance. In this model, the CH node is responsible for collecting aggregated cluster data, and the relay node (RN) is responsible for sharing data transmission tasks with the CH to balance the load, and transmits data to the BS through reasonable inter-cluster routing. In addition, this study considers key factors such as node location, node energy, base station distance, intra-cluster compactness, inter-cluster dispersion, and node directionality to construct different objective functions for selecting CH and RN and designing inter-cluster routing.*

Keywords: Wireless sensor networks (WSNs),Low-Energy Adaptive Clustering, Hierarchy (LEACH), Secure Positioning for Sensor Networks (SPIN)

I. INTRODUCTION

In these days, wireless sensor network emerging as a promising and interesting area. Wireless Sensor Networks (WSN's) are being used in surveillance, industrial monitoring, traffic monitoring, habitat monitoring, health care monitoring, air pollution monitoring, forest fire detection, land slide detection, water quality monitoring, natural disaster prevention, industrial monitoring, cropping monitoring, machine health monitoring and crowd counting etc. which calls for monitoring before taking an appropriate action. The WSN is built from a few to several hundreds or thousands of nodes, where each node is connected to one or sometimes several sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. Wireless sensor networks (WSN) have acquired intensive popularity due to the wide range of applications in different fields. A recent emerging application is the Internet of Things (IoT), which allows the interconnection of different objects or devices through the world of the Internet . About 5 billion intelligent devices are already connected, and the number is increasing quickly worldwide.The number of people interacting can exceed the number of virtual devices that connect to them. As a result, significant traffic will be generated in which humans are the slightest contributor to this traffic.lenges in designing any sensor network. The nodes may be deployed over a hos tile location owing to the application that makes the battery recharging almost unman agreeable. Moreover, the nodes are expected to perform data acquisition for an indefi nite time to achieve the application requirements. Hence, many researchers are currently engaged in exploring various techniques to extend the network lifetime to achieve high quality of service by balancing the energy consumption over the network .The energy source consists of limited battery power, which is one of the major challenges in designing any sensor network .The nodes may be deployed over a hostile location owing to the application that makes the battery recharging almost unmanaged able .

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Moreover, the nodes are expected to perform data acquisition for an indefinite time to achieve the application requirements. Hence, many researchers are currently en gaged in exploring various techniques to extend the network lifetime to achieve high quality of service by balancing the energy consumption over the network . Wireless sensor network can be categorized into two types:

Unstructured WSN and Structured WSN. In unstructured WSN, the nodes are densely deployed and also the nodes can be deployed in ad-hoc manner in the sensing area or region. In Structured WSN Sensor node developments of some or all nodes are replanted. The nodes placement is also planned. So, the maintenance of structured WSN is much easy as compare to Unstructured WSN.

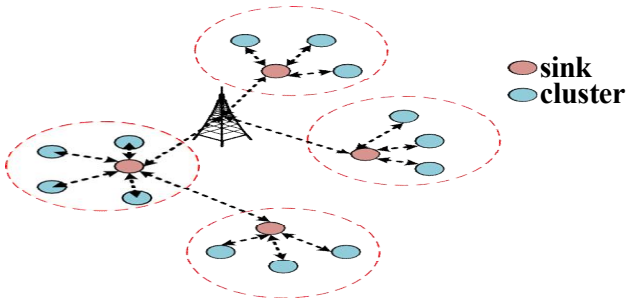

Figure 1. Clustered-based WSN.

Figure 2. (**a**) ADV message. (**b**) REQ message.The clustered network helps the system to maintain a longer life term by scheduling a duty cycle between nodes in a cluster without affecting the normal functionalities of the network The CH sets a time division multiple access (TDMA) schedule for data transmission to prevent any collision of messages. The non-CH node sends its data to the respective CHs with the DSSS (Direct Sequence Spread Spectrum) communication, in which each cluster has its unique.

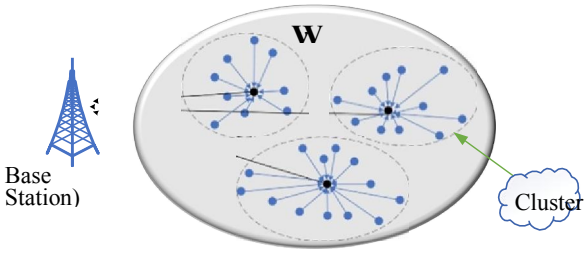

Figure 3. Cluster architecture in wireless sensor networks

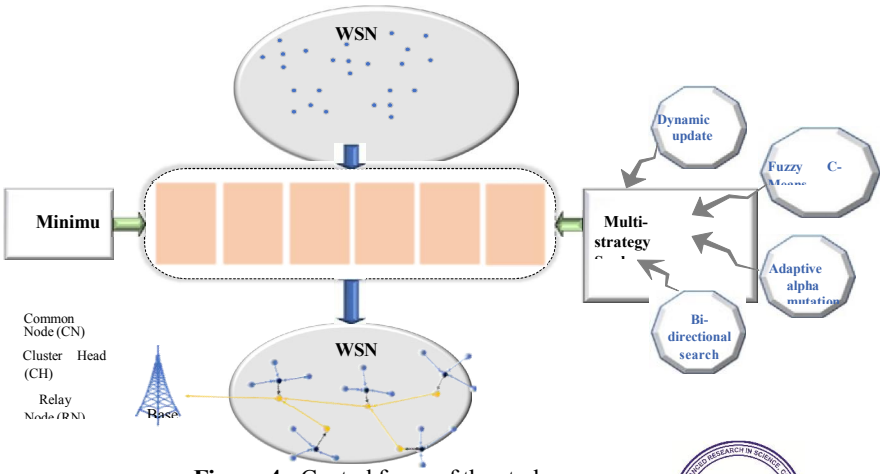

Figure 4. Central focus of the study.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

WSN ARCHITECTURE

The design chart for the WSN architecture is shown Architecture of a WSN The chart portrayed above maps out the general engineering of a WSN, which is delegated single-level and multi-level design, it is essential to think about the usefulness of all segments utilized in this engineering. Standard sound and video sensors catch sound, still or moving pictures and recordings of low goals. Scalar sensors are another kind of sensors that sense scalar information and physical qualities, for example, temperature, moistness and weight, and report estimated qualities to their group head. These are normally asset constrained gadgets as far as vitality utilization, memory stockpiling and preparing abilities. Sight and sound handling hubs act as bunch heads. These gadgets have relatively extensive computational assets and are appropriate for totalling sight and sound streams from singular sensor hubs. This should be possible by different calculations actualized in it. Calculations are equipped for overseeing the stream of control (outlines every second) by including and disposing of casings. At last, it is fit for diminishing both the dimensionality and volume of information passed on to the submerged and capacity appliance.

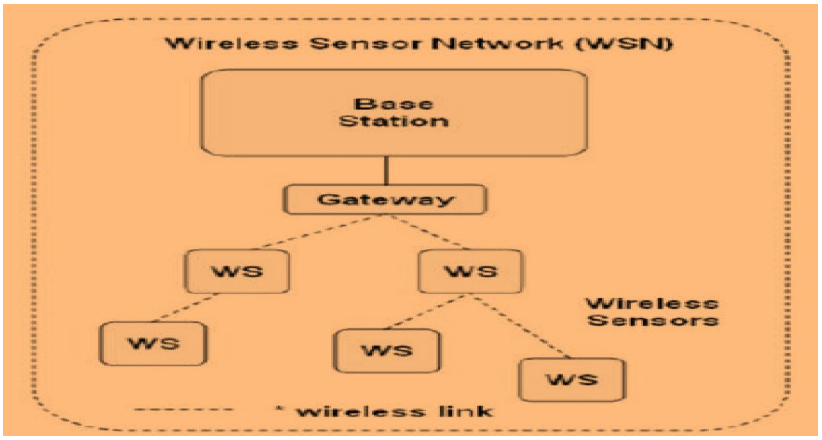

Fig. 5 Architecture of a WSN [1]

The chart portrayed above maps out the general engineering of a WSN, which is delegated single-level and multi-level design, it is essential to think about the usefulness of all segments utilized in this engineering.

ENERGY EFFICIENCY IN SENSOR NETWORKS

The sensor network energy efficiency is always a point of discussion in the research area of WSN. The underlying concepts discuss the type of hardware used to develop the sensor nodes. Efficient hardware is not just sufficient to optimize the energy usage of the network. Software part plays a key role in building a better network. All the defined protocols will be developed at Network Layer level which describes how a node should behave when it has a packet to be sent. All the layers of the TCP/IP model is discussed below.

1.1 PHYSICAL LAYER

The sensor, which is often a straightforward indication, is introduced in the first layer. Information is handled responsibly after sign moulding and digitisation. In this layer, the sensor makes information from its manageable ordinal behaviour available. In order to reduce the amount of data from all nodes, the information that is exposed needs to be strengthened and closely monitored. Each of the many measures in this case has an electronic component in the circuit that uses up an astonishing amount of endurance. Layers in a network are important for maintaining balance, transmitting data, and implementing strategies. A novel method for recognising various network layer properties is presented in this work.

1.2 MEDIUM ACCESS CONTROL (MAC) LAYER

In order to efficiently utilise the continuity-restricted resources of sensor nodes, the MAC layer must first align a number of non-functional elements of the network, such as eternal quality, energy productivity, high throughput, and low get to postpone. The energy-saving MAC techniques accessible at WSNs, such as obligation, parcel booking, variable transmission range, and flexible transmission duration, can be used in medium access layer operations such as crash, catching, bundle control.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

1.3 NETWORK LAYER

The protocols or techniques developed for the network layer are crucial, especially for the quality of service in WMSNs, for the reasons given below. handling the information transmission between the application layer and MAC layer, which has a substantial impact on communication performance, and making sure data transmission lines are reliable and energy-efficient from start to finish. Reliability of methodologies and timely assurance are the two key tactics for improving quality of service for mobility management at the network layer.

1.4 TRANSPORT LAYER

Transport layer approaches are primarily made to offer dependable end-to-end data (packet) transit and congestion control for conventional wired and wireless networks. Due to the close proximity to the sensor nodes, which occasionally results in sensors meandering without transmitting any data and turning on only in response to an event, these problems are not essential for WSNs. Ensuring end-to
end event transfer makes more sense and would work better in the majority of WMSNs than end to-end packet transfer.

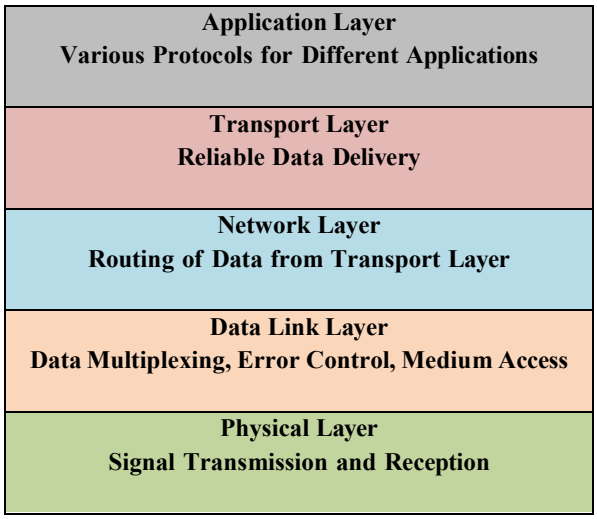

Figure 6. Protocol stack for WSN[2].

Physical Layer:- To receive and transfer data collected from the hardware, the physical layer must meet the needs of the receiving and transmitting device. The layer is responsible for generating and selecting the carrier frequency, signal detection, modulation and signal encryption, and signal reception. Due to the radio channel's usage for transmission and reception of data, the amount of energy consumed is significant. The channel can be oper- ated in three distinct modes: Idle, Active, and Sleep. Consequently, the energy consumed can be minimized by shutting off the radio when the channel is idle.

Data link Layer:- This layer is responsible for preventing neighboring signals from interfering with each other in a noisy environment. This layer should have the appropriate access, error control, multiplexing, and error detection and correction. TDMA-based proto- cols have been extensively used to avoid collisions of packets. However, Halkes et al. reported that their deployment in multi-hop ad-hoc networks is very complex. Another method for efficient energy management is to reduce the time between transmission of a frame and idle listening.

Network Layer:- Several approaches, including topology control and routing schemes, have been adopted in this layer, increasing network lifetime. Selecting a suitable topology that could provide a well-connected network is often a difficult task. Routing plays a major role in lifetime enhancement by selecting the most energy-efficient path from sensing nodes to the base station (BS) . Routing techniques can be categorized as location-based, data-centric, hierarchical, mobility-based, and quality of service (QoS)-based. However, hierarchical clustering routing algorithms have proved to be effective in enhancing lifetime and reducing power consumption by determining the optimal route.

Transport Layer:- Traffic flow regulation is provided by the transport layer, which distributes network traffic to the distant end. Additionally, traffic is provided with reliability measures. It is divided into sequential segments to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

forward upper layer application data, which are then reassembled into data packages. The transport layer can perform flow control, congestion control, and error checking at a higher level.

Application Layer: The application layer serves as a connection point between users and the network services dedicated to electronic mail, file transfers, virtual terminals.Clustering Strategies in WSN

Because battery power is limited, proper clustering is essential for significantly ex- tending the network's life span. To perform clustering, there are many methods to choose from The clustering strategies in WSN can be classified as shown in Figure

Deterministic: Here, the CHs are set at fixed positions in the network . The sensors broadcast a HELLO message to their neighbours, and the node that first receives the maximum number of these messages is elected as CHs and initiates the cluster formation phase. The important attributes of these clustering schemes are node identity numbers (IDs) and node degree (number of neighbouring nodes).

Adaptive: Instead of random CH selection, adaptive clustering schemes are based on the selection of CH considering particular parameters, such as remnant energy, the distance between nodes, energy dissipated in the last round, and distance to BS. Specific combinations of these parameters form the objective function for CH selection that can adapt to the rapid variations in the network. Adaptive schemes can be further categorized as BS-assisted or probabilistic (self-organized) based on who has the power to initiate the CH selection process. Again, considering the parameters for the role of a sensor node, the probabilistic scheme can be classified as resource adaptive and fixed parameters.

Hybrid: This clustering strategy considers combined clustering metrics with other architectures to increase energy efficiency.

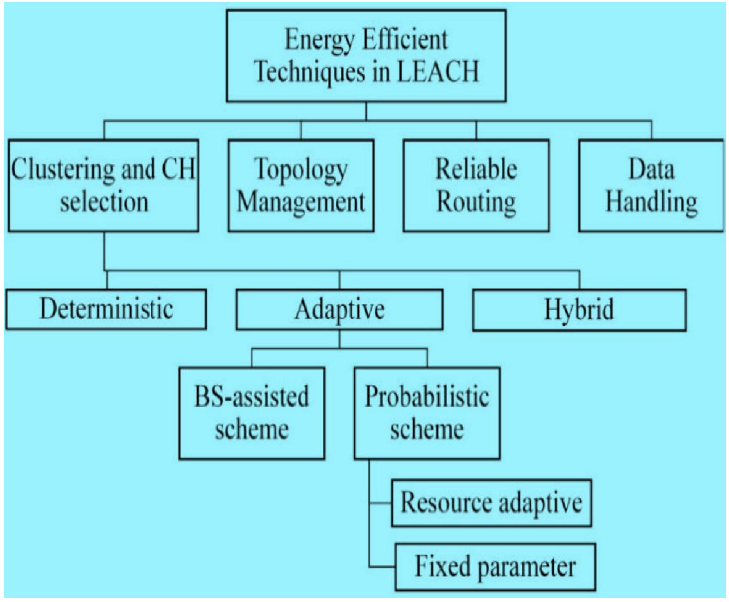

Figure 7. Taxonomy of clustering strategies

Energy model

The sensor node's components, including the microcontroller unit, communication unit, and power management unit, are depicted in Here describes how energy consumption is taken into consideration in this paper: Both the energy consumed for data transmission and reception is included in the communication link's energy consumption. Since the nodes in the network have data fusion capabilities, the amount of data that the CH needs to transmit is greatly reduced, thereby reducing the energy consumption of transmission within the network. However, it is still necessary to consider the energy consumption of data aggregation. The descriptions of key parameters are listed in Table 1. The total energy consumption in the network is as follows:

$$E_{TOTAL} = E_{TX} + E_{RX} + E_{DA} \quad (1)$$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

In Eq. (1), E_{TX} is the energy consumption of transmitting data, E_{RX} is the energy consumption of receiving data,and E_{DA} is the energy consumption of data fusion. Assuming that the transmission distance is d and the packet length is l ,the calculation methods of transmitting energy consumption, receiving energy consumption, and aggregation energy consumption are as follows:

$$E_{TX}(l,d) = \begin{cases} l\delta_{elec} + l\varepsilon_{fs}d^2 & \text{if } d < d_0 \\ l\delta_{elec} + l\varepsilon_{mp}d^4 & \text{if } d \geq d_0 \end{cases} \quad (2)$$

$$E_{RX}(l) = l \times E_{elec} \quad (3)$$

$$E_{DA}(l) = l \times \varepsilon_{da} \quad (4)$$

In Eq. (2), δ_{elec} represents the energy dissipated by the transmitter or receiver to process each bit of data, ε_{fs} and ε_{mp} are the power amplification parameters of free space transmission and multipath fading transmission, respectively. ε_{da} is the data aggregation parameter, and d_0 is the distance threshold. If the transmission distance is less than d_0, the data is transmitted according to the free space model; otherwise, the multipath model is used to transmit data.

The calculation method of d_0 is:

$$d = \frac{\varepsilon_{fs}}{\varepsilon_{mp}}$$

Objective function;-

Assuming that the probability of CH is p, the WSN should be divided into K different clusters, where K = Nalive × p, Nalive is the number of surviving nodes in the network. As mentioned above, each cluster includes.

Overview:

WSN is a bridge element that combines the digital virtual world with the real world. A WSN is formed by collecting many sensors called nodes, which have limited computing, sensing, and communication functionaries. The sensor nodes are implemented in a geographical area for monitoring physical phenomena such as humidity, temperature, and vibrations. The nodes are small devices with essential components, such as the detection, processing, and communication of subsystems and a power supply unit, as shown in Figure 8

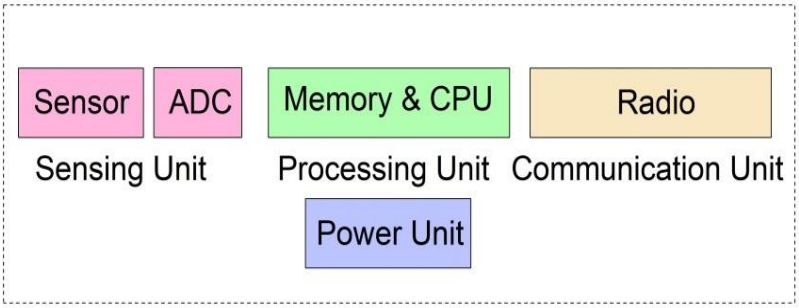

Figure 8. Sensor node structure.

Categorization of Routing Protocols for WSN

Data is efficiently transferred around WSNs between the spatially distributed nodes and sink nodes intermittently. Due to its unrealizable link with a computer, the sorting of the nodes in WSN cannot satisfy the need for all applications with a single routing protocol. Many routing protocols have been studied, according to the features of grouped applications. These protocols will typically be categorized for five classes,flood routing protocol, hierarchical and data-centred routing protocol, location-based routing protocol and the routing protocol based on QoS as shown in figure 9.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

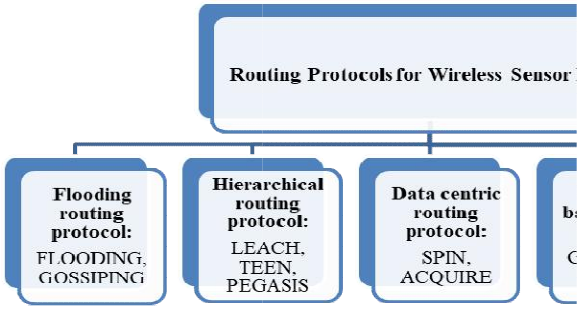

Figure 9. Conceptual Classification of Routing Protocols in WSN[3]

II. LITERATURE SURVEY

This section presents an overview of the state-of-the-art secure routing protocols of wireless sensor networks. This overview composed of discussion about the assumptions, methodologies, and key approaches present in existing works. Based on this section, we will present taxonomy and comparison in the following sections.

Light weight Secure-Low-Energy Adaptive Clustering Hierarchy (LS-LEACH) Routing Protocol

Alshowkan have proposed a Lightweight Secure-Low-Energy Adaptive Clustering Hierarchy (LS- LEACH) in which they firstly discourage the attacker to join the wireless sensor network using lightweight and energy-efficient authentication function in which the cluster head verifies the validity of nodes, which ask to join the cluster. Secondly, they described the threshold for the typical node-to-node number of connections through the time. This is used to detect the strange activities happened between nodes. Thirdly, they described the effective use of time division multiple access (TDMA) in the LEACH so that every node can only send data to the cluster head. They also described the mechanism to use LS-LEACH in WSNs by election, connection, and transmission in which different formulas are used. They assume that every node has two secret keys. One key is shared among all nodes, and it is also shared with the base station. When the node becomes a cluster head, then the private key will be shared with the base station. On the other hand, the group key is used to join clusters. They also assume that the number of cluster heads should not be more than 5% of total nodes. At the start of each subsequent cycle after network deployment, cluster head will be elected. They describe that wireless sensor network is facing lots of problems such as inadequate resources in energy, power consumption and storage. There is another challenge that the uniqueness of the broadcast medium makes the wireless sensor networks at risk to a number of attacks. An attacker can join the wireless sensor network and may seize, insert or broadcast the data. They compared the performance of LS-LEACH and LEACH using system throughput, lifetime of the network and the amount of energy they consumed.

Taxonomy of Secure Routing Protocols

We divided the secure routing protocols into two different categories one is a cluster base and second is none cluster based figure 1. In the cluster bases routing, a network is divided into sub structures we call it cluster, for the coordination of sub-structure every node in network have its own cluster head. It is also used to transfer data among the nodes in the network. In none cluster base approaches there is no cluster in the network they use approaches other than this approach. Then we further subdivided these two categories into three subcategories. One is symmetric key cryptography second is asymmetric key cryptography and third is hybrid. In symmetric key cryptography it encrypt the message using same key also use the same key for decryption of the message. In asymmetric key cryptography, it encrypts the message using same key also use the same key for decryption of the message. In asymmetric key cryptography, two different keys are used. One is public key other is private key. In hybrid, both asymmetric and symmetric cryptography approaches are used.

Fig.1. Taxonomy of Secure Routing Protocols

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

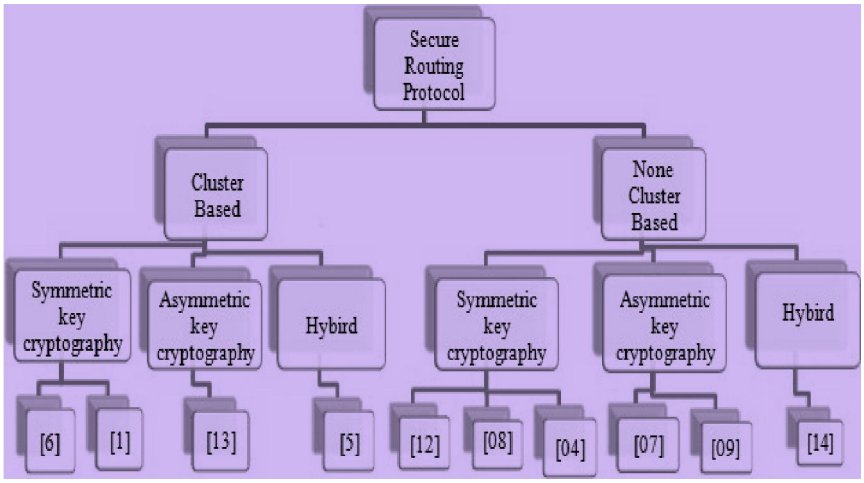

Fig.1. Taxonomy of Secure Routing Protocols

Attacks and Security Approaches

Existing secure routing protocols uses various symmetric and asymmetric cryptographic approaches to provide protection against various attacks like, eavesdropping, DoS attack, Sybil attack, spoofing, jamming etc. Table 1 summarizes the details about the secure routing protocols provide protection against which types of attacks.

Table 1. Attacks on OS Layer and Security Different Approaches against These Attacks

Secure Routing Protocols	Attack on Layer	Type of Attacks	Security Approach
LS-LEACH [1]	Link layer	Eavesdropping	Symmetric Key Cryptography
SCRA [4]	Network layer	Dos attack	Symmetric Key Cryptography
Secure Directed Diffusion [5]	Network layer	Selective forwarding	Hybrid
TEESR [6]	Data link layer	Sybil attack	Symmetric Key Cryptography
EENDMRP [7]	Network layer	Spoofing, altering, Altered Routing	Asymmetric Key Cryptography
SEAR [8]	Physical layer	Jamming, Routing Traceback	Symmetric Key Cryptography
tSEL [9]	Network layer	Altered Routing, Byzantine	Asymmetric Key Cryptography
CASER [12]	Physical and Link layer	Routing traceback Jamming, Eavesdropping	Symmetric Key Cryptography
SCMRP [13]	Network Layer	Sinkhole, Wormhole, Selective forwarding	Asymmetric Key Cryptography
HySecNJog [14]	Transport layer	Hello Flood attack	Hybrid

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Comparison of Secure Routing Protocols

The provides a qualitative comparison of the existing secure routing protocols of WSNs. For this purpose, we have used the following parameters:

1) protocol type,
2) protocol classification,
3) security assumption, and
4) environmental assumptions

According to this table, Lata et al. and Alshowkan et al. have adopted the cluster based symmetric key cryptography approach for the security of routing protocols. Whereas, Tang et al. Tingting et al. and Khan have adopted none cluster based symmetric key cryptography approach. Kumar et al. have adopted the cluster based asymmetric cryptography approach, whereas D'Souza et al. Yuvaraju and K. Rani et al. have adopted the none cluster-based asymmetric cryptographic approach. To overcome the drawbacks of symmetric and asymmetric cryptographic approaches, Belkadi and Kalita et al. have adopted the hybrid approach to secure the routing protocol. This comparison gives us the clear idea of different approaches for secure routing protocols and how to deal with these security issues using appropriate approach, which is efficient, secure, easy to use and less costly.

III. FUTURE CHALLENGES AND ISSUES

With the advancement in wireless sensor network technology, its usage in our daily life is increasing. Even though there is a lot of work has been done for the secure transmission, but the issues regarding security of WSNs still not overcome yet.

From the literature survey, we found that most of the existing routing protocols are not providing basic security features like confidently, authentication integrity, and reliability.

A challenging issue in designing a secure routing protocol for a wireless sensor network is availability of limited resources of sensor node e.g., storage, and computation power. In wireless sensor network, energy efficiency is also an important issue

Another main problem is that there is no security evaluation on framework for the routing protocols in WSNs that is needed for the comparison purpose. Currently, every researcher uses their own criteria for evaluation.

Furthermore, most of the existing schemes ignore the issues of accountability and freshness of data. Use of traditional symmetric and asymmetric approaches is computationally expensive task for the sensor nodes. It will be interesting to see the effects of elliptic curve cryptography in secure routing protocols.

IV. CONCLUSION

Wireless sensor network comprises of resource constraint sensor nodes. That is why, designing and selecting an appropriate secure routing protocol for the network is a tough task. In this research paper, firstly, we have discussed the various types of security attacks. Secondly, we have presented a taxonomy of secure routing protocol and then provided a qualitative comparison. Finally, we have highlighted future challenging issues. Results show that most of the existing routing schemes are not very efficient in providing security.

REFERENCES

[1] M. Alshowkan, K. Elleithy, and H. Alhassan, "Ls-leach: A new secure and energy efficient routing protocol for wireless sensor networks," 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Oct 2013, pp. 215–220.

[2] V. Sharma and K. Nayanam, " Sixth Generation (6G) to the Waying Seventh (7G)Wireless Communication Visions and Standards, Challenges, Applications", International Journal of Advanced Research in Science & Technology, vol. 13, no. (2), pp. 1248-1255, Feb. 2024. [https://doi.org/10.62226/ijarst20241319].

[3] V Sharma, K Nayanam Implementation of Enhanced Energy Detector in Cluster Based Multistage Relaying Cooperative Spectrum Sensing International Research Journal of Advanced Engineering and Science volume 9 issue 1 page 11

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

[4] B. Lata, V. Tejaswi, K. Shaila, M. Raghavendra, K. Venugopal, S. Iyengar, and L. Patnaik, "SGR: Secure geographical routing in wireless sensor networks," 9th International Conference on Industrial and Information Systems (ICIIS), Dec 2014, pp. 1 – 6.
[5] H. Cheng, C. Rong, and G. Yang, "Design and analysis of a secure routing protocol algorithm for wireless sensor networks," IEEE International Conference on Advanced Information Networking and Applications (AINA), March 2011, pp. 475–480.
[6] F. Khan, "Secure communication and routing architecture in wireless sensor networks," 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE), Oct 2014, pp. 647–650.
[7] M. BELKADI, R. AOUDJIT, M. DAOUI, and M. LALAM, "Energy efficient secure directed diffusion protocol for wireless sensor networks," International Journal of Information Technology and Computer Science (IJITCS), vol. 6, no. 1, p. 50, 2013.
[8] Vatsala sharma" Optimization of Performance of Cooperative Spectrum Sensing in Mobile Cognitive Radio Networks", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.10, Issue 4, page no.b579-b583, April-2023, Available :http://www.jetir.org/papers/JETIR2304169.pdf
[9] Sharma, V., Joshi, S. (2021). Real-Time Implementation of Enhanced Energy-Based Detection Technique. Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-7533- 4_1
[10] Shahraki, A.; Taherkordi, A.; Haugen, Ø.; Eliassen, F. A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms. IEEE Trans. Netw. Serv. Manag. 2020, 18, 2242–2274. [CrossRef]
[11] AS Kang, V Sharma, JS Singh "Efficient Spectrum Sensing Using Discrete Wavelet Packet Transform Energy Detection in Cognitive Radio" Advances in Wireless and Mobile Communications volume 10 issue 2 page 193-212
[12] Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions.
[13] V. Sharma and S. Joshi, "A Literature Review on Spectrum Sensing in Cognitive Radio Applications," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 883-893, doi: 10.1109/ICCONS.2018.8663089.
[14] Jubair, A.M.; Hassan, R.; Aman, A.H.M.; Sallehudin, H.; Al-Mekhlafi, Z.G.; Mohammed, B.A.; Alsaffar, M.S. Optimization of Clustering in Wireless Sensor Networks: Techniques and Protocols. Appl. Sci. 2021, 11, 11448. [CrossRef]
[15] Wohwe Sambo, D.; Yenke, B.O.; Förster, A.; Dayang, P. Optimized clustering algorithms for large wireless sensor networks: A review. Sensors 2019, 19, 322.
[16] V. Sharma and S. Joshi, "Design of Energy Detection based Multistage Sensing Technique," 2020 "Journal of Scientific Research "India , 2020, DOI:10.37398/JSR.2020.640255
[17] Ali M, Dey T, Biswas R, "ALEACH: Advanced LEACH routing protocol for wireless microsensor networks," Proc. Int. Conf. Electr. Comput. Eng., pp. 909-14, 2008. [5] M. C. M. [18] T. and T. Thein, "An Energy Efficient Cluster-Head Selection for Wireless Sensor Networks," Proc. Int. Conf. Intell. Syst., [18] Model. Simul., pp. 287-291, 2010. [6] A. A. and M. I. Mohammad, "Hybrid LEACH: A Relay Node Based Low Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks," Proc. Int. Conf. Commun., pp. 911-916, 2009.
[19] M. R. Senouci, A. Mellouk, H. Senouci, and A. Aissani, "Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols," J. Netw. Comput. Appl., vol. 35, no. 4, pp. 1317 1328, Jul 2012, doi: 10.1016/j.jnca.2012.01.016. [29] S. A. [20]Nikolidakis, D. Kandris, D. [20] D. Vergados, and C. Douligeris, "Energy efficient routing in wireless sensor networks through balanced clustering," Algorithms, vol. 6, no. 1, pp. 29–42, 2013, doi: 10.3390/a6010029.
[21] S. Kumar and S. Jena, "Scmrp: Secure cluster based multipath routing protocol for wireless sensor networks," 2010 Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), Dec 2010, pp. 1 – 6.
[22] V Sharma,K Nayanam A Reliable Optimal Hybrid Spectrum Sensing Algorithm with Hardware Impairments for Cognitive Radio Network SSRG International Journal of Mobile Computing and Application Volume 11 Issue 1, 1-8, Jan-Apr 2024 ISSN: 2393–9141 / https://doi:10.14445/23939141/IJMCA-V11I1P101 © 2024 Seventh Sense Research Group

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

[23] H. Kalita and A. Kar, "HySecNJoining: A hybrid secure node joining algorithm for wireless sensor network," 2011 Third International Conference on Communication Systems and Networks (COMSNETS), Jan 2011, pp. 1-6.
[24] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad, "The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures", IJWMT, vol.2, no.2, pp.33-44, 2012.
[25] Sharma, V., Joshi, S. (2021). Design of Hybrid Blind Detection Based Spectrum Sensing Technique. Journal of Scientific Research, 2020, Vol 12, Issue 4, p575. Academic Journal. https://doi.org/10.3329/jsr.v12i4.46870.
[26] Kamal Nayanam, and Vatsala Sharma, "Cognitive Radio Based Enhanced Compressive Spectrum Sensing Technique For 5g Adhoc Networks," International Journal of Engineering Research and Technology (IJERT), vol. 13, no. 2, 2024.
[27] Lee, S., Lee, S., Yu, J. and Lim, H., 2016. Semi distributed clustering algorithm for large scale wireless sensor networks. Sensors, 16(12), p.2143. 10. Mostafaei, H., 2018. A distributed learning automata based routing algorithm for mobile wireless sensor networks. Wireless Networks, 24(3), pp.655-667.
[28] T. G. Nguyen, C. So-In, and N. G. Nguyen, "Two energy-efficient cluster head selection techniques based on distance for wireless sensor networks," 2014 Int. Comput. Sci. Eng. Conf. ICSEC 2014, pp. 33–38, 2014, doi: 10.1109/ICSEC.2014.6978125.
[29] A. A. and M. I. Mohammad, "Hybrid LEACH: A Relay Node Based Low Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks," Proc. Int. Conf. Commun., pp. 911-916, 2009. [7] F. X. and S. Yulin, "The Improvement of LEACH Protocol in WSN," Proc. Int. Conf. Comput. Sci. Netw. Technol., pp. 1345-1348, 2011. Weizheng Ren, Yaodong Zhang ,"A wireless sensor network clustering algorithm based on energy and distance," Proc. Work.