INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 11 | NOV - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Survey on Wireless Sensor Network Structure Attacks and Energy Optimization

[1]Jayant Shukla, Research Scholar RNTU Bhopal jayants1981@gmail.com
[2] Laxmi Singh, Associate Professor RNTU Bhopal laxmi15singh@gmail.com

Abstract— A Wireless Sensor Network (WSN) is a novel form of embedded real-time device that can be used for a variety of applications that make conventional networking impractical. Concerning the energy production of the nodes, WSN has significant issues that may affect the system's stability. Researchers have developed a range of methods and strategies to decrease wireless sensor network energy consumption. This paper has brief WSN structure for the optimization of communication with routing techniques. As network is vulnerable hence attacks were also present. This paper has list attacks as per number of layers. Further paper has list some of latest research work that not only optimize the network energy but also increases the robustness.

Index Terms— Adhoc Network, Wireless Sensor Network, Communication Attacks, Virtual machines.

I. INTRODUCTION

Wireless sensor networks (WSNs) have recently garnered a great deal of interest from both industry and academia. WSNs are utilized extensively in distributed monitoring and control applications, such as environmental monitoring, industrial field control, smart residences, and smart factories [1,2,3]. WSNs typically comprise of a number of sensor nodes that perform a variety of tasks, including data collection, processing, and transmission. Compared to traditional wired systems, WSNs have evident cost, flexibility, and convenience advantages [4]. In many industrial applications, wireless sensor networks (WSNs) are powered by batteries, whose limited capacity and burdensome replacement requirements have become the most significant restrictions on the use of WSNs. In WSN applications, lifetime power consumption management is of paramount significance [5, 6, 7].

Various techniques, including clustering, scheduling of sleep cycles, routing, and the incorporation of sink nodes, can be utilized to conserve energy. Clustering and routing are the recommended methods for minimizing energy consumption to the greatest extent. This realization prompted the proposition of this energy conservation-focused activity. Clustering conserves energy by utilizing a Cluster Head (CH) node that efficiently manages the cluster's nodes. This CH collects the data detected by the Member (MN) nodes of the Cluster and forwards it to the Base Station (BS).

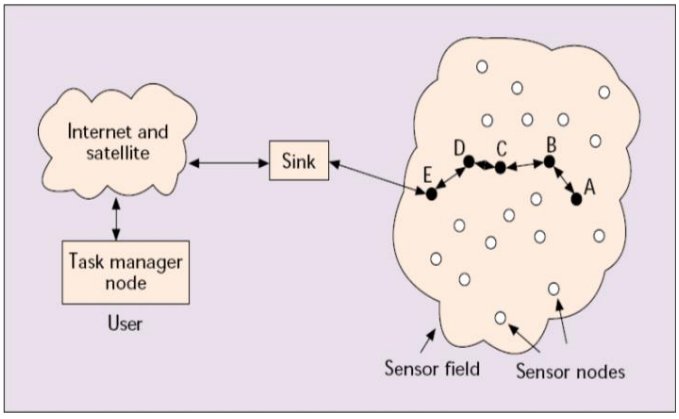

Figure 1 shows a wireless sensor network.

The primary objective of clustering is to reduce overall energy consumption, which can be accomplished in the following methods. As all data is delivered to the CH node, redundancy becomes obsolete. In addition, the routing cost can be avoided by imposing the restriction

that communication can only occur between the CH node and the BS. This ensures that all network communications remain within the same network. Additionally, it maintains the communication bandwidth of the sensors. Clearly, these characteristics extend the tenure of the network. The objective of the proposed T-CBRSS is to extend the lifespan of the network by enforcing clustering and routing techniques, with trust as the underlying model, because they have been proven to be efficient and effective.

II. WSN Structure

WSN sink

The brains of a WSN are the sensor nodes. They provide information vital to the WSN's operation. Sensor node data is raw and must be processed before use [8]. In this context, "data" can refer to either aggregated statistical information or fine-grained measurements of factors that describe the state of an item. Identifying and following moving objects—vehicles, animals, people—is a subset of WSN uses. WSN data processing is essential in each of these cases. Due of their limited computer power and energy efficiency, sensor nodes typically cannot do such processing. Beyond the sensor nodes, the WSN server is usually responsible for the last data processing step in WSNs. There is just one sink or base station sensor node linked to the WSN server. A WSN sink collects data from sensor nodes and communicates with the WSN server.

WSNs with the cluster structure

It is critical that the limited and nonrenewable energy stored in sensor nodes be used as effectively as possible. In Figure 2 [9], we see how data travels from sensors to a collection point. Sink periodically compiles information from all sensors. Each arrow on the graphic denotes the transfer of a certain number of measurements within the time period depicted.

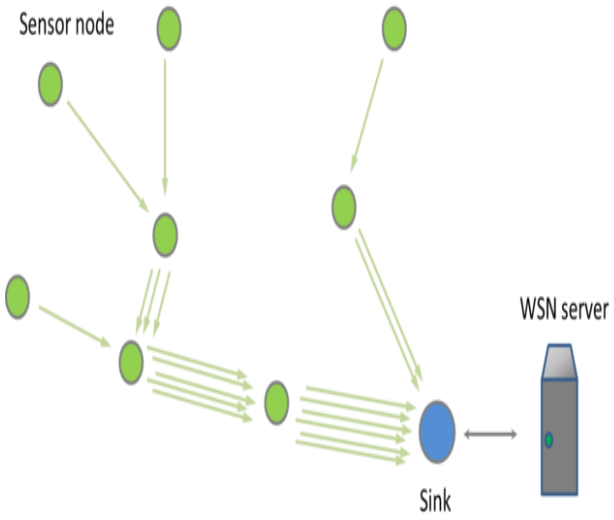

Figure 2: Data streaming from sensor nodes.

As a result of using all sensor nodes to gather data, the sensor nodes closest to the sink must also receive and send measurements from the sensor nodes furthest away. Therefore, transceivers of nearby sensor nodes retransmit significantly more data than transceivers of far-off sensor nodes, resulting in higher energy consumption. As a result, the nearest sensor nodes fail considerably earlier than the rest of the WSN, which disrupts its operation, because they are all of the same kind and have the same energy content.

Therefore, the autonomous working duration of sensor nodes nearest to the drain is dramatically decreased owing to more frequent retransmission if a WSN application offers periodic data gathering (which is the case in most circumstances). In the long run, all connections from sensors will go through the sensor nearest to the washbasin. As the number of sensor nodes in a WSN grows, so does the amount of data being sent between them. Large WSNs with a central drain cannot make efficient use of resources from an energy efficiency standpoint.

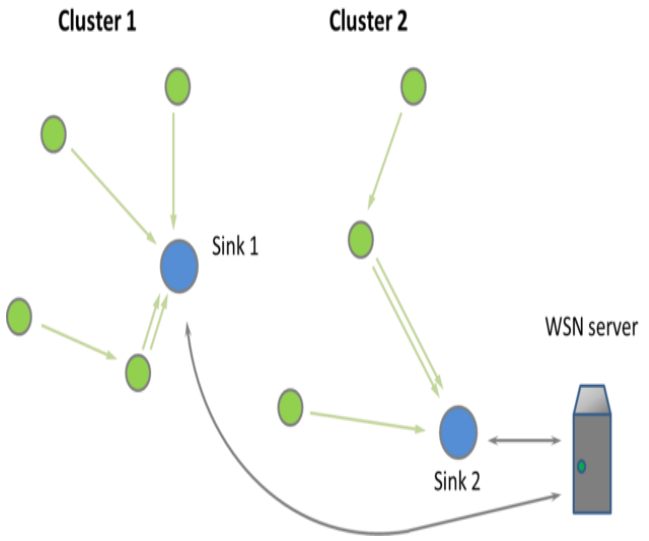

Figure 3: Multiple-sink WSN

The solution to this problem is to divide the WSN into smaller networks, or clusters. Each cluster is its own, smaller WSN with its own sink. Each washbasin may talk to the central hub independently. In Figure 3, we see a system with two drains. Once upon a time, the diagram's arrows indicated the volume of data being transferred. It is clear that the quantity of retransmissions has been drastically cut, relieving pressure on the sensor nodes located closest to the sinks.

Multiple-sink There is no such thing as an arbitrary sub-division of a WSN [10]. This separation is often performed automatically when WSN is deployed and used. The destination to which data from a sensor node is sent is determined automatically. The WSN protocol's algorithm provides the basis for this choice. Depending on the specifics of the use case, other criteria may be prioritized, including the shortest possible time to send data, the fewest possible retransmissions, and the most equitable traffic allocation across WSN nodes.

WSN gate It has been assumed in the discussions of WSN organization schemes thus far that all WSN parts are situated in the same physical place. Accessing WSN data remotely is a common practical requirement. For instance, a WSN installation in a suburban forest may necessitate data gathering and processing in a city centre. Specialized gates are used to accept sensor network data from the sink and retransmit them using a different (i.e., non-WSN) wireless communication standard in order to arrange data delivery from a WSN to a distant server. The network depicted in Figure 4 uses the Internet to relay information from a gate to a server.

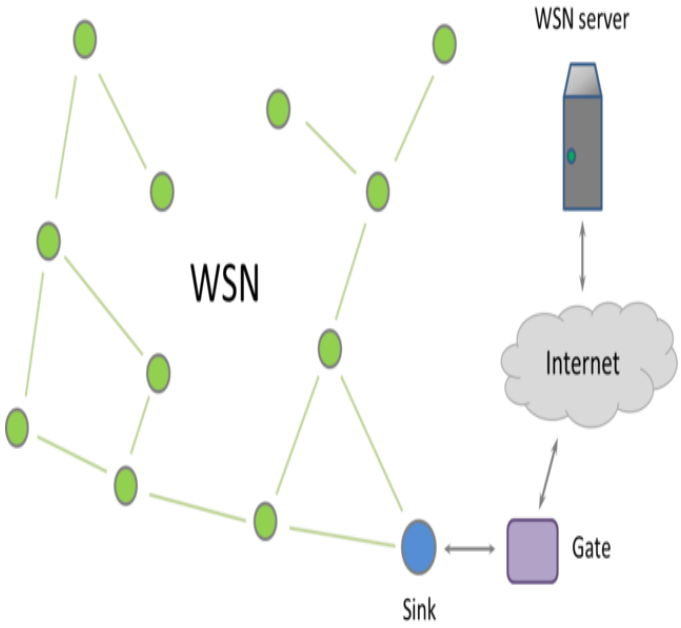

Figure 4: WSN server is connected via the Internet

.

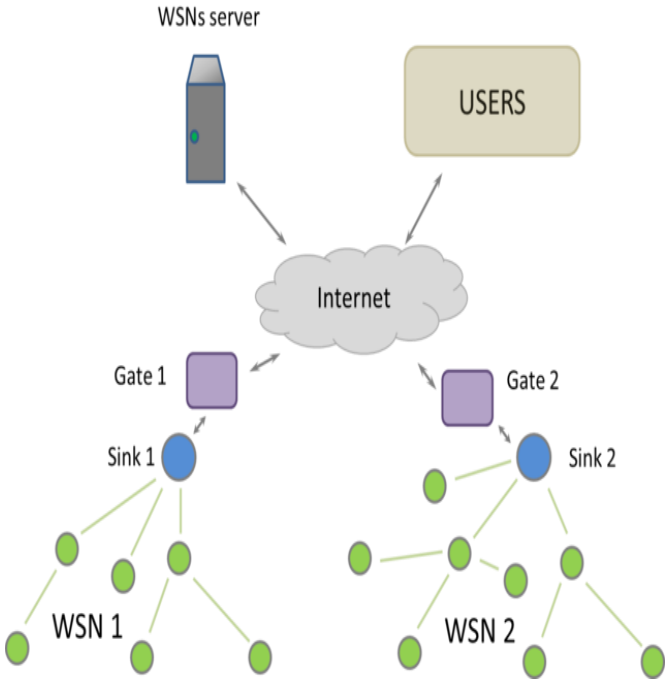

Figure 5: Scheme of provision of WSN services

Additionally, gates allow for the coordination of service delivery. Connecting WSNs to the Internet is often straightforward in the modern day when Internet connectivity is ubiquitous via cellphone, cable, and satellite networks. The proposed user-WSN interaction pattern is depicted in Figure 5.

III. ROUTING IN WSN

One of the primary goals of WSN setup is information exchange while making an effort to extend the lifespan of the system and prevent integration degradation via the use of robust energy management techniques [11, 12]. Several factors in testing have been found to impact the setup of steering conventions.

Node Deployment WSNs allow for manual (deterministic) or random node organization, depending on the needs of the application. Sensors are physically placed and information is routed in predetermined ways in manual transmission. In contrast, in an ad hoc configuration, the nodes are placed at random to form a guiding structure.

Energy Consumption The battery life of a sensor node is a major factor in how long it will last. Each node in a multi-bounce WSN acts as both a data transmitter and a data router. Some sensor nodes failing as a result of power failure might result in significant topological changes, necessitating the possible rerouting of packets and a complete overhaul of the system.

Fault Tolerance Lack of force, bodily injury, or natural impedance might cause certain sensor nodes to fall short or be blocked. Failures at individual sensor nodes shouldn't have an effect on the system as a whole. The alternative path that may be used to route the data to the sink node has to be the primary focus of the steering convention.

Scalability Sensor nodes in the detection area might number in the hundreds, thousands, or even millions. In order to manage steering among the many sensor nodes, any proposed strategy must be able to be scaled up. Nodes in the sensor network are typically in a dormant state and are switched to an active one when an event is detected.

Coverage Every sensor node in a WSN has its own unique view of the planet. The range and precision of any one sensor's view of Earth are limited. There is a limited geographical area it can reach. Therefore, the scope of the communication's range is also an important WSN design option. In a WSN, information is exchanged between nodes as it travels across the network. However, there are many uses for sensor systems that need knowledge of node area. This regional information allows early anticipation of the wonder, so reducing the severity of any potential dangerous catastrophe. The nodes' area information contributed in the easy finding of a guiding path between the source and the destination, which reduced the amount of lag time inherent in the data transmission process.

IV. Classification Of Energy Efficient Techniques

Link layer attacks

Data multiplexing, frame detection, media access, and error management are all tasks delegated to the link layer [14]. This level is susceptible to deliberate impacts, depletion of resources, and unfair distribution of those same resources. A collision happens when two nodes try to communicate on the same frequency at the same time [13]. Packets are lost and must be resend if they are damaged during collision. An attacker may deliberately trigger collisions in selected packets, such as ACK control messages. A costly exponential falloff might occur in the event of such a collision. An attacker might easily break the rules of the communication protocol by constantly sending out messages in an effort to create collisions. A target's resources can be depleted by repeated collisions [13]. For example, a naive link layer implementation can keep trying to send over and over again after receiving a damaged packet. The nodes' energy supplies would quickly decrease if these retransmissions weren't detected as soon as possible. Injustice is a weak denial-of-service [13]. By randomly deploying the aforementioned link layer attacks, an attacker might potentially induce unfairness. By

occasionally interfering with the frame transmissions of other nodes, the attacker impairs the performance of real-time applications running on those nodes.

Network layer attacks

Spoofed routing information, selective packet forwarding, the sinkhole, the Sybil, the wormhole, the welcome flood, and acknowledgement spoofing are just a few examples of the attacks that may be launched against the network layer of WSNs[25]. The following is a synopsis of these attacks: Forging data in the network's routing information is the most direct assault on a routing protocol. It is possible for an attacker to cause traffic disruption by forging, modifying, or replaying routing information [14]. Disruptions can occur when routing loops arise, when specific nodes become more or less attractive to network traffic, when source routes lengthen or shorten, when false error messages are generated, when the network is partitioned, and when end-to-end latency increases.

Selective forwarding: In a WSN or other multi-hop network, all nodes must faithfully forward messages for them to reach their intended recipients. A compromised node might be used by an attacker to send or ignore messages at will [3].

Sinkhole: An attacker employs a sinkhole attack when he or she forges routing information to increase the attractiveness of a compromised node to other nodes in the network [15, 14, 13]. Therefore, the hacked node becomes the next-hop node for traffic from other nodes in the area. Selective forwarding would be incredibly easy because all network traffic from a sizable chunk of the network would pass through the hacked node.

Sybil attack: The Sybil attack occurs when a single network node pretends to be several different entities. Redundancy techniques in P2P networks' distributed storage systems were initially identified as a target of this attack [13]. From the perspective of a WSN, Newsome et al. [15] describe this type of assault. The Sybil attack may also be used to circumvent measures taken to prevent malicious conduct from being detected and to undermine routing algorithms, data aggregation, voting, fair resource allocation, and more. Whether the goal is voting, routing, or aggregate, Sybil's method works the same. In both methods, covert identities are used. The Sybil attack, for example, may use numerous identities to cast more "votes" in a sensor network voting method. Sybil attacks, in a similar vein, rely on a malicious node taking on the identities of numerous nodes and redirecting traffic through a single malicious node.

Wormhole: In order to replay network communications, an attacker needs a wormhole, which is a low-latency link between two network segments [14]. This connection can be made by two nodes in different parts of the network talking to each other, or by one node passing messages between two adjacent but otherwise non-neighboring nodes. In the latter scenario, an attacking node near the base station can offer a one-hop link to the base station via another attacking node situated in a faraway portion of the network, similar to the way a sinkhole attack works.

Hello flood: Most protocols that rely on Hello packets incorrectly assume, leading to a "Hello flood," that receiving a Hello packet means that the sender is in radio range of the receiver. A strong transmitter might be used by an attacker to trick a large number of nodes into thinking they are in its vicinity [14]. All the other nodes that have received Hello packets will then seek to send to the attacker node since it has fraudulently advertised a shorter path to the base station. These nodes, however, are out of the range of the attacker's radio signals. Some wireless sensor network routing techniques require the sending of acknowledgement packets. Attacking nodes can listen in on surrounding nodes' packet broadcasts and counterfeit their acknowledgements to trick them into thinking everything is OK [12]. This enables the attacker to propagate misleading data about the nodes' health.

Physical layer attacks

The physical layer is responsible for the selection of frequencies, the creation of carriers, the detection and modulation of signals, and the encryption of data [14,

15]. Interference is possible in every medium that uses radio waves. WSN nodes may also be placed in unsafe areas where an attacker may get physical access. Jamming and manipulation are the two types of physical layer assaults.

Jamming: Jamming is an attack technique that disrupts the radio signals utilised by nodes in a WSN to communicate [13]. A single point of interference might cause widespread problems for the network. An opponent might possibly impair network-wide communication even with less powerful jamming sources by strategically distributing the jamming sources. Intermittent interference can be damaging to message transmission in a WSN because of how time-sensitive it can be [13].

Tampering: Sensor networks are usually deployed in the wild. Physical assaults on WSN nodes are particularly dangerous because of their unsupervised and scattered nature. Physical assaults on the nodes might cause permanent damage. Captured nodes can have their cryptographic keys stolen, their hardware tampered with, their software altered, or even have a malicious sensor swapped in for it [17]. [16] It has been shown that sensor nodes like MICA2 motes can be hacked in under a minute.

Denial of Service (DoS) attacks

DoS attacks are defined by Wood and Stankovic [13] as events that diminish or seek to diminish a network's ability to carry out its intended purpose. The creation of a general defensive mechanism against DoS assaults is still an unresolved subject, despite the existence of several standard strategies in the literature to combat some of the most common denial of service attacks. In addition, most forms of defense have a heavy computational overhead, making them unsuitable for WSNs with constrained resources. Researchers have spent a great deal of effort identifying the various types of DoS attacks on WSNs and creating remedies because of the high financial stakes involved. This section details some of the most typical types of denial-of-service attacks against WSNs.

Transport layer attacks

The transport layer of an SN is vulnerable to assaults such as the deluge attack and the desynchronization attack.

Flooding: When a protocol has to keep state on both sides of a connection, it might be flooded and cause memory fatigue [18]. An attacker can repeatedly try to establish new connections until either all available resources are used up or the number of connections is capped. Any further legitimate requests will be disregarded in any situation.

De-synchronization: Disconnection is what we mean when we talk about de-synchronization [18]. Forged messages sent repeatedly to an end host by an adversary, which causes the host to constantly seek retransmission of missing frames, is only one example. If an attacker knows when to do so, he or she can degrade or even block the end hosts from successfully exchanging data, forcing them to waste resources trying to rectify phantom mistakes.

V. Related Work

Energy-efficient uneven clustering (EEUCB) was proposed by Jasim et al. [21]; it employs minimum and maximum distance to reduce power consumption. In addition, EEUCB has devised a clustering rotation approach with two stages, intra- and inter-clustering procedures, that utilizes factor-based and UDCH data to increase lifespan by 57.75%, 19.63%, 14.7%, and 13.05%, respectively. By analyzing the distinct set of characteristics possessed by each SN.

Kumar et al. [22] proposed a technique for identifying malicious nodes (MNs) in a WSN. By selecting the Cluster Head (CH) based on the remaining energy of the sensor, this study also considers safety. During the Malicious Nodes Detection (MND) phase, the Improved Deep Convolutional method detects the MN, the Trusted Nodes (TN) are organized into groups, and the t-Distribution based Satin Bowerbird Optimization (t-DSBO) algorithm selects a CH for each group based on the residual energy of the nodes in that group. Through

the CH, data from this cluster is transmitted to the BS. If the present CH abruptly loses power, the t-DSBO will switch to another CH. Experimental evidence demonstrates that the proposed methods effectively detect MN and provide DT with minimal energy consumption.

To address the hotspot problem, Jain et al. [23] introduced Harris hawk optimization (HHO) based techniques, collectively known as HHO-UCRA. First, a method for selecting CHs based on HHO was presented. The clustering procedure then employs the CH Assignment function that was derived from it. Using the HHO-based methodology, we have devised efficient hawk encoding systems and distinctive fitness functions for both algorithms. HHO-UCRA is executed with a distinct number of sensors and control nodes (CH) in every simulated WSN scenario. To demonstrate the efficacy of the proposed algorithm in terms of WSN benchmark indicators such as network energy consumption, network lifetime, convergence rate, data packets received by the BS, and the number of ad hoc packets, network energy consumption, network lifetime, convergence rate, data packets received by the BS, and the number of a To increase the efficacy and lifespan of networks.

Rawat et al. [24] presented a protocol based on particle swarm optimization (PSO-EEC) for energy-efficient clustering. The proposed protocol uses particle swarm optimization to determine which nodes will function as the network's cluster head and relays. In particle swarm optimization, the fitness function used to determine which node should serve as cluster head takes into account the nodes' energy ratio (initial energy to residual energy), distance from the cluster head, and degrees. The proposed technique selects relay nodes for multi-hop data transmission to the base station by using fitness values derived from residual energy of the cluster head and distance to the base station as inputs. Energy consumption, network endurance, and throughput are just a few of the performance metrics used to evaluate how well the proposed protocol compares to other existing techniques.

Juneja et al. [25] devise the Enhanced Mobile Sink-based Coverage protocol in this article. The proposed EMSCOLER effectively resolves the coverage restoration problem and minimizes network transmission failures. Both coverage restoration and Link Stability Estimation-based Routing are included in the two phases (LSER) of this initiative. The grid-based Red Deer Simulated Annealing (GRDSA) model relocates redundant nodes to the hollow area when a CH is detected in the sensing field. In order to maximize the network's lifecycle and provide energy-efficient routing, the LSER algorithm calculates a connection quality evaluation and selects relay nodes to transmit data. MATLAB software is used to implement the suggested protocol. CR, EC, average residual energy (ARE), moving EC, and network lifetime are utilized to evaluate the proposed EMSCOLER's results.

Energy saving Distributed Monitoring based Firefly Procedure (EDiMoFA) Protocol was proposed by Idrees and Couturier [26] to ensure the coverage and to extend the lifetime of WSNs. The EDiMoFA protocol is executed by every node in the resulting compact areas. The Firefly Algorithm (FA) is utilised for scheduling wireless nodes and is part of the EDiMoFA protocol alongside virtual network partitioning and dynamic distributed virtual region head selection in each area. The EDiMoFA procedure is governed by consistency. Each period consists of two phases: the steady-state phase and the surveillance phase. During the monitoring phase, the sensing field in each virtual region will be monitored by the FA-generated optimal sensor device schedule.

Inspiring by PIO, Duan et al. [27] proposed a pigeon-homing behavioral swarm procedure that has obtained remarkable success in various fields in recent years, such as unmanned air vehicle formation (UAV), swarm control parameters, and image processing.

VI. Conclusion

Since battery-powered sensor nodes have limited energy, enhancing the lifetime of the WSNs is considered to be an important issue. This paper has finds that many of researchers has improves the WSN network by increasing the strength of nodes capacity and its architecture. In order to improve the life span of network energy uses plays an important role. This paper finds that node clustering based packet routing is efficient. Further robustness of the network was also important as network is open and work in limited channel range. For this trust based models were efficient. In future scholars can proposed a model that reduces the energy wastage and improve the robustness.

References

1. Azarhava, H.; Niya, J.M. Energy efficient resource allocation in wireless energy harvesting sensor networks. IEEE Wirel. Commun. Lett. 2020, 9, 1000–1003.
2. Erdelj, M.; Mitton, N.; Natalizio, E. Applications of industrial wireless sensor networks. In Industrial Wireless Sensor Networks: Applications, Protocols, and Standards; CRC Press: Boca Raton, FL, USA, 2013; pp. 1–22.
3. Manfredi, S.; Tucci, E.D. Decentralized control algorithm for fast monitoring and efficient energy consumption in energy harvesting wireless sensor networks. IEEE Trans. Industr. Inform. 2003, 13, 1513–1520.
4. Harb, H.; Makhoul, A. Energy-efficient sensor data collection approach for industrial process monitoring. IEEE Trans. Industr. Inform. 2017, 14, 661–672.
5. Xie, J.; Zhang, B.; Zhang, C. A Novel Relay Node Placement and Energy Efficient Routing Method for Heterogeneous Wireless Sensor Networks. IEEE Access 2020, 8, 202439–202444.
6. Liu, X.; Wu, J. A method for energy balance and data transmission optimal routing in wireless sensor networks. Sensors 2019, 19, 3017.
7. Hung, L. Energy-Efficient Cooperative Routing Scheme for Heterogeneous Wireless Sensor Networks. IEEE Access 2020, 8, 56321–56332.
8. Cui S, Cao Y, Sun G, et al. A new energy-aware wireless sensor network evolution model based on complex network. EURASIP J Wireless Commun Netw 2018; 2018(1): 218.
9. Kim B-S, Park H, Kim KH, et al. A survey on real-time communications in wireless sensor networks. Wireless Commun Mob Comput 2017; 2017: 1864847.
10. Behera TM, Samal UC, Mohapatra SK. Energy-efficient modified leach protocol for IoT application. IET Wireless Sens Syst 2018; 8(5): 223–228.
11. Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan, Routing protocol design for secure WSN: Review and open research issues, Journal of Network and Computer Applications, Volume 41, 2014.
12. Manuel, A.J.; Deverajan, G.G.; Patan, R.; Gandomi, A.H. Optimization of Routing-Based Clustering Approaches in Wireless Sensor Network: Review and Open Research Issues. Electronics 2020, 9, 1630.
13. A.D. Wood and J.A. Stankovic, “Denial of service in sensor networks”, IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.
14. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.
15. J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defenses”, In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 259-268, ACM Press 2004.
16. C. Hartung, J. Balasalle, and R. Han, “Node compromise in sensor networks: The need for secure systems”, Technical Report CUCS-988-04, Department

of Computer Science, University of Colorado at Boulder, 2004.

17. X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.

18. Da-Zhi Sun, Zahra Ahmadian, Yue-Jiao Wang, Mahmoud Salmasizadeh, and Mohammad Reza Aref. "Analysis and Enhancement of Desynchronization Attack on an Ultralightweight RFID Authentication Protocol". eprint.iacr.org, 2015.

19. Lohan P. and Chauhan R., "Geography-informed sleep scheduled and chaining based energy efficient data routing in WSN," Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, vol., no., pp.1,4, 1-2 March 2012.

20. Gherbi Chirihane & Aliouat Zibouda, "Distributed energyefficient adaptive clustering protocol with data gathering for large-scale wireless sensor networks", Programming and Systems (ISPS), 12th International Conference, IEEE,2015.

21. [21] A. A. Jasim, M. Y. I. Idris, S. R. B. Azzuhri, et al., "Energyefficient wireless sensor network with an unequal clustering protocol based on a balanced energy method (EEUCB)," Sensors, vol. 21, no. 3, 2021.

22. [22] M. Kumar, P. Mukherjee, K. Verma, et al., "Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks," IEEE Trans. on Network Science and Engineering, vol. 9, no. 5, pp. 3272-3281, 2021.

23. [23] D. Jain, P. K. Shukla, and S. Varma, "Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks," Journal of Ambient Intelligence and Humanized Computing, 2022.

24. [24] P. Rawat and S. Chauhan, "Particle swarm optimization-based energy efficient clustering protocol in wireless sensor network," Neural Computing and Applications, vol. 33, no. 21, pp. 14147- 14165, 2021.

25. [25] S. Juneja, K. Kaur, and H. Singh, "An intelligent coverage optimization and link-stability routing for energy efficient wireless sensor network," Wireless Networks, vol. 28, no. 2, pp.705-719, 2020.

26. [26] A. K. Idrees and R. Couturier, "Energy-saving distributed monitoring-based firefly algorithm in wireless sensors networks," The Journal of Supercomputing, vol. 78, no. 2, pp. 2072-2097, 2022.

27. [20] H. Duan and P. Qiao, "Pigeon-inspired optimization: A new swarm intelligence optimizer for air robot path planning," International Journal of Intelligent Computing and Cybernetics, vol. 7, no. 1, pp. 24–37, 2014.