International Journal on Emerging Technologies **11**(2): 57-65(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Comprehensive Survey on Energy Efficient Routing Techniques and Various Attacks in Wireless Sensor Networks

***Priyanka R.*[1] *and Satyanarayan Reddy K.*[2]**
[1]Assistant Professor, Department of Information Science and Engineering,
Cambridge Institute of Technology Bangalore, Affiliated to VTU, Belagavi (Karnataka), India.
[2]Professor & Head, Department of Information Science and Engineering,
Cambridge Institute of Technology, Bangalore, Affiliated to VTU, Belagavi (Karnataka), India.

(Corresponding author: Priyanka R.)

(Received 28 December 2019, Revised 24 January 2020, Accepted 28 February 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Demand and application of Wireless Sensor Networks (WSN) has grown rapidly during last decade. Wireless sensor networks follow distributed nature of sensor deployment, these networks are vulnerable to various threats which can affect the communication performance and functioning of WSN. These threats are widely known as security attacks on sensor nodes. Along with security threats, Quality of Service and energy efficiency is also considered as challenging task for researchers in WSN. For real-time applications, packet delivery and energy consumption are important tasks which can improve the performance of Wireless Sensor Network communication. Recent works are focused on the security and energy efficient communication in Wireless Sensor Networks. In this paper, we present recent studies in the field of WSN which includes security, sensor node localization and energy aware communication for better quality of communication. Drawbacks of WSN are security attacks, battery capacity is very less and there are practical problems in the deployment of the nodes. A comparative study is also presented by considering various threats on WSN architectural layers. Similarly, energy aware approaches are also compared based on the localization Error performance, Energy aware routing techniques and secure routing protocols for data encryption and decryption. This study shows the current problems of WSN communication in terms attacks on different layers and actions taken. The challenging factor in WSN is conserving the Energy for improving the network lifetime, improving performance and WSN localization.

Keywords: Attack, Energy Efficiency, Layer, Localization, Security, Performance Analysis, Wireless Sensor Networks.

Abbreviations: WSN, Wireless Sensor; GPS, Global Positioning System; DOS, Denial-Of-Service; TOA, Time Of Arrival; RSS, Received Signal Strength; LEACH, Low Energy Adopting Clustering Hierarchy; EECED, Energy Clustering Algorithm for Event Driven; EERRT, Energy Efficient Redundant Routing Protocol Received Signal Strength; GA, Genetic Algorithm; PSO, Particle swarm Algorithm; CH, Cluster Head; 3D-GAIDV, 3 Dimensional Genetic Algorithm based Improved Distance Vector Hop; AES, Advanced Encryption Standard; 3DES, 3 Dimensional Triple Data Encryption standard; 3D-PSODV, 3 Dimensional Particle Swarm Optimization with Distance Vector; 3D-GADV, 3 Dimensional Genetic Algorithm Distance Vector; 3D-DV, 3 Dimensional Distance Vector.

I. INTRODUCTION

A WSN consists of self-governing sensor nodes deployed in spatial domain to check climatic conditions or physical changes, such as noise, humidity, temperature, atmospheric pressure [1]. These sensors nodes are light-weight devices with cheap installation costs. They have restricted hardware and software resources, like low memory, smaller processing capacity, lesser input/output ports, etc. The Sensor Nodes are built to monitor the changes, detect those changes, and gather collected information from the environment. This accumulate data can be transmitted to particular device or person. Transmission occurs by a network of nodes. Sensor nodes contain limited power instruments with one or more sensors, central controller or processor, memories, inputs & outputs, energy sources, a trans-receiver and an actuator.

Remote Sensor Nodes comprise of low power on-board controller or processor, low speed radio antenna, limited memory, less sensitive sensor, battery for power, and in some cases, GPS (global positioning system) too. Batteries are the only source of energy for these nodes and thus, they have limited supply of energy. Once the installation of nodes is completed, the batteries cannot be replaced. Moreover, generating energy is also not possible, due to various reasons. Thus, energy conservation is a critical issue in WSNs and Energy Efficient schemes are highly important. In general, transmission requires higher amounts of energy. Hence, an Efficient Routing Protocol is very much required in WSNs, which minimizes unnecessary use of energy, and it also enhances the overall network lifespan. Shortest path routing is efficient and less energy is spent during data transmission. However, there are chances that all other transmission also takes place along this path, as it is the shortest path. This makes the devices in the path to deplete early and resulting in shut down of that path. Furthermore, there are other nodes which contain large battery power, that are rarely used.

So an efficient algorithm should distribute the load equally among all the nodes, to make sure that none of the node dies early [2].

A general architecture of standard wireless sensor node is depicted in Fig. 1 [9].

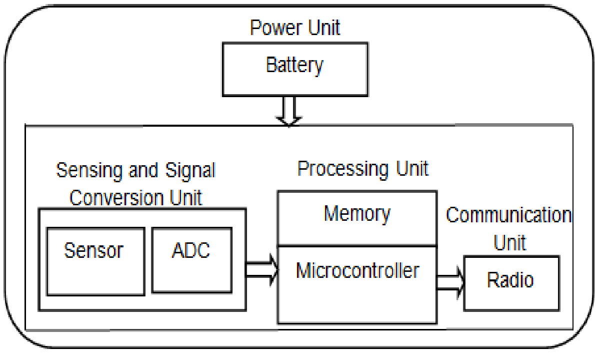

Fig. 1. A typical sensor node structure.

A typical sensor node comprises of five main components. The Sensing and Signal conversion unit is comprised of a sensor which senses data and gathers required information. Analog to Digital Convertor receives analog signals produced by the sensors and is digitized for transferring it to controllers for further processing. A microcontroller is often embedded in the processing unit along with memory unit for processing the data and controlling the functions of the other components. As the memory capacity in a node is very less, energy should be efficiently managed.

The mobility of sensor nodes in WSN affects the energy which reduces the lifetime of a network. This factor gives raise to constraint on energy.

A network of remote sensor nodes can be established by installing the nodes in a given area. The detected information from the node is transmitted to central observing station, commonly referred as sink or base station. The data travels from source to sink through multi-hop routing or flooding. The base stations will be set up at farther distance from the nodes. Therefore, higher number of hops and more energy is required to transmit data from source node to base station.

However, the number of hops can be reduced by installing multiple base stations. Thus, significant energy saving can be done at each nodes, which enhances the overall lifespan of the network [3]. Each sensor extracts different type of information from the atmosphere Battery is the main source of energy for the sensor nodes. Based on the functionality and requirement, the actuator may also be included within the sensors [4].

There are various attacks on sensor networks such as Interruption, Modification, Interception and Fabrication. The different layers of WSN are also prone to DOS attacks. The security issue focuses on active and passive attacks in WSN.

The limitations of the earlier study include Energy Constraints as outlined by Gao *et al.*, (2010) [10], Limited Hardware and Software Resources where the devices in WSN are lightweight and cheap [11], Random and Massive Deployment with self-governing repairs and Diverse Applications [13, 17]. In previous study, localization approaches focus mainly on 2D (two-dimensional) plane but in real time implementation the nodes are usually deployed in three-dimensional (3D) space in WSNs such as forest areas, defense and many more [42].

II. RELATED WORK

A. Types of WSN

Based on previous research, five types of parameters in WSN are possibly dependent on the where and how the sensors nodes are deployed and monitored. As per these parameters of sensor node installation, the WSN can be grouped into five different types as discussed below.

Ground (Terrestrial) WSNs: The terrestrial WSN are composed of numerous sensor nodes, which are cheaper and simpler than underground sensor nodes [5]. The sensor nodes are placed in a particular region and they are installed randomly. In such WSN, the communication must be reliable to overcome dense atmosphere. The sensor nodes should collect the information and transmit them efficiently to the nearest base station. In general, the energy constraint of sensor nodes limits the functionality of the network. Moreover, in many cases, the batteries cannot be replaced. However, as the sensor nodes in terrestrial WSN lie on the surface, sensor nodes can be set up with a solar cell or self-rechargeable batteries as secondary source of energy. But in most cases, this does not work. Therefore, it is more sensible to implement an energy saving mechanism, rather than embedding a secondary energy source.

Underground WSNs: Underground WSNs contains numerous sensor nodes which are placed inside the earth crust or mines and caves. They are used to monitor underground variations to check for volcanic activities, seismic activities and underground water flow [6]. The base station or any other normal nodes can be placed above the ground to forward the collected data from the underground nodes to central station. Their operational costs are also high, in comparison to terrestrial WSNs. The reason for such high cost is that the device has to function against all underground obstacles, such as water, soil, rocks, borrowing animals, weight of soil and objects above them. Due to presence of soil, the communication to external world needs more energy as substantial amount of signal is lost due to attenuation.

Aquatic (Underwater) WSNs: Aquatic WSNs are composed of few sensor nodes. They are deployed and setup under water. In comparison to sensor nodes in terrestrial WSNs, the aquatic sensor nodes are expensive and less number of sensor nodes is diffused in the concerned region.

Autonomous underwater vehicles are used to explore and extract useful information from sensor nodes. The distributions of sensor node in aquatic WSN are sparse. The nodes communicate underwater using acoustic waves [7].

Mobile WSNs: Mobile WSNs contains a number of moving Sensor Nodes, which interact with external environment to sense atmosphere changes. Mobile nodes have the ability to process the data like any other normal static nodes. Mobility on WSNs is primary implanted in defense and military application, and few industrial applications as well [8].

Multi-media WSNs: Multi-media WSNs are composed of vast number of cost-effective sensor nodes with embedded microphones, speaker, cameras and other multimedia devices. The connections in such networks are slightly different from traditional WSNs. However, the nodes can still sense external data, process them, etc. Additionally, they can perform information correlation, and data compression.

B. Applications of WSN

The WSNs are largely adopted in various real-time applications like forest monitoring i.e. fire or other activities of animals, defense applications such as surveillance, medical applications such as patient's movement tracking, and industrial applications such as machine automation. Despite of several advantages of WSN, it suffers from various challenging issues such as energy constraints which is critical issue in any WSN, as the Sensor nodes are powered by batteries, they have limited uptime and energy capacity [9]. To ensure longer lifespan of the WSN, the protocol and algorithms must be energy-aware and consume less amount of energy, limited hardware and software resources is another challenging issue in WSN because these devices have lower storage and memory capacity, slower processors, which contributes to fewer computations [12]. To address this issue, Sensor nodes uses flash memory for faster operation. As shown in Fig. 1, the central processing unit contains a microprocessor or a microcontroller, which performs data processing and computation of energy consumption. Moreover, sensor networks are made up of large number of sensor nodes, with over hundreds, sometimes thousands of devices. The sensor nodes will be deployed in harsh and remote location, and thus, they have to function accurately without manual supervision [13, 14]. Therefore, the sensor nodes must locate themselves in the network. They should be able to independently configure, adapt, sustain and repair themselves [15] in any type of environment such as dynamic, harsh, unknown environments. Generally, these networks are operated in different types of operating systems. Some of the popular OS for WSN are, Contiki, Tiny OS, Lite OS and Mantis Nano-RK [16]. Similarly, security is also a challenging task where different types of attacks can occur on networks.

Diverse Applications: The WSNs can be implemented for numerous applications [17]. Therefore, the requirements and specification for different applications are not similar. Till now, there is no technique or algorithm which can be implemented to suit all types of applications. The main reason being different criteria of the networks application. Motley middleware is a middleware used in WSNs [18]. This has assisted in enabling multi-application and shared infrastructure support for WSNs.

C. Types of attacks on WSN

Attacks on WSN network affects availability, confidentiality, authenticity, eavesdropping on communication and unauthorized data modification which are discussed here.

Interruption: Interruption is an attack on the network that badly affects its availability [19]. For instance, the attacks generally involve capturing or corrupting the nodes, tampering the data messages, inserting a malicious code. The fundamental aim of interruption is to keep the network unavailable to service by initiating denial-of-service (DoS) attacks [20].

Modification: Modification refers to unauthorized data modification by an unauthorized agent. Modification attacks are instilled application layer and network layer [19]. Data modification results in loss of integrity of the message [20]. The objective of modification is to generate misperception or mislead the users within the communication protocol.

Interception: Interception attack is imposed to disturb the confidentiality [19]. The sensor network can be compromised by an attacker to gain unauthorized access to a sensor node or transmitted data. Such attacks are usually performed by eavesdropping on the data carried in the messages [20].

Fabrication: Fabrication affects the authentication [19]. It is an attack on the authenticity of the message. Wireless sensor networks are vulnerable to numerous kinds of external attacks such as, traffic analysis, privacy attacks, collisions, and physical attacks [21].

Active Attack: Active attacks occur from unauthorized modifications or eavesdropping on communication in the network, by an external adversary. Depending on the security requirements, attacks on WSN are determined by the following parameters like Attacks on Availability of Network. And Authentication related attacks.

Passive Attack: In this attack, the unauthorized user inflicts an attack on WSN through sensing, tracking and monitoring an ongoing communication channel. A violation in privacy is considered as passive attack.

As presented in previous sections, the DoS attacks can target any layer of WSN. Thus, different attacks on different layers of WSN are present in subsequent sections. Table 1 presents the attacks and actions on different layers of the network.

Table 1: Attacks on different layers and Actions.

OSI Network Layers	Attacks	Actions
Network and routing Layer	Wormholes Hello flood attacks Sinkholes Sybil Acknowledgement -spoofing Selective forwarding Spoofed	Authentication using geographic location Redundancy Authentication and monitoring Authentication probing Bi-directional link verification Egress filtering monitoring and authentication Redundancy and probing
Physical Layer	Jamming Tampering	Tamper proofing, Hiding spread spectrum, Lower duty cycle Priority message
Transport Layer	De-synchronization Flooding	Authentication Client puzzles
Data link layer	Exhaustion Unfairness Collision	Error correction code Rate limitation Small frames

Physical Layer: Some of the commonly inflicted attacks at physical layer are frequency selection, data encryption, carrier frequency generation modulation and signal detection. The probability of physical layer attacks is high due to the easier task of gaining access to the physical layer of WSN. Attacks on physical layer can be analyzed as Node outage, Device tampering [34], path based, DOS and Jamming. However, Jamming and Tampering are two critical weaknesses in WSN which is discussed below.

— **Jamming:** Jamming results due to external attacks on sensor node, which creates interference in radio transmission frequencies.

— **Tampering:** Tempering is another physical layer attacks. In such attacks, the adversary can attack a node with help of another malicious node, to gain access to sensitive and confidential information.

Data Link Layer: The Data link Layer features functions such as, frame detection, data multiplexing, medium access, error correction, etc. It helps in establishing reliable links between point-to-point and point-to-multipoint communication in the network. The most popular attacks witnessed by these layers, are collision, unfairness and exhaustion. Attacks on Data link layer can be categorized as unfairness, collision, Traffic Manipulation and Resource Depletion [41].

— **Collision:** Collision occurs in the network, when two different nodes simultaneously forward two distinctive messages with identical frequency. Thus, the two messages collide and the information contained within will be corrupted. The receiver experiences checksum mismatch error which means that the receiver will be unable to recognize the packets. Such collision issues can be overcome by Error correcting code.

— **Unfairness:** Unfairness is also considered as a type of DoS. With the help of this attack, the unauthorized user can gain access to the information and can make illegal modification to the priorities of transmission and its duration.

— **Exhaustion:** When corrupted data packets are forwarded repeatedly, higher number of collisions occurs in the network. Therefore, substantial amount of energy will be lost. As collision requires retransmission of lost packets, more energy is wasted. One such possible solution to this problem is the TDM or time division multiplexing.

Network and Routing Layer: To improve energy efficiency, network and routing layer are very significant. They also assist in making sensor network more data centric, helps in addressing and knowledge of location. However, these layers are also susceptible to several attacks like Homing, Neglect and greed, rushing, node malfunction, Flooding, Sinkhole, Black hole, Wormholes, Sybil, eavesdropping and selective forwarding. Some critical attacks are discussed here.

— **Selective Forwarding:** The attacker can create a fake node to transmit faulty or corrupted messages. Such messages include black holes, which makes the nodes to reject genuine messages and accept faulty packets. The black holes can be detected and they can be diverted to different path [12, 13].

— **Sinkhole.** In sinkhole attack, a malicious node is created by the adversary, which traps and misleads the routing information. This makes an easier task for the attacker to perform selective forwarding [14].

— **Sybil:** Sybil attack arises in the network, when node has more than one identity. In such cases, the network cannot choose a particular node for a specific task, which results in chaos in network operations like, topology, fault-tolerance, and storage.

-Wormhole: A wormhole is considered as a low potential link between two different segments of a network. Actually, the link is established between two Nodes from two different segments of the network. This wormhole sink is used to transmit data from one location to other, until it reaches the sink node [15].

Transport Layer: The end-to-end communication between source and sink are established by Transport layer. Hence, this layer is also targeted by few attacks such as De-Synchronization, Data aggregation and clock skewing.

Vampire attacks are one of the Denial-Of-Service (DOS) attacks in WSNs, which hinders the routing algorithms and depletes the network resources. In a WSN, batteries are primary source of energy, and hence it is a vital resource. All sensor nodes rely on battery for energy and to support its operations. The vampire attacks concentrate on the battery and manage to deplete the residual battery power. So, the node is turned off, which gradually deactivates the network. Vampire attacks can be considered as a type of DOS attacks. In this type of attacks, faulty or unwanted messages are forwarded by malicious nodes which result in expenditure of energy for wasteful work.

Vampire attacks can be segregated into two types.

Carousel Attack: The attacker generates message which can repeatedly propagate along a path more than one time. The message keeps circling the same path over and again, along the same node. It is illustrated in Fig. 2.

Stretch Attack: In this attack, the attacker manually sets a longer path for a message from its source to destination. This creates a longer path, and the message covers as much nodes as possible. It is illustrated in Fig. 2. Due to longer transmission distance, the path covered by the message will be unnecessarily longer [7].

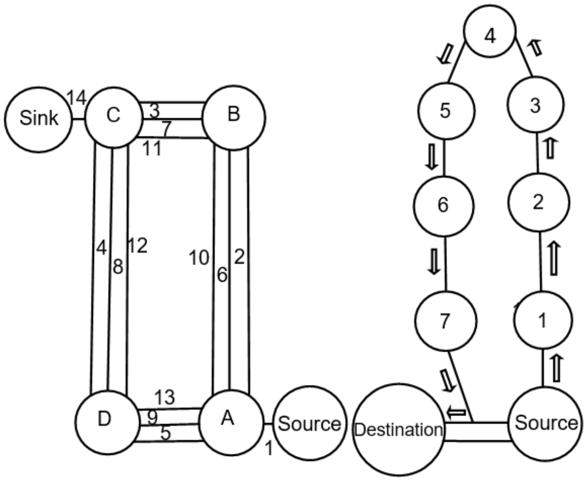

Fig. 2. Carousel and Stretch attack.

This section may each be divided by subheadings or may further divide into next heads as shown below.

III. METHODOLOGY

WSN Localization Techniques: Generally, the sensor networks are deployed randomly in a huge geographical region where determining the location of these sensor nodes is not feasible. In various applications the information collected by these nodes is not useful unless the location of sensor node is not available. Moreover, it may lead towards the collection of faulty information. Thus, the localization techniques are the interesting research topic in the field of WSN [35].

In order to solve these problems, several localization techniques have been developed. The existing techniques assume consider only limited number of nodes are equipped with GPS rather than installing GPS to each sensor node because it increases implementation cost. These sensor nodes are known as anchor nodes. In the considered network, other sensor nodes communicate with nearby nodes and estimate the distance using suitable localization techniques such as Time of Arrival (ToA) and Received Signal Strength (RSS) [36]. Currently, evolutionary and optimization techniques have been reported to improve the localization performance by reducing the localization error such as genetic algorithm for localization using one-hop neighbor computation [37]. Chagas *et al*., (2012) presented the two-phase centralized localization technique using combined Simulated Annealing (SA) Algorithm and Genetic Algorithm [38]. Singh and Sharma (2017) outlined the focus on optimization technique and Particle Swarm Optimization (PSO) based algorithm to reduce the localization error [39]. An evolutionary computation scheme which uses two objective functions to solve the localization problem with the help of simulated annealing model [40].

Energy aware approach for WSN: This section presents a brief summary on the existing energy aware techniques for WSN, including, data aggregation, routing, and shortest path computation. Wireless Sensor Networks have numerous advantages and disadvantages. In various applications, the sensor nodes are mostly installed at random positions. As soon as the nodes are installed, they should organize themselves and form a functional network to carry out designated task.

Furthermore, most WSNs applications are deployed at remote location, which requires a battery powered energy supply. This creates a problem for the network administrator to replace or replenish the drained batteries. Another disadvantage of WSN is the data redundancy, which reduces the efficiency of network. So find solutions for such limitation, numerous techniques are presented with an aim to enhance the overall lifespan of the network and reduce energy utilization. Hierarchical Routing is one of the fascinating mechanisms, which establishes an idea of cluster generation and allocating a central cluster head (CH) to perform special tasks within that cluster. It is an efficient mechanism to minimize energy utilization by performing data accumulation to lower the total number of data transmissions to the Base Station. Heinzelman *et al*., outlined Low Energy Adaptive Clustering Hierarchy (LEACH) which is one of the first hierarchical protocols [22]. The LEACH works by creating clusters of nodes on the basis of received signal strength. It uses local cluster heads (CHs) as routers to establish a path to the target node. Because the nodes transmit data directly to the cluster heads, the communication between nodes are reduced, which further reduced energy consumption. The LEACH protocol was so effective, that numerous other protocols were designed using this concept.

A comparison of LEACH based energy aware routing protocols as LEACH-B (Balanced) protocol, LEACH-C (centralized) protocol as shown in [23, 24] respectively. Energy Efficient Weight Clustering (EWC) protocol, Energy-Efficient Cluster Head Selection (NECHS) technique [26], Energy Clustering Algorithm for Event Driven (EECED), EAMR (Energy Aware Multipath Routing) as briefed in [25, 27]. Energy Efficient Redundant Routing Tree (EE-RRT) was proposed for WSNs [13]. The assumptions, CH selection, improvement over LEACH and drawbacks are discussed in Table 2 shown below.

Table 2: Brief description about LEACH algorithm.

Name of the Protocol	Assumption made	Cluster Head selection	Improvement of other algorithms over LEACH	Drawbacks
LEACH-B [23]	Simple and cheaper nodes in the network. They contain power management schemes to adjust the transmitting power of the data packets	Two stages: Random, and based on residual energy	A new adaptive strategy is proposed to select CH and to adjust their frequency of selection considering the energy dissipated	Higher overhead of computation for CH selection
LEACH-C (Centralized) [24]	Each node broadcasts it information about its present location and residual energy level to a concerned sink node	Base station selects CHs on the basis of the Residual energy of the node	LEACH-C enables larger number of rounds in smaller are of nodes in a network	Because of overhead on the Base station LEACH C is not much considered for larger area of networks
EWC [25]	The nodes are static, homogeneous, location aware and are distributed randomly	Distance, Residual energy, node's degree.	Network lifetime will be enhanced	Additional overhead in processing, which results in higher energy consumption to select CHs
NECHS [26]	The nodes are stationary, homogeneous, location aware and are distributed randomly,	Energy remaining and Degree of the nodes.	Selection of CH is enhanced by NECHS model by applying fuzzy logic.	There is no assurance that a non-CH node belongs to cluster, due to collisions of advertisement, or join packets

EECED [27]	Base station is assumed to that locations of the nodes are known. It follows event-driven protocol architecture. All sensor nodes are considered to be static and contain limited energy resources. All nodes are having capability of with energy management to adjust their transmitting Power	Residual Energy Level	Enhanced network lifetime, lower energy consumption compared to traditional LEACH	Additional overhead for the BS and elector nodes to choose appropriate CHs
LEACH-P [28]	The nodes are static, homogeneous, location aware and are distributed randomly	Including EMAR probability selection in conventional LEACH protocol	Network lifetime will be extended	Additional overhead to compute probability selection formula for choosing CHs
LEACH-M [29]	All nodes are considered homogeneous with respect to their antenna gain. The nodes are aware of their location information, which are extracted with the help of GPS. The location of Base station is fixed	Movements of the node and its residual energy	Mobility of the nodes is supported by declaration of membership to the existing LEACH protocol. The performance of LEACH-M is better than conventional. LEACH-M guarantees that the communication between node and CH are intact even if node is moving	Usage of Energy is not efficient in LEACH-M. Rate of data delivery for Huge number of packets are low, and more packets are lost if the CH moves before choosing a new CH for the next round
TL-LEACH [30]	The location of base station will be fixed and located far away from sensor nodes. The sensor nodes in the network are homogeneous and energy constrained. “High energy” nodes are not present in the communication	Random, Introducing primary CHi, and secondary CHij	Next stage of hierarchy is presented to create detailed information for forwarding it to a base station (BS) upon different levels. This will enhance the energy efficiency of the network	Additional overhead for selecting secondary CHs and creating cluster
Multi-Hop LEACH [31]	Base station is fixed. The nodes are assumed to be stationary,	Random	Maintaining Energy minimizing mechanisms like Multi-hop routing	Depletion of CHs will be problematic
LEACH-GA [32]	Sensor nodes are considered to be homogenous, stationary and uniformly distributed in the sensor region. They are assumed to contain similar energy levels. The location of base station will be fixed	Base station selects CHs on the basis of the Residual energy of the node, with the help of genetic algorithm	GA-LEACH estimates the optimal probability to be used in the selection process of CH.	Additional overhead on base station for calculating CH percentage
FL-LEACH [33]	Sensor nodes are considered to be stationary and homogenous with respect to their initial energy. Sensors are setup uniformly over the concerned region, while the location of BS is fixed	Random	Fuzzy logic on LEACH protocol was implemented to evaluate the percentage of Cluster Head to enhance the lifetime of the network	Maintain accuracy and managing fuzzification and defuzzification process is highly complicated

IV. RESULTS AND DISCUSSIONS

Comparative Performance Analysis: In this section, we preset a comparative analysis of WSN localization, routing and security aware routing techniques in terms of various performance parameters like localization error which is the The error that occurs estimation of distance during localization of the unknown nodes. Total numbers of alive nodes for different energy aware routing techniques are those nodes that are able to serve as the intermediate nodes in the WSN are termed as alive nodes. A plot of total number of alive nodes is presented in Fig. 4.

Although the performance seems to be similar at the initial stages, the Genetic Algorithm outperforms other algorithms. And encryption and decryption time for different routing protocols. In order to provide security, communication data must be encrypted and decrypted. Below given Fig. 3 shows a comparative analysis in terms of average localization error for varied node density as mentioned in [37].

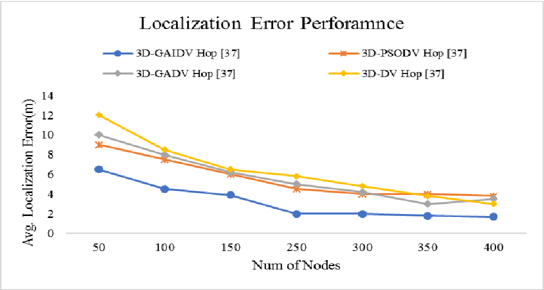

Fig. 3. Localization error performance.

According to this comparative study, we obtained the average localization error as 3.2 m, 5.5 4 m, 5.7 m and 6.34 m using 3D-GAIDV Hop, 3D-PSODV Hop, 3D-GADV Hop and 3D-DV Hop [37].

In next experiment, we evaluated the performance of different energy aware routing techniques. The performance is measured in terms of total alive nodes in the complete simulation shown in Fig. 4.

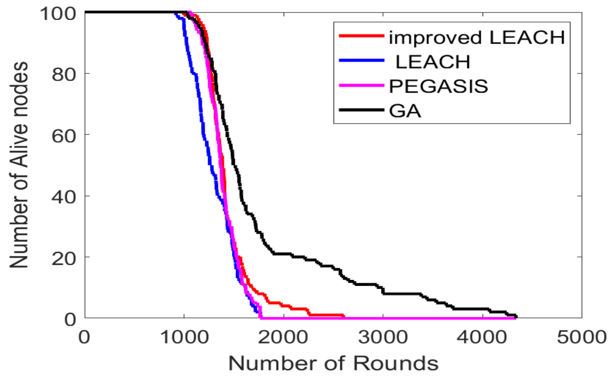

Fig. 4. Alive node performance.

The greater number of alive nodes indicates the better network lifetime [37]. This comparative study shows that the average number of alive nodes are obtained as 36%, 53%, 68% and 73% using Low Energy Aware Clustering Hierarchy (LEACH), Power Efficient gathering on Sensor information Systems (PEGAIS), improved LEACH and genetic algorithm. Finally, we present the comparative analysis for secure routing protocols as depicted in Fig. 5 and 6 for data encryption and decryption respectively [41].

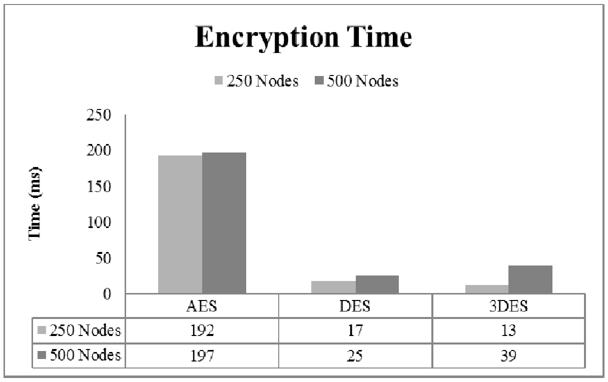

Fig. 5. Encryption Time Performance.

According to Fig. 5, we measured the performance in terms of encryption time for 250 and 500 nodes. The average encryption time is obtained as 194.5ms, 21ms and 26ms using Advanced Encryption Standard (AES) Data Encryption Standard(DES), and 3DES(Triple Data Encryption standard). Similarly, we measure the performance for decryption time as depicted in Fig. 6, where average decryption time is obtained as 210ms, 26ms, and 33.5ms using AES, DES, and 3DES.

V. DISCUSSION ON RESULTS

Simulation results show that 3D-GAIDV Hop [37] algorithm performs better in terms of localization error performance in comparison with 3D-PSODV Hop, 3D-GADV Hop and 3D-DV Hop [37]. Genetic algorithm performance with respect to alive nodes in a network is better compared to Low Energy Aware Clustering Hierarchy (LEACH), Power Efficient gathering on Sensor information Systems (PEGAIS), improved LEACH. With respect to encryption and decryption for secure routing algorithms Encryption time and decryption time is highest for Advanced Encryption Standard (AES). 3DES algorithm performance in terms of time of encryption and decryption is good when there are 250 nodes against time compared to DES. When the performance is analyzed for 500 nodes DES algorithm outperforms 3DES algorithm [41].

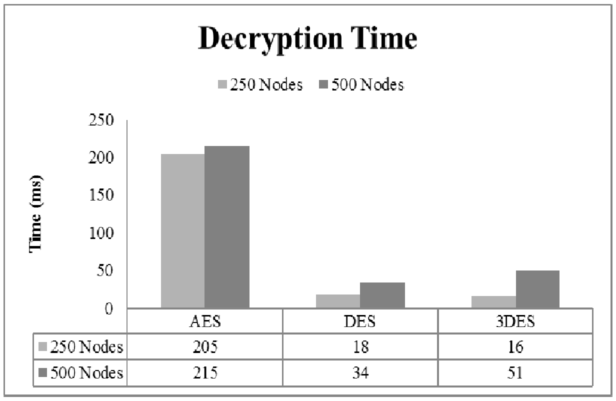

Fig. 6. Decryption time performance.

VI. CONCLUSION

This work is based on the study about Wireless Sensor Networks. During communication, Wireless Sensor Networks suffer from various attacks which may lead to inaccurate communication resulting in degraded quality of communication and it can affect the privacy aspects. Based on this issue, several models have been presented which are focused on the security improvement in wireless sensor networks. Along with the security aspects, wireless sensor networks suffer from the performance issues such as packet delivery and energy consumption etc. Several researches have been presented for improving the QoS of WSN.

In this paper, we have discussed such approaches for WSN which are mainly focused on security and QoS improvement. A comparative study is also presented for both security and QoS issues. These studies shows that still security and QoS performance of WSN can be increased by developing any adaptive schemes which can handle traffic and security threats. Moreover, the performance can be improved by developing energy efficient scheme for communication. The contributions towards the work are on a comparative study of LEACH based energy aware routing protocols with various parameters. Localization error performance is analyzed with various algorithms; Comparison of energy aware routing techniques is compared in terms of alive nodes. Encryption and decryption time is calculated for various algorithms.

VII. FUTURE SCOPE

This study has paved way for further research to improve performance of WSNs by adopting various energy aware transmission techniques for maximum network lifetime using optimization algorithms. Energy efficient routing technique and shortest distance Routing is considered in future work.

ACKNOWLEDGEMENTS

The authors would like to thank authorities of Visvesvaraya Technological University, Belagavi for their cooperation and full support.

Conflict of Interest. There is no conflict of interest for any of the authors in this paper.

REFERENCES

[1]. Yetgin, H., Cheung, K. T. K., El-Hajjar, M., & Hanzo, L. (2017). A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials, 19*(2), 828–854.

[2]. Benatia, M. A., Louis, A., Baudry, D., Mazari, B., & El-Hami, A. (2014). Impact of radio propagation in buildings on WSN's lifetime. *2014 Global Summit on Computer & Information Technology (GSCIT),* 1-6.

[3]. 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*, 1–16.

[4]. Rehan, W., Fischer, S., Rehan, M., & Rehmani, M. H. (2017). *A comprehensive survey on multichannel routing in wireless sensor networks. Journal of Network and Computer Applications, 95,* 1–25.

[5]. Ranjan, P., & Om, H. (2017). Computational Intelligence Based Security in Wireless Sensor Networks: Technologies and Design Challenges. *Computational Intelligence in Wireless Sensor Networks,* 131–151.

[6]. Agrawal, D. P. (2017). Deployed Large-Scale Wsns And Associated Design Steps. In Embedded Sensor Systems, Springer Singapore, 429-445

[7]. Zhou, Z., Fang, W., Niu, J., Shu, L., & Mukherjee, M. (2017). Energy-Efficient Event Determination in Underwater WSNs Leveraging Practical Data Prediction. *IEEE Transactions on Industrial Informatics, 13*(3), 1238–1248.

[8]. Abu znaid Ammar M. A., Idris, M. Y. I., Wahab, A. W. A., Qabajeh, L. K., & Mahdi, O. A. (2016). Low communication cost (LCC) scheme for localizing mobile wireless sensor networks. *Wireless Networks, 23*(3), 737–747.

[9]. Fei, Z., Li, B., Yang, S., Xing, C., Chen, H., & Hanzo, L. (2017). A Survey of Multi-Objective Optimization in Wireless Sensor Networks: Metrics, Algorithms, and Open Problems. *IEEE Communications Surveys & Tutorials, 19*(1), 550–586.

[10]. Gao, S., Zhang, H., & Das, S. K. (2010). Efficient data collection in wireless sensor networks with path-constrained mobile sinks. *IEEE Transactions on Mobile Computing*, *10*(4), 592-608.

[11]. Jun Zheng, Abbas Jamalipour (2009). Wireless Sensor Networks – A Networking Perespective, IEEE, A John Wiley & Sons, Inc. Publication, 7-8.

[12]. Sharma, S., Bansal, R. K., & Bansal, S. (2013). Issues and challenges in wireless sensor networks. In *2013 International Conference on Machine Intelligence and Research Advancement* (pp. 58-62). IEEE.

[13]. Anastasi, G., Conti, M., & Di Francesco, M. (2009). *Extending the Lifetime of Wireless Sensor Networks Through Adaptive Sleep. IEEE Transactions on Industrial Informatics, 5*(3), 351–365.

[14]. Peng, Y., Li, Z., Zhang, W., & Qiao, D. (2010). Prolonging sensor network lifetime through wireless charging. In *2010 31st IEEE Real-Time Systems Symposium* (pp. 129-139). IEEE.

[15]. Ye, D., Zhang, M., & Vasilakos, A. V. (2017). A Survey of Self-Organization Mechanisms in Multiagent Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47*(3), 441–461.

[16]. Jabeen, Q., Khan, F., Hayat, M. N., Khan, H., Jan, S. R., & Ullah, F. (2016). A Survey : Embedded Systems Supporting By Different Operating Systems. *International Journal of Scientific Research in Science, Engineering and Technology, 2*(2), 664-673.

[17]. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 8*(2), 2–23.

[18]. Katona, R., O'Shea, D., Cionca, V., & Pesch, D. (2016). Challenges in supporting diverse applications in a shared WSN: The Motley middleware. In *2016 27th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). IEEE.

[19]. Monnet, Q., Sassolas, M., & Mokdad, L. (2017). Modeling DoS attacks in WSNs with quantitative games. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[20]. Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L.,Cui, X. (2016). Attacks and countermeasures in the internet of vehicles. *Annals of Telecommunications, 72(*5-6), 283–295.

[21]. Mallikarjunan, K. N., Muthupriya, K., & Shalinie, S. M. (2016). A survey of distributed denial of service attack. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)* (pp. 1-6). IEEE.

[22]. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd annual Hawaii international conference on system sciences*, 1-10. IEEE.

[23]. Tong, M., & Tang, M. (2010). LEACH-B: An improved LEACH protocol for wireless sensor network. In *2010 6th international conference on wireless communications networking and mobile computing (WiCOM)* (pp. 1-4). IEEE.

[24]. Tripathi, M., Gaur, M. S., Laxmi, V., & Battula, R. B. (2013). Energy efficient LEACH-C protocol for wireless sensor network. *Third International Conference on Computational Intelligence and Information Technology (CIIT 2013),* 402-405.

[25]. Cheng, L., Qian, D., & Wu, W. (2008). An Energy Efficient Weight-Clustering Algorithm in Wireless Sensor Networks. *2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology,* 30-35.

[26]. Hu, Y., Shen, X., & Kang, Z. (2009). Energy-Efficient Cluster Head Selection in Clustering Routing for Wireless Sensor Networks. *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing,* 1-4.

[27]. Buyanjargal, O., & Kwon, Y. (2009). An Energy Efficient Clustering Algorithm for Event-Driven Wireless Sensor Networks (EECED). *2009 Fifth International Joint Conference on INC, IMS and IDC,* 1758-1763.

[28]. Danlin, Cai, & Daxin, Zhu. (2010). Research and simulation of energy efficient protocol for wireless

sensor network. *2010 2^{nd} International Conference on Computer Engineering and Technology, 1,* 600-604.

[29]. Kim, D. S., & Chung, Y. J. (2006). Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Network. *First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06),* 622-626.

[30]. Loscri, V., Morabito, G., & Marano, S. (2005). A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). VTC-2005-Fall. 2005 *IEEE 62nd Vehicular Technology Conference*, 1809-1813.

[31]. Aslam, M., Javaid, N., Rahim, A., Nazir, U., Bibi, A., & Khan, Z. A. (2012). Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks. *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems,* 1232-1238.

[32]. Liu, J. L., & Ravishankar, C. V. (2011). LEACH-GA:Genetic Algorithm-Based Energy-Efficient Adaptive Clustering Protocol For Wireless Sensor Networks. *International Journal of Machine Learning and Computing, 1*, 219-222.

[33]. Al-Ma'aqbeh, F., Banimelhem, O., Taqieddin, E., Awad, F., & Mowafi, M. (2012). Fuzzy logic based energy efficient adaptive clustering protocol. *Proceedings of the 3rd International Conference on Information and Communication Systems - ICICS 12,* 1-5.

[34]. Anchugam, C. V., & Thangadurai, K. (2016). Security in Wireless Sensor Networks (WSNs) and Their Applications. *Information Fusion for Cyber-Security Analytics,* 195–228.

[35] Goyal, S., & Patterh, M. S. (2015). Modified Bat Algorithm for Localization of Wireless Sensor Network. *Wireless Personal Communications, 86*(2), 657–670.

[36]. Arora, S., & Singh, S. (2017). Node Localization in Wireless Sensor Networks Using Butterfly Optimization Algorithm. *Arabian Journal for Science and Engineering, 42*(8), 3325–3335.

[37]. Sharma, G., & Kumar, A. (2017). Improved range-free localization for three-dimensional wireless sensor networks using genetic algorithm. *Computers & Electrical Engineering, 72,* 808-827.

[38]. Chagas, S. H., Martins, J. B., & de Oliveira, L. L. (2012). Genetic Algorithms and Simulated Annealing optimization methods in wireless sensor networks localization using artificial neural networks. *2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS),* 928-931.

[39]. Singh, S. P., & Sharma, S. C. (2017). A PSO Based Improved Localization Algorithm for Wireless Sensor Network. *Wireless Personal Communications, 98*(1), 487–503.

[40]. Wang, H., & Zhang, L. (2018). An Improved Simulated Annealing Localization Algorithm for WSN. *2018 IEEE 3rd International Conference on Communication and Information Systems (ICCIS)*, 93-96.

[41]. Mansour, I., & Chalhoub, G. (2012). Evaluation of different cryptographic algorithms on wireless sensor network nodes. *2012 International Conference on Wireless Communications in Underground and Confined Areas,* 1-6.

[42]. Rashid, B., & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of Network and Computer Applications, 60,* 192–219.

How to cite this article: Priyanka, R. and Satyanarayan Reddy, K. (2020). A Comprehensive Survey on Energy Efficient Routing Techniques and Various Attacks in Wireless Sensor Networks. *International Journal on Emerging Technologies*, *11*(2): 57–65.