Comparative Review of Routing Protocols for Energy-Efficient and Security in Wireless Sensor Network

T.C. Okeahialam[1], C.T. Ikwuazom[1], C.G. Onukwugha[2], D. O. Njoku[2], J.E. Jibiri[3]

[1]*Department of Information Media Technology, Federal University of Technology, Minna, Niger State-Nigeria*
[2]*Department of Computer Science, Federal University of Technology, Owerri-Imo State, Nigeria*
[3]*Department of Information Technology, Federal University of Technology, Owerri, Imo State-Nigeria*

***Abstract*: Recent developments in advanced wireless system have resulted in several improvements in the deployment of sensor networks communicating wirelessly. In order to monitor and control physical processes or parameters in a given system or environment, sensing device(s) is/are required. Thus, wireless sensor network (WSN) is a connection of sensor nodes designed to sense data from environment where they are deployed according to application. One of the most critical issues in WSN is the energy-efficiency. As a fundament factor to effective WSN installation, energy-efficient in the operation of WSN is a necessary topic that has attracted great attention in wireless sensor applications. Another important issue is the security of the WSN. As a result of the sensitive of data gathered by WSN, securing its nodes especially the sink node, will help prevent attackers from stealing important data that require high confidentiality in such areas as military applications. This paper has reviewed some of the routing protocols that have been designed for energy-efficient operation to prolong the lifetime and provide security for nodes of WSN**

***Keywords*- Energy-efficient, Routing protocol, Security, Wireless sensor network**

I. INTRODUCTION

Since wireless sensor networks (WSNs) technology are been extensively installed for use in both military and commercial applications, this study is motivated from the perspective of recent protocols that have been proposed to enable energy-efficiency and sink node security because these networks are remotely deployed, and as such are vulnerable to malicious attack and usually suffer performance degradation due to energy sapping. As a result of the mutual nature of wireless communication network, an attacker is capable of easily spying on the wireless communications network either by acquiring personal sensor devices or by exploiting other wireless devices capable of checking message transmission. Despite the fact that all traffic or message in a security WSN is encrypted, the relative information that is exposed is significant. That is the information that revealed the place the communication took place and who took part in the communication. The task performed by the sink node in the sensor network makes it a high potential target for attack; as such, sink node privacy is important to the security of a WSN deployed for strategic use because of the sensitivity of the information it carries. The anonymity scheme helps to hide or protect the sink node from an adversary.

In this paper, an empirical review of literature on routing protocols for WSNs based on energy efficient and sink node privacy is discussed.

II. PRIVACY OF WIRELESS SENSOR NETWORK

Understanding the architectural layer of a network is necessary to defend and protect a WSN. There is need for a high degree of collaboration and harmonization for effective communication between sensors. These communications are composite and have to be broken into subtasks that are implemented independently[1]. The architectural layer of a network aids the implementation of these subtasks. The most generalized network layering model is built around the Open System Interconnection (OSI). The common network layering architecture based on the OSI is illustrated in Figure 1. The structural design that describes the functionality of the network is divided into layers that jointly form the network protocol stack [2]. Every one of the layer in stack carries out a related subset of the tasks needed to interact with another system. The protocol stack integrates power and routing awareness, combines data with networking protocols, efficiently communicates power via wireless medium, and supports collaborative efforts among sensor nodes [3]. The security issues at each layer can be analysed and determined the way and manner security strategies can be implemented at each layer of known layered network architecture.

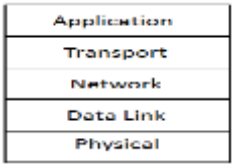

Figure 1 Five layers of the network on the OSI model [2]

The responsibility of the physical layer includes selection of frequency, generation of carrier frequency, detection of signal, modulation, and encryption of data [3]. The simplest way of protecting sensors is at the physical layer. The major types of physical attacks are jamming and tampering. The normal protection against jamming entails different forms of frequency hopping communication that requires more intricacy than employing low-power, low-cost sensors. The nodes can be physically tempered with and interrogated or compromised by an attacker [4]. Protection mechanisms such as passive temper as well as protective coating and temper seals are famous in sensors due to the fact that they do not need extra circuitry or energy. Even as intrusion detection is a exceptional first line of protection if the sensor is located, the fundamental functions are well known, and the implementation is left to manufacturers of commercial sensor.

The multiplexing of data streams, detection of data frame, medium access control (MAC) and control of error are the responsibility of the data link layer. It makes sure that there is consistent point-to-point and point-to-multipoint connections in a communication network. The MAC protocol creates communication connections for transfer of data [3]. The availability of the WSN is compromised and the nodes' battery depleted by attacks at the link layer of the data[4]

The communication reliability for point-to-point data exchanged by sensor nodes is provided by the transport layer[3]. This layer is in particular, required when the system will be accessed via the internet or some other external network, just like the case for the sink node. The attacks that are capable of threatening the WSN security at the transport layer are flooding and desynchronization attacks [5].

Communication with the stack by the application programmes is facilitated by the application layer. For instance, the hypertext transfer protocol (HTTP), which is an application protocol that is used for internet browsing, is used to connect to the internet browser (the application) to the layering stack for the internet browsing experience.

There are several literatures on network layer privacy. Implementation of privacy tactics at the network layer require specific protocols for multi-hop routing to be developed. The delivering of data from a sensor node to the sink node is achieved using these protocols at the same time as ensuring that privacy is protected [4]. There are number of innovative techniques to maintain the privacy of WSN at the network layer. These techniques or approaches can be divided into two types: source-location privacy and sink-location privacy [5].

A. Sources Node Technique

Environmental sensing takes place at the source node. There are a number of reasons for protecting the privacy of the source node, failure to do this, can be detrimental. As mentioned earlier, sensors are vulnerable at any level of the network protocol stack. In a situation that the security of a source node is compromised, the node becomes exposed to detection, intrusion and meddling. Security agency depends on WSN applications for intelligence gathering. The attacker can locate and obliterate a source node if its privacy is compromised. Even without obliterating the node, the attacker can destabilize the WSN by influencing the traffic at source node either by increasing the volume of traffic or by deliberately bypassing it. Data gathering by sensors is an important function of the network, and compromising a source node can undermine the effectiveness of the WSN.

B. Sink Node Techniques

The problem with location privacy for the sink node is that the network traffic is asymmetric, such that remote nodes from the sink node see dramatically less traffic compared to nodes within immediate range of the sink node.

Deceptive Packets

Deceptive packets are generated from low traffic volume sensor nodes and ensure the avoidance of routing through high traffic areas, ending their transmission at another low traffic volume node [6]. The deceptive packets protocol presumes that the attacker is carrying out traffic analysis within the WSN and can correlate data transmissions to find out the end to end path.

The Belief is a value which represents the confidence of the attacker that the destination node is the sink node [6]. The purpose of using deceptive packets is to make the belief values of other nodes similar to or higher than the sink node. This technique is like the source simulation approach for source-location privacy. The difference between the two is the method to generate these deceptive packets.

The drawback of the deceptive packet method is that its performance is extremely variable. In order to calculate the belief values, the adversary must analyse the data it has collected. Deceptive packets make use of online processing to imitate the belief calculations of the adversary and find out where additional traffic should be generated. If the attacker is calculating the belief values at a different rate to the one the additional deceptive packets are being generated, then it is likely that the attacker may not be foiled by the deceptive packets. The greatest challenge to this is that there is a considerable amount of communication overhead associated with evaluating the belief and adjusting the volume and location of the deceptive packets. It is difficult to optimize the minimizing communications overhead and normalizing the belief value of multiple nodes.

Location Privacy Routing

In the Location Privacy Routing (LPR) protocol, every one of the sensor divides its neighbours into two groups: a closer group comprises of neighbours closer to the sink node, and

another group of neighbours that are farther from the sink node. When a packet is forwarded by a sensor, neighbours are randomly selected from one of the two groups. The route for multiple messages emanating from the same source node is not always the same due to the fact that next hop is selected at random. The two groups make it more complicated to predict the next hop and direction of the sink node for the reason that traffic does not always travel in the cardinal direction of the sink node [7]. Finally, this means that an attacker that is carrying out a packet tracing attack has to take several hops before getting to the sink because it is often deviated in the wrong direction.

If LPR is applied alone, the location privacy will not be significantly strong in protection. This is because the entire traffic movement in the network still points toward the sink node. Even though this limitation can be reduced by increasing the possibility that a sensor forwards to a neighbour on the farther group, it causes longer delay and higher delay and higher energy costs [7].

One way to address this problem is to integrate LPR with fake packet injection similar to deceptive packets. The basic concept of fake packet injection is that when a real data packet is forwarded by a sensor node, it can generate a fake packet and transmits it to a neighbour randomly selected from the farther group. This leads an attacker away from the sink node, distributes the outgoing packets direction even as data latency for real data is reduced, and enhances the location privacy of the sink node in the WSN. These techniques complement one another but are in the end challenged by a large-scale attacker who can see that all real messages eventually arrive always at the sink while fake messages do not.

k- anonymity

The objective of the *k*-anonymity model is that at least *k* entities show the same characteristics as nodes located close to the sink. In achieving *k*-anonymity, a Euclidian minimum-spanning tree-based routing algorithm is developed to route traffic so that traffic volumes are equally high at *k* sensor nodes in the WSN. Since at least *k* nodes show related traffic statistics, an attacker intending to locate the sink node has to locate and check all nodes within the communication range of each node [5].

On the other hand, positioning *k* nominated nodes within the WSN is difficult as it affects two conflicting objectives: the routing energy cost and the achievable privacy level [5]. This is actually an optimization problem which involves prioritizing one objective or the other.

Randomized Routing with Hidden Address

The approaches discussed so far have assumed an inactive attacker whose methods are restricted to observing network traffic. An attacker who is active can influence a node and read the header field of a packet to spot the receiver. The Randomized Routing with Hidden Address (RRHA) technique keeps the identity or characteristics of the location of the sink secret in the network. Sensors do not know who and where the sink is when packets are being routed and do not indicate a destination when reporting their measurements. Different random paths are used to forward the packets all along a specified path length and are then removed when the length is reached [8].

Some packet delays are introduced by the random path taken by RRHA .The more time a packet remains in the WSN, the more energy it consumes. Once there is high traffic volume, the delay occasioned by the random paths can build up to cause considerable network congestion, overstressing the delay further and degrading the performance. The major limitation of RRHA is that it cannot assure that the sink will receive the data. Simulations revealed that the longer the path length, the higher the success rate of information getting to the sink [8]. Nevertheless, in many applications that are time sensitive, this is obviously an unacceptable result.

C. Energy Efficiency in WSN

Conservation of energy in a WSN is an important issue since all the sensor nodes are in a network powered by limited battery sources. Designing energy efficient system for a WSN has attracted significant interest from many researchers. This has brought about in the development of different techniques for saving the limited energy of the sensor nodes, and by extension prolonging the life of the network [9];[10]; [11]; [12].

Sensors make use of their energy for sensing and processing data and also to carry out transmitting and receiving data. More energy consumed by the communication subsystem of a sensor node consumes than the processing subsystem. It has been revealed that transmitting one bit of data may take as much energy as executing a few thousand computational instructions[9]. Therefore, it is essential that energy efficiency be focused on the communications subsystem as only minimal gains are achieved by optimizing the energy of the sensing and processing subsystems. In developing energy efficient communication methods in a WSN, the focus will be on the network layer of the protocol stack. Efficient models or algorithms can be developed at the network layer such that consistent route setup and relaying of data from the sensor nodes to the sink is accomplished and the lifetime of the network is maximized [13].

III. SECURITY REQUIREMENT AND POTENTIAL ATTACKS IN WSN

A. Security Requirement in WSN

The WSN is a delicate network in the particular area of deployment. The following are the security requirements of a typical wireless sensor network (WSN).

i. Authenticity and integrity: harmful massage can alter the originality and uniqueness of the data passing through the WSN, the authentication of data as well as the sender. These are also essential security requirements. Source authentication offers the reliability of originality of the sender. Data authentication guarantees the receiver that the data has not been changed at some point in the transmission [14].

ii. Confidentiality of Data: the most important requirement of military, security agency and other commercial applications in the deployment of WSN is the data confidentiality. Encryption of data is the normal method that prevents illegal user intrusion in the WSN leading to the data confidentiality.

iii. Availability: It is expected of a sensor node be available at what time it is needed. Since sensor nodes have limited battery power, needless computations can weaken them before their normal lifetime and thereby rendering them unavailable [14]. In the course of implementing the security policies in WSN, the unnecessary computations and hence the battery power must be taken into consideration.

iv. Freshness: when confidentiality and integrity is achieved, the focus will then be on the data freshness passing through the WSN. Informally, data freshness implies that the data is up to date, and it guarantees that no old messages have been replayed [15]. This requirement is particularly significant when there are shared-key approaches engaged in the design. Typically shared keys have to be changed over time. Nevertheless, it takes time for new shared keys to be transmitted to the whole network. This way, it is simple for the attacker to use a replay attack [14].

B. Potential Attacks in WSN

The security integrity of a WSN can be compromised by the following categories of attacks:

i. Secrecy and authentication attack: Standard cryptographic methods can shield the secrecy and authenticity of communication channels from malicious attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets [14].

ii. Network availability attack: Attacks on network availability are usually referred to as denial-of-service (DoS) attacks. Any layer of a sensor network may be targeted by DoS attacks [14].

iii. WSN physical attack: In this attack, full control over some sensor nodes through direct physical access is gained by attackers [16]. As full control over sensor node in the WSN is acquired by attacker, it becomes very much easy to gain access over the memory of the node and provides opportunity to access the encrypted key stored on the node which prevents the unauthorized access to the network.

iv. Attack on WSN physical layer: the physical layer of a WSN is responsible for actual transmission and reception of data, frequency selection, and carrier frequency generation, signaling function and data encryption [17]. Transmission and reception of data between varieties of nodes of the WSN brings about the radio interference and jamming.

v. Jamming: this is one of the most frequent attacks carried out by adversaries or attackers by knowing the transmission frequencies used in the wireless sensor network.

vi. Attack on WSN Link Layer: The data link layer of WSN is accountable for data streams multiplexing, detection of data frame, medium access and error control. This layer is susceptible to data collision when more than one sender tries to send data on one transmission channel [14].

vii. DoS Attack by Collision Generation: collision is generated to weaken the sensor node's energy. In a bid to generate collision, the adversary pays attention to the transmissions in WSN. When the attacker gets to know the starting of a message, a radio signal is sent for a small amount of time to interfere with the message [16]; [14]. As a result of this attack, the receivers is not able to receive the message correctly [14].

viii. Selective forwarding: this is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to reduce the suspicion to the neighbour nodes. The effect becomes worse when these malicious nodes are closer to the base station [18]; [14]. Then several sensor nodes route messages via these malicious nodes. As a result of this attack, a WSN may give incorrect measurement about the environment which adversely impact on the purpose of mission critical applications such as, military surveillance, security report and emergency monitoring.

ix. Sinkhole attack: In this type of attack, a compromised node attracts a large number of traffic of nearby neighbours by spoofing or replaying an advertisement of high quality route to the base station [14]. Sinkhole attack is also known as black holes attack. Black hole attack impacts on different parameters of WSN like energy, delay etc.

x. Wormhole Attack*:* this is a critical attack, in which the attacker receives packets at one point in the network, channels them through a less latency link than the network links to another point in the network and replay packets there locally [14]. This persuades the neighbour nodes of these two end points that these two distant points at either end of the channel are very close to each other. If one end

point of the tunnel is at near to the base station, the wormhole tunnel can attract significant amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station [14].

xi. Sybil Attack: In this attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [14].The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node [19].

xii. WSN Transport Layer attack: In network layer end to end connections are managed.

xiii. WSN Flooding Attack: According to [20]; [21]; [14] at this layer, adversaries exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node [14].

IV. IMPLEMENTED PROTOCOLS

[22] presented different types of security attacks, their effects and defense mechanisms in Wireless Sensor Network (WSN) which is vulnerable to security attacks and threats as a result of its characteristics and limitations. The study focused on various aspects of different security attacks, their effects and defense mechanisms corresponding to each attack. The author believed that the study has a very strong concept about the security issues; existing attacks and they can also use the ideas and concepts to build more secure wireless sensor network system in future. Also, a direction can be obtained to develop new security mechanisms to protect new possible attacks along with existing ones.

[23] presented a set of security protocols optimized for sensor networks in terms of confidentiality and authentication, data freshness, data integrity. Using the sensor network Encryption Protocol, the authors explained the basic primitives for providing confidentiality, authentication between the two nodes, data integrity and message freshness present in a wireless sensor network. That was designed as base component of Security Protocols for Sensor Networks. In the study, primarily two security properties were checked, which were authenticity and confidentiality of similar messages components. The first case was the communication between the networks nodes and base station in order to retrieve node confidential information. In the second case is a key distribution protocol in a sensor network using sensor network encryption protocol (SNEP) for securing messages.

[24] presented an enhanced source location privacy based on data dissemination in WSN. The study identified and addressed the issue of eavesdropping in the exposed environment of the sensor network, which rendered it vulnerable for the adversary or attacker to trace the packets to find the originator source node, hence compromising the contextual privacy. The method provided an enhanced three-level security system for source location privacy. The base station was at the centre of square grid of four quadrants and it was surrounded by a ring of flooding nodes, which act as a first step in confusing the attacker. The fake node was set up in the opposite quadrant of actual source and start reporting base station. The selection of phantom node using the developed algorithm in another quadrant provided the third level of confusion. The results showed that Dissemination in Wireless Sensor Networks was able to reduce the energy consumption by 50%, safety period increased by 26%, while providing a six times more packet delivery ratio along with a further 15% decrease in the packet delivery delay as compared to the tree-based method. It also provides 334% more safety period than the phantom routing, while it lags behind in other parameters as a result of the simplicity of phantom method. The authors maintained that the study illustrated the privacy protection of the source node and the designed procedure could be useful in designing more robust algorithms for location privacy. A schematic of the model is shown in Figure 2 and it was assumed that all the sensor nodes are evenly distributed in the surveillance area.

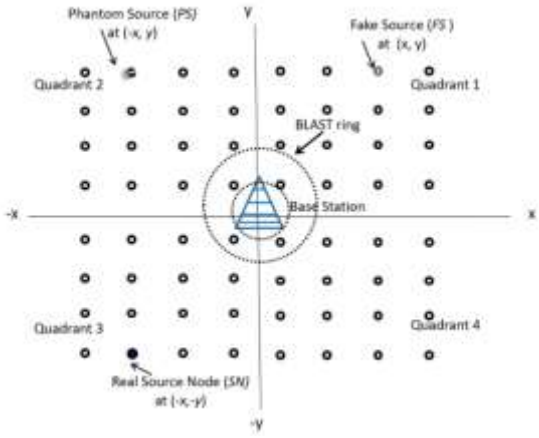

Figure 2 Proposed model configuration [24]

[25] proposed modified LEACH protocol known as MaximuM-LEACH for increasing lifetime of WSN. The modified algorithm consisted of two phases: the setup phase and the steady state phase. In the setup phase, the base station knows the energy status and location of all the nodes. The

base station evaluated the average energy of the network. All the nodes with energy greater than the average energy were selected as cluster heads. The steady state phase is similar to the steady state phase of the LEACH and LEACH-C protocols. The nodes send data to the cluster head. The study focused on improving LEACH performance to reduce the number of nodes stranded as the cluster heads die and on increasing network lifetime and throughput via load balancing. Figure 3 is a flowchart showing the comparative study of different LEACH algorithm and its types.

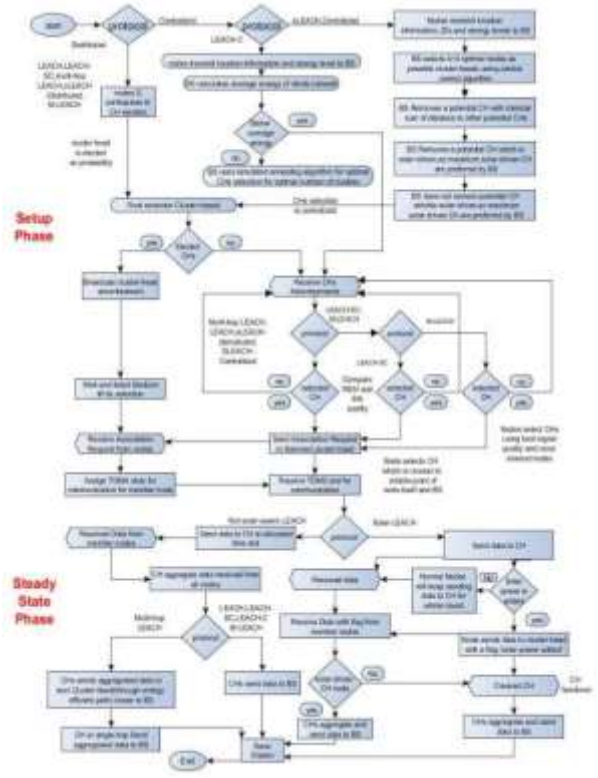

Figure 3 Flowchart of LEACH protocol and its types[25]

[26] proposed an adaptive coding (AC) method that can be adapted with the channel state and inter-node distances so as to decode and correct the packets or request for retransmissions. The authors examined the energy performance of error control coding and proposed an energy efficient and adaptive coding framework for multi-hop WSN. The proposed method considered the trade-off between the decoding energy and transmission distance by taking into account the free space and multipath propagation to choose adaptively when to apply Forward Error Correction (FEC) decoding or request for retransmissions. The proposed AC method proved to be more energy efficient compared to Automatic Repeat request (ARQ) and FEC schemes in multi-hop WSN. The mechanism of the proposed adaptive algorithm is shown in Figure 4.

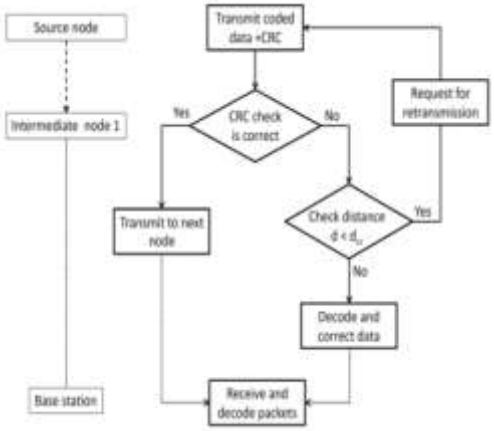

Figure 4: Adaptive coding algorithm [26]

[27] proposed network coding aware energy efficient routing (NAER) for wireless sensor networks. In order to deal with the problem of network coding condition failure and neglecting of node energy, a network coding aware energy efficient routing for wireless sensor networks was proposed. In terms of the in-depth analysis of existing network coding condition, universal network coding condition (UCC) was presented to avoid network coding condition failure problem. Based on UCC, the cross layer network coding discovery method combined with coverage control and topology control was presented to further increase the number of network coding opportunities. Additionally, a network coding aware energy efficient routing metric (NERM) was presented, which took into account coding opportunity, node energy, and link quality jointly. Simulation results demonstrated that NAER improved the accuracy of coding discovery system, increases the number of coding opportunities, saves node's energy consumption, and extended network lifetime. The concept of cross layer communications in the proposed coding scheme is shown in Figure 5.

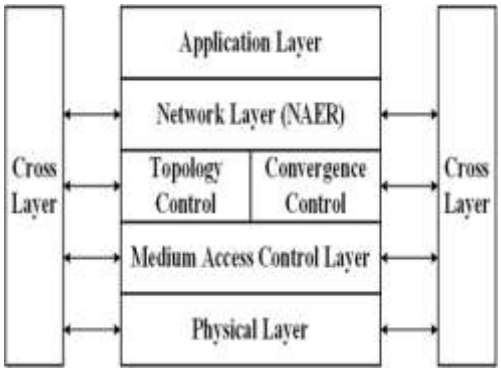

Figure 5: cross layer interaction principle of NAER coding scheme [27]

[28] presented an energy efficient routing protocol for wireless sensor networks (WSNs) using A-star algorithm. It proposed a new energy-efficient routing protocol (EERP) for WSNs using A-star algorithm. The proposed routing method

improved the network lifetime by forwarding data packets via the optimal shortest path. The optimal path can be discovered with regard to the maximum residual energy of the next hop sensor node, high link quality, buffer occupancy and minimum hop counts. Simulation results indicate that the proposed scheme improves network lifetime in comparison with A-star and fuzzy logic protocol.

[29] presented an improved energy-efficient routing protocol for WSN. A low-energy adaptive clustering hierarchy (LEACH) was proposed as an application-specific protocol architecture for WSNs. Nevertheless, the authors stated that without considering the distribution of the cluster heads (CHs) in the rotation basis, the LEACH protocol would increase the energy consumption of the network. In order to improve the energy efficiency of the WSN, the authors proposed a novel modified routing protocol. The proposed scheme improved energy-efficient LEACH (IEE-LEACH) protocol considered the residual node energy and the average energy of the networks. In order to achieve reasonable performance in terms of reducing the sensor energy consumption, the proposed IEE-LEACH was responsible for the numbers of the optimal CHs and prohibits the nodes that were closer to the base station (BS) to join in the cluster formation. In addition, the proposed IEE-LEACH used a new level for electing CHs among the sensor nodes, and used single hop, multi-hop, and hybrid communications to further improve the energy efficiency of the networks. The simulation results demonstrated that, compared with some existing routing protocols, the proposed protocol substantially reduced the energy consumption of WSNs. The flowchart of developed protocol is shown in Figure 6.

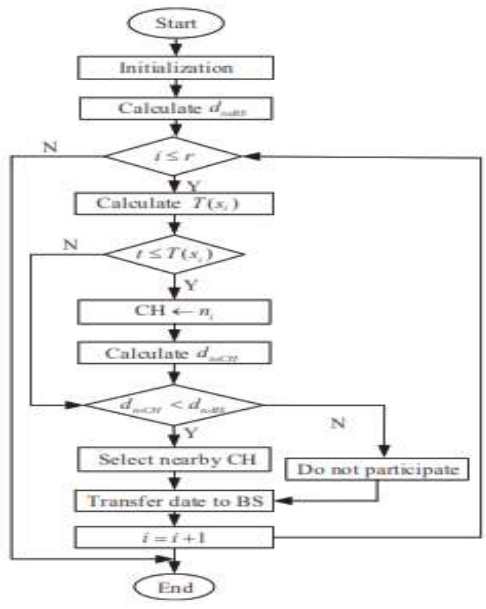

Figure 6: Flowchart of proposed protocol [29]

[5] Presented a study on enhancing sink-location privacy in WSNs through *k*-anonymity. In order to protect the sink-location privacy from a powerful adversary with a large-scale view, the author proposed to achieve *k-anonymity* in the network so that at least *k* entities in the network were impossible to differentiate to the nodes around the sink with regard to communication statistics. Organizing the location of *k* entities was complex as it impacted two conflicting objectives: the routing energy cost and the achievable privacy level, and both objectives were evaluated by a non-analytic function. The authors modeled such a positioning problem as a nonlinearly constrained nonlinear optimization problem. In order to solve this problem, a generic-algorithm-based quasi-optimal (GAQO) method that obtained quasi-optimal solutions at quadratic time was designed. The obtained solutions closely approximated the optima with increasing privacy requirements. In addition, to solve *k*-anonymity sink-location problems more proficiently, an artificial potential-based quasi-optimal (APQO) method was developed that was of linear time complexity. An extensive simulation results showed that both algorithms were capable of effectively finding solutions to hide the sink among a large number of network nodes.

[30] studied privacy preservation of sink node location in wireless sensor network. The study proposed a technique to preserve the privacy of the sink node in addition to secure data transmission from adversaries' attacks. A random fake sink node (RFSN) approach was used to mislead the adversary. After forming the clusters, and cluster heads (CH), one of the cluster head would be selected randomly as fake sink node (FSN), and all other CHs send fake data packets to this FSN to mislead adversary. Fake sink nodes were changed dynamically at intervals to make it difficult for an adversary to differentiate between FSN and original sink node. The author maintained that simulation results showed that the privacy of the sink node location was preserved from the adversaries with an extended lifetime of sensor nodes. The simulation result also proved that the proposed technique with RSA algorithm offered more security with reduced packet loss. The model of the proposed WSN simulated in NS2 simulator is shown in Figure 7.

Figure 7: Sink node model simulated NS2 simulator [30]

[31] presented achieving source location privacy protection in monitoring WSNs through proxy node routing. The study addresses some limitations of four existing methods by offering highly random routing paths between the source nodes and sink node. The method randomly sends packet to the sink node through tactically positioned proxy nodes to guarantee the routes are highly confusing to the adversary. In order to achieve high privacy, the proposed method used a randomizing factor to generate a new random route for every successive packet. Simulation results demonstrated that the proposed method offered longer safety period and stronger privacy to outperform other methods. Additionally, the method provided stronger privacy against both, patient and cautious adversary models. The proposed routing algorithm achieved trace time of 900 which is 0.09 privacy level. Figure 8 is an illustration of the packet routing technique using the proposed proxy node routing scheme.

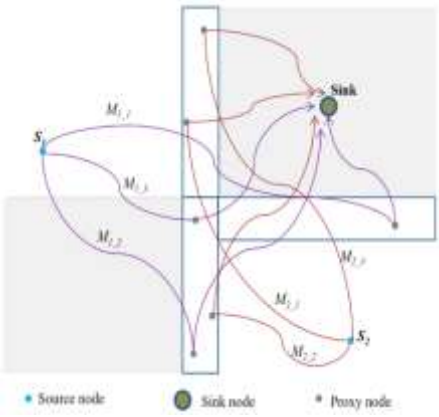

Figure 8: Proxy node routing scheme [31]

[32] proposed a new privacy preserving method to secure mobility control protocols against attacks that locate and sabotage the sink node. The privacy preserving method confused the sink location with dummy sink nodes. Analysis showed that the method could effectively hide the sink location via anonymity. The method can also be easily combined into current mobility control protocols without raising much additional overhead. The performance simulation and analysis showed that, with the sink node well-protected, mobility control protocols achieve similar performance as original protocols.

[33] presented a method that involves dividing the entire sensor network into various levels. That is each node in the network acts according to its position and status. Two routing techniques, static multi-hop routing (SMR) and dynamic multi-hop routing (DMR), were developed for routing the data between levels. These techniques employed two types of data routing namely, intra-cluster data routing and inter-cluster data routing. Simulation results presented revealed that the proposed routing protocol increased sensor network lifetime, provided improve stability and increased the network throughput compared with the Low Energy Adaptive Clustering Hierarchy (LEACH), Improved Multi-Hop LEACH (IMHT-LEACH) and Enhancing Dynamic Multi-Hop LEACH (EDMHT-LEACH) protocols. Furthermore, the DMR technique provided better performance than the SMR technique. The structure of a WSN employing the proposed scheme is shown in Figure 9.

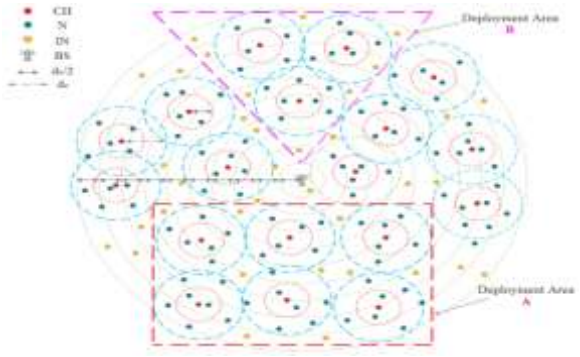

Figure 9: Topology of a WSN employing the proposed routing scheme

[34] used an Energy Efficient Unequal Clustering Routing (EEUCR) algorithm The technique involves the division of the network into a number of rings with unequal size and with each further split into a number of clusters such that rings closer to the BS has smaller area than those farther. Nodes with closer proximity to the BS have more energy than nodes more distant from BS. Static clustering, but with non-fixed cluster heads (CHs) that are chosen based on residual energy was used. The network architecture is shown in Figure 10.

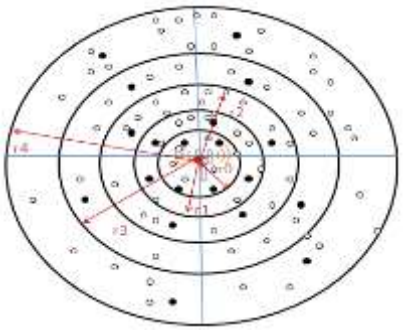

Figure 10: Architecture of network

V. CONCLUSION

Wireless Sensor Network (WSN) can be applied for a variety of purposes such as security services in military and police operations, civilian and commercial services. This paper has presented review of literature related to this work. Wireless sensor network privacy was first considered. This is followed by energy conversation in WSN. Then security requirement and potential attacks in WSN was considered. Finally a review of previous work was presented. It was observed from the reviewed works studied that most of the previous works focused either on energy efficiency of WSN or on the sink

node privacy using different techniques. In this work, the two most important aspect of WSN have been studied which include: sink node privacy and energy efficiency of WSN and applied to a security outfit. In the work done by [35] presented energy efficient analysis of a heterogeneous Wireless Sensor Network that can be applied in a varieties of purposes such as security services in Military, police operations, also in civilian and commercial services.

REFERENCES

[1]. Stallings, W. (2011). Data communications, Data Networks, and the Internet, Data and Computer Communications, 9th ed., Upper Saddle River, NJ: Prentice Hall.

[2]. Wu, C.-H., & Irwin, J. D. (2013). An Introduction to Information Network, Introduction to Computer Networks and Cyber Security. Boca Raton, FL: CRC Press.

[3]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A Survey on Sensor Networks, IEEE Communications Magazine, 40(8):102–114.

[4]. Chen, X., Makki, K. Yen, K., & Pissinou, N. (2009). Sensor network security: A survey, IEEE Communication Surveys and Tutorials, 11(2), 52-73.

[5]. Chai, G. Xu, M., Xu, W. & Lin, Z. (2012). Enhancing sink-location privacy in wireless sensor networks through k-anonymity, International Journal of Distributed Sensor Networks, 8(4), 1-16

[6]. Ebrahimi, Y., & Younis, M. (2011). Using Deceptive Packets to Increase Base Station Anonymity in Wireless Sensor Network, in Proc. Wireless Communications andMobile Computing Conference, 842–847.

[7]. Jian, Y., Chen, S., Zhang, Z., & Zhang, L. (2008). A novel scheme for protecting receiver's location privacy in wireless sensor networks, IEEE Transactions on Wireless Communications, 7(10), 3769-3779.

[8]. Ngai, E. C.-H. (2010). On Providing Sink Anonymity for Sensor Networks, Security and Communications Networks, John Wiley & Sons, 267-273.

[9]. Anastasi, G., Conti, M., Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey, Ad Hoc Networks, 7(3), 53-568.

[10]. Perwaiz, N., & Javed, M. Y. (2009). A study on Distributed Diffusion and Its Variants. in 12th International Conference on Computing and Information Technology, 44–49.

[11]. Intanagonwiwat, C., G. Govindan, R. & Estrin, D. (2000). Directed diffusion: s scalable and robust communication paradigm for sensor networks, Proceedings of the 6th Annual international Conference on Mobile Computing, 56-67.

[12]. Kulik, J., Heinzelman, W., & Balakrishnan, H. (2002). Negotiation-based protocols for disseminating information in wireless sensor networks, Wireless Networks, 8(2), 169-185.

[13]. Karthickraja, N. P., & Sumathy, V. A. (2010). Study of Routing Protocols and a Hybrid Routing Protocol based on Rapid Spanning Tree and Cluster Head Routing in Wireless Sensor Network, Proc. IEEE International Conference on Wireless Communications and Sensor Computing, 1–6.

[14]. Thakral, D., & Dureja, N. (2012). A Review on Security Issues in Wireless Sensor Networks, International Journal of Advanced Research in Computer Science and Software Engineering, 2(7), 26-32.

[15]. Xiao, Y. (2006). Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press.

[16]. Tanveer, Z., & Albert, Z. (2006). Security issues in wireless sensor networks, ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication, IEEE Computer Society, Washington, DC, USA.

[17]. Walters, J-P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing, 78-84.

[18]. Saraogi, M. (2004). Security in Wireless Sensor Networks, ACM SenSys, 64-69.

[19]. Ashima, S., & Ratika, S. (2007). Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks, Computer Network, 51(13)3750– 3772.

[20]. Wood, A., & Stankovic, J. (2002). Denial of service in sensor networks. Computer, 35(54), 54-62.

[21]. Raymond, D.R., & Midkiff, S. F. (2008). Denial-of Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing, 7, 67-75.

[22]. Singh, G. (2016). Security Attacks and Defense Mechanisms in Wireless Sensor Network: A Survey, International Journal of Innovative Science, Engineering & Technology, 3(4), 129-136.

[23]. Veeramallu, B., Sahitya, S., & LavanyaSusanna, Ch. (2013). Confidentiality in wireless sensor networks, International Journal of Soft Computing and Engineering, 2(6), 471-474.

[24]. Jan, N., Al-Bayatti, A. H., Alalwan, N., & Alzahrani, A. I. (2019). An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP), Sensors, 19(2050), 1-22.

[25]. Kumar, S.A., Ilango, P., & Dinesh, G.H. (2016). A Modified LEACH Protocol for Increasing Lifetime of the Wireless Sensor Network, Cybernetics and Information Technologies, 16(3), 154-164. DOI: 10.1515/cait-2016-0040.

[26]. Ez-zazi, I., Arioua, M., & El Oualkadi, A. (2017). On The Design of Coding Framework for Energy Efficient and Reliable Multi-Hop Sensor Networks, The 8th International Conference on Ambient Systems, Networks and Technologies,Procedia Computer Science 109C (2017),537–544.

[27]. Shao, X., Wang, C., & Gao, J. (2018). Research on Network Coding Aware Energy Efficient Routing for Wireless Sensor Networks, EURASIP Journal on Wireless Communications and Networking, 2018(231), 1-31. doi.org/10.1186/s13638-018-1245-8.

[28]. Ghaffari, A. (2014). An Energy Efficient Routing Protocol for Wireless Sensor Networks using A-star Algorithm, Journal of Applied Research and Technology, 12, 815-822.

[29]. Liu, Y., Wu, Q., Zhao, T. Tie, Y., Bai, F., & Jin, M. (2019). An Improved Energy-Efficient Routing Protocol for Wireless Sensor Networks, Sensors, 19 (4579), 1-20. doi:10.3390/s19204579.

[30]. Kishore, K. V. K., Kumar, P. S., Venketasulu, D. (2018). Privacy preservation of sink node location in wireless sensor network using RFSN-RSA, Advances in Modelling and Analysis B, 61(2). 57-63.

[31]. Mutalemwa, L., & Shin, S. (2019). Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing, Sensor, 19(1037), 1-19.

[32]. Gu, Q., Chen, X., Jiang, Z. & Wu, J. (2009). Sink-Anonymity Mobility Control in Wireless Sensor Networks, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 36-41. DOI 10.1109/WiMob.2009.16.

[33]. Alnawafa, E., & Marghescu, I. (2018). New energy efficient multi-hop routing techniques for wireless sensor networks: Static and dynamic techniques.

[34]. Handa, P., Panag, T. S., & Sohi, B. S. (2019). Enhancing packet delivery ratio and lifetime of wireless sensor networks using energy-efficient unequal clustering routing algorithm. International Journal of Innovative Technology and Exploring Engineering, 8(12), 376 – 382.

[35]. D. O. Njoku, F. U. Madu, C.G. Onukwugha, I.A. Amaefule and J.E. Jibiri(2021)"Energy Efficient Analysis of Heterogeneous Wireless Sensor Network Journal of Scientific and Engineering Research, 8(6):55-63 ISSN: 2394-2630, CODEN (USA): JSERBR