Review Techniques in Energy Conservation and Sink Node Privacy Preservation in Wireless Sensor Networks

Nwokonkwo, O.C.[1], Ofeogbu, C.I.[2], Njoku, O. A.[3], Madu, F.U.[4], Okeahialam, T.C.[5], Ikwuazom, C. T.[6]

[1]*Department of Information Technology, Federal University of Technology, Owerri, Imo State- Nigeria*
[2,3]*Department of Computer Science, Federal University of Technology, Owerri, Imo State- Nigeria*
[4]*Department of Computer Science, Federal Polytechnic, Nekede, Owerri-Imo State*
[5,6]*Department of Information Media Technology, Federal University of Technology, Minna, Niger State- Nigeria*

***Abstract*: Wireless sensor networks are applied in different fields of human endeavor such as security services in military and police operations, civilian and commercial purposes. Their use is of increasing demand in the global society recently as the need for data gathering to solve big data problem is on the rise. Today, Internet of Things (IoT) is the technology being used to provide seamless remote operations in all fields using sensors that are wirelessly networked. Hence, considering the amount of that passing through these networks and the security required of them to ensure that privacy of data is concealed and secured; the need for providing adequate protection for WSNs while ensuring prolong operation by increasing their life span by ensuring energy saving capacity becomes very paramount. This paper has carried out empirical review of implemented techniques for energy preservation and privacy provision in WSNs.**

***Keywords:* Energy conservation, Sink node privacy, Security, WSN**

I. INTRODUCTION

Since wireless sensor networks (WSNs) technology are been widely deployed for use in both military and commercial applications and requires adequate to be used to gather intelligence and confidential data regarding the environment where they are deployed, this study is prompted from a security point of view in that, because these networks are remotely installed, and as such are vulnerable to malicious attack or penetration. 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.

Several studies have been carried out in this area in recent times to implement techniques that will aid and enable sink node or base station (BS) to be hidden or made obscure from potential attack. These algorithms developed are mainly designed to protect the base station from malicious attack from foreign agent or authorize person that may try to gain access into such WSN infrastructure without permission. This is because the function of the sink node makes it a high source of attack. This potent great danger for such operation like military intelligence gathering that requires high level of security. Njoku et al. [21] work centred on energy efficient analysis for heterogonous WSN stated that every sensor node in a WSN arrangement has a predetermined amount of energy and a power subsystem is always used to power the sensor.

In this paper, a review of various studies that have implemented different strategy for sink node privacy and energy preservation in WSN is presented. The empirical studies are critical examined for works carried out not more than a decade.

II. THE NEED FOR SECURITY IN WSN

Wireless sensor networks may be deployed to carry out information in areas that may not be easily accessible or required high level of intelligence thereby making them vulnerable to potential attack. The security requirements of a typical WSN are outline as follows.

- *Authenticity and Integrity:* The data passing through a WSN can have its originality and uniqueness altered including the data authentication and the sender. These are important requirements for WSN security. The reliability of originality of the sender is provided by source authentication. Data authentication guarantees the receiver that the data has not been changed at some point in the transmission [1].

- *Data Confidentiality:* In military or security services and other commercial applications, data confidentiality is most important requirement in the deployment of WSN. Encryption of data is the normal strategy that prevents malicious attacker to gain access to network infrastructure. This prevention of an authorize user intrusion in the WSN results in data confidentiality.
- *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 [1]. In the course of implementing the security policies in WSN, the unnecessary computations and hence the battery power must be taken into consideration.
- *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 [2]. 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 [1].

III. POTENTIAL ATTACKS A WSN CAN FACE

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

- *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 [1].
- *Network availability attack:* Attacks on network availability are usually referred to as denial-of-service (DoS) attacks. Any layer of a sensor networkmay be targeted by DoS attacks [1].
- *WSN physical attack:* In this attack, full control over some sensor nodes through direct physical access is gained by attackers [3]. 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.
- *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 [4]. Transmission and reception of data between varieties of nodes of the WSN brings about the radio interference and jamming.
- *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.
- *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 [1].
- *Denial of service attack by collision generation:* Collision is generated to weaken the sensor node's energy. In a bid to generatecollision, 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 [1, 2]. As a resultof this attack, the receivers is not able to receive the message correctly.
- *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 [5]. 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.
- *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 [1]. Sinkhole attack is also known as black holes attack. Black hole attack impacts on different parameters of WSN like energy, delay and others.
- *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 [1].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 [6].

- *WSN transport layer attack:* In network layer end to end connections are managed.
- *WSN flooding attack:* According to Wood and Stankovic [7] and Raymond and Midkiff [8] 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 [1].

IV. Implementation

Singh [9] 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.

Veeramallu et al. [10] 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.

Jan et al. [11] 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 Fig. 1 and it was assumed that all the sensor nodes are evenly distributed in the surveillance area.

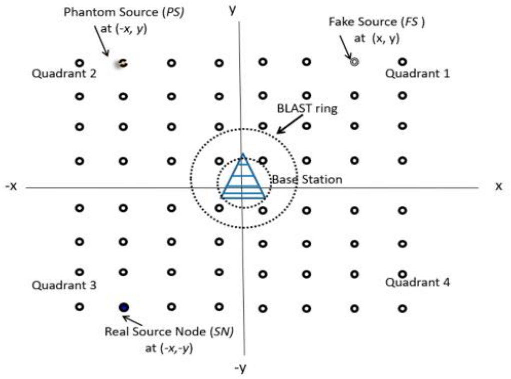


Fig. 1 Proposed model configuration [11]

Kumar et al. [12] 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 2 is a flowchart showing the comparative study of different LEACH algorithm and its types.

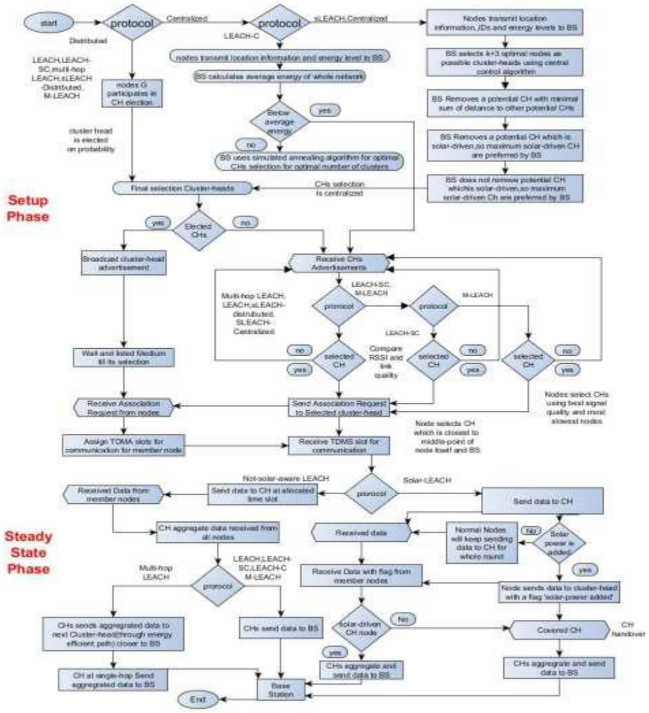

start
protocol
Centralized
Distributed
LEACH,LEACH-SC,multi-hop LEACH,sLEACH-Distributed, M-LEACH
nodes G participates in CH election
cluster head is elected on probability
protocol
sLEACH,Centralized
LEACH-C
nodes transmit location information and energy level to BS
BS calculates average energy of whole network
Below average energy
yes
no
BS uses simulated annealing algorithm for optimal CHs selection for optimal number of clusters
Nodes transmit location information, IDs and energy levels to BS
BS selects k+3 optimal nodes as possible cluster-heads using central control algorithm
BS Removes a potential CH with minimal sum of distance to other potential CHs
BS Removes a potential CH which is solar-driven,so maximum solar-driven CH are preferred by BS
BS does not remove potential CH whichis solar-driven,so maximum solar-driven Ch are preferred by BS
CHs selection is centralized
Final selection Cluster-heads
Setup Phase
Elected CHs
yes
no
Broadcast cluster-head advertisement
Receive CHs Advertisements
Multi-hop LEACH, LEACH,sLEACH-distrubuted, SLEACH-Centralized
LEACH-SC, M-LEACH
protocol
protocol
M-LEACH
LEACH-SC
selected CH
Compare RSSI and link quality
selected CH
selected CH
no
yes
Nodes select CHs using best signal quality and most slowest nodes
Node selects CH which is closest to middle-point of node itself and BS
Wait and listed Medium till its selection
Receive Association Request from nodes
Send Association Request to Selected cluster-head
Assign TDMA slots for communication for member node
Receive TDMS slot for communication
Not-solar-aware LEACH
protocol
Solar-LEACH
Received Data from member nodes
Send data to CH at allocated time slot
Send data to CH
CH aggregate data received from all nodes
Received data
Normal Nodes will keep sending data to CH for whole round
No
Solar power is added
yes
Steady State Phase
Multi-hop LEACH
LEACH,LEACH-SC,LEACH-C M-LEACH
protocol
Receive Data with flag from member nodes
Node sends data to cluster-head with a flag 'solar-power added'
CHs sends aggregrated data to next Cluster-head(through energy efficient path) closer to BS
CHs send data to BS
solar-driven CH node
No
Covered CH
CH handover
yes
CHs aggregate and send data to BS
CHs aggregrate and send data to BS
CH at single-hop Send aggregrated data to BS
Base Station
End

Fig. 2 Flowchart of LEACH protocol and its types [12]

Ez-zazi et al. [13] 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 Fig. 3.

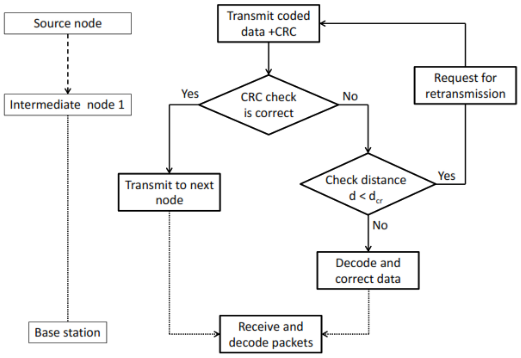


Fig. 3 Adaptive coding algorithm [13]

Shao et al. [14] 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 Fig. 4.

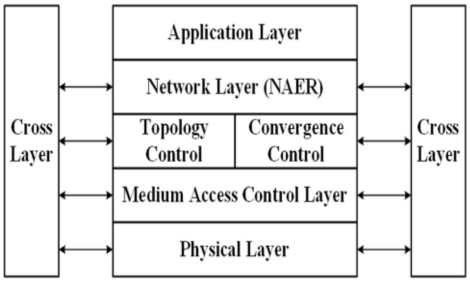


Fig. 4 cross layer interaction principle of NAER coding scheme [14]

Ghaffari [15] 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.

Liu et al. [16] 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 Fig. 5.

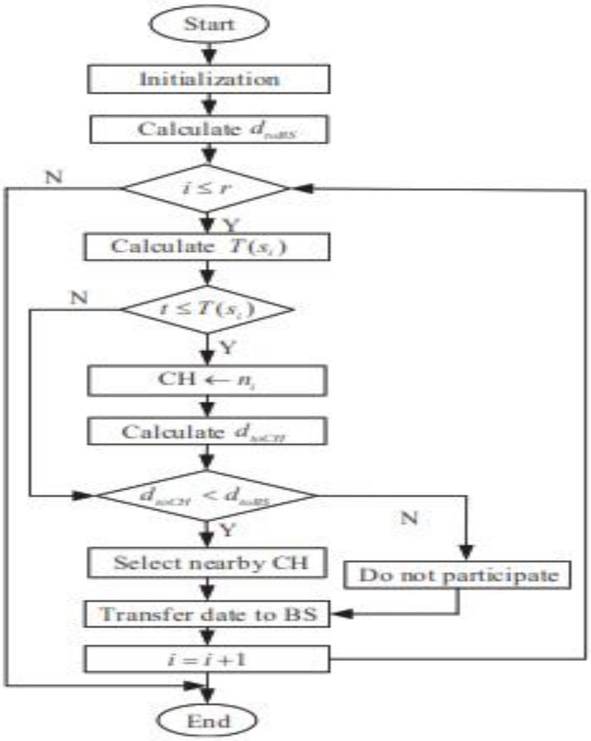
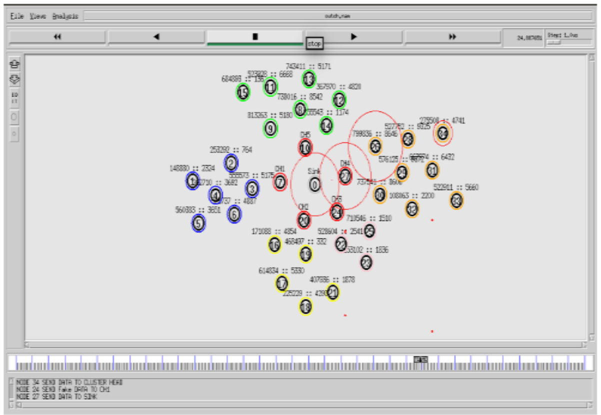


Fig. 5 Flowchart of proposed protocol [16]

Chai et al. [17] 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.

Kishore et al. [18] 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 Fig. 6



```
NODE 34 SEND DATA TO CLUSTER HEAD
NODE 24 SEND Fake DATA TO CH1
NODE 27 SEND DATA TO SINK
```

Fig. 6 Sink node model simulated NS2 simulator [18]

Mutalemwa and Shin [19] 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. Figure 7 is an illustration of the packet routing technique using the proposed proxy node routing scheme.

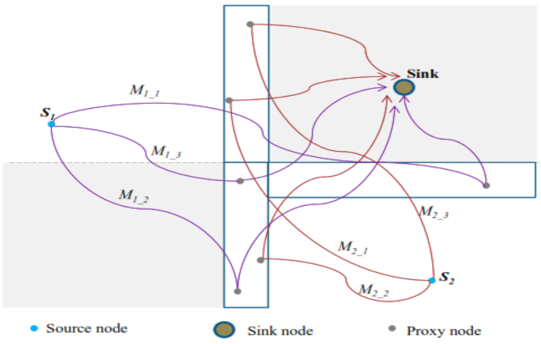


Fig. 7 Proxy node routing scheme [19]

Gu et al. [20] 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.

V. CONCLUSION

This paper has presented a review of literatures that are related to energy efficiency and sink node privacy. The paper also reviews and considered security requirement and potential attacks in wireless sensor networks (WSNs). Finally, a review of implemented strategies was presented and 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 paper, the two most important aspect of WSN have been studied which include: sink node privacy and energy efficiency of WSN.

REFERENCES

[1] 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

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

[3] 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, 40.

[4] 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.

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

[6] Ashima, S., & Sachdeva, R. (2013). Review on security issues and attacks in wireless sensor network, International of Advanced Research in Computer Science and Software Engineering, 3(4). 56-59.

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

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

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

[21] Njoku, D. O. Madu, F.U. Onukwugha, G.C, Amaefule, I. A. & Jibiri, J.E.(2021) "Energy Efficient Analysis of a Heterogeneous Wireless Sensor Network" Jo*urnal of Scientific and Engineering Research*, 8(6):55-63