Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2021, 8(8):126-134

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Sink Node Privacy Preservation for Wireless Sensor Network Security

Chinemelu, C., Akpoilih, O. E.

Department of Electrical & Electronic Engineering, Petroleum Training Institute Effurun, PMB 20, Delta State, Nigeria

Abstract This paper has presented sink node privacy preservation for Wireless Sensor Network (WSN) security. As a form of distributed network, a WSN aids the gathering of information in wireless communication within an area of interest. A WSN topology model and algorithm was developed and implemented in MATLAB. Simulations were conducted in MATLAB environment to analyze the effectiveness of the developed algorithm in concealing the location of the sink node in the WSN while ensuring that energy consumed by a node is minimized. The simulation result revealed that the anonymity factor varied with number of simulation trials and across the various simulated messages or traffic volumes. However, the result of the anonymity factor eventually did not depend on the messages. The range of number of nodes broadcast to by the broadcast cluster heads was from 20 to 30.A remarkable consistency was observed from the result obtained in the sense that the value of the anonymity factor of the sink node in the WSN for each simulation trial was within 0.04 and this value was in conformity with the average value of the anonymity factor obtained in terms of the probability plot for normal distribution, which was also 0.04 and this confirmed the consistency of the results. With sink node anonymity factor of 0.04, this simply means that the average anonymity factor indicated that an attacker or an adversary carrying out traffic analysis to steal from or compromise deployed WSN will have less than 4% possibility of locating the sink node.

Keywords Anonymity factor, Privacy preservation, Sink node, WSN

Introduction

A significant characteristic of Wireless Sensor Network (WSN) security is the capability to shield the sink node. The sink node is essential for collecting, summing and conveying information of sensor. From the point of view of security applications, once sensors gather information, the sink node is the central controller where this data is sent. As a result of this, the provision of critical information to persons about the operation and security of WSN depends on the sink node. In view of the fact that the sink node is a fundamental point of failure, an illegitimate person can demolish the sink and make the data gathering tasks of the whole sensor network ineffective. Therefore, failure to shield the network entirely undermines the anticipated purpose of sensor network applications [1]. It is imperative therefore to apply specific protocols that hide the location of the sink node.

Considering the fact that wireless sensor networks (WSNs) are remotely deployed, and as such are vulnerable to malicious attack. The increasing capacities of WSNs have also resulted to increasing potential threat from any attacker. This requires some tactics modification, methods and steps used for the strategic application of WSNs. Wireless Sensor Network deployed for secured application faces basically two challenges, which are limited power of battery of each sensor node and the privacy of the sink node. Since the function of the sink node in WSN makes it high source of target for attack, sink node privacy is important to the safety of WSN put into use for strategic application. Another crucial parameter for realizing sink node privacy is energy efficiency of the node. This is because the energy of nodes in sensor network ensures that reliable communication among nodes is achieved with less cost when properly managed.

(a) 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 [2]. 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 structural design that describes the functionality of the network is divided into layers that jointly form the network protocol stack [3]. Every one of the layers 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 [4].

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 [5]. 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 [6].

- Source 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.
- Sink node techniques: This involves the use of approaches such as *deceptive packets protocol*, which 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. 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 [7]. The purpose of using deceptive packets is to make the belief values of other nodes similar to or higher than the sink node. The Belief is a value which represents the confidence of the attacker that the destination node is the sink node [7]. The drawback of the deceptive packet method is that its performance is extremely variable. *Location privacy routing (LPR) protocol,* in this scheme, every one of the sensors 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 [8]. 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 [8]. One way to address this problem is to integrate LPR with fake packet injection similar to deceptive packets. *k-anonymity protocol*, in which case the objective 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 messages are uniformly 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 [6]. 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 [6]. This is actually an optimization problem which involves prioritizing one objective or the other. *Randomized routing with hidden address* is a scheme designed to 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 [9]. The major limitation of RRHA is that it cannot assure that the sink will receive the data.

(b) Summary of Previous Studies

Singh [10] 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. Using the sensor network Encryption Protocol (SNEP), Veeramallu et al. [11] 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. Primarily, two security properties were checked, which were authenticity and confidentiality of similar messages components. Jan et al. [12] 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. In order to protect the sink-location privacy from a powerful adversary with a large-scale view, the Chai et al. [6] 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. 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. [13] 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. Mutalemwa and Shin [14] 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. Gu et al. [15] 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.

Materials and Methods

In this paper, the privacy of sink node in WSN is considered. In order to safeguard the sink node and at the same time improve the energy efficiency of the network, a randomly distributed sensor nodes configuration over sink node is proposed. The proposed system is represented by the block diagram in Figure 1.

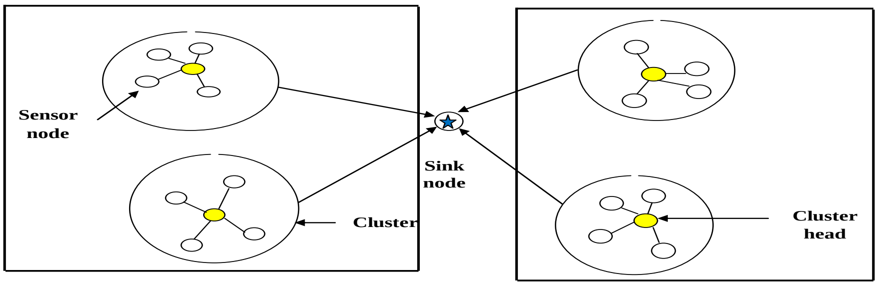

Figure 1: Block diagram of propose WSN

(a) Modeling of Threat

The sink node is the aggregating point for data collection within WSN. In targeting the physical location of sink an adversary can attack it and as such can effectively utilize the WSN to collect intelligence and plan operations. The capabilities of the adversary impact on way or manner that is chosen to protect the network and calculate the success of the proposed algorithm. Hence, for this purpose, following capabilities are assumed.

- The attacker is assumed to have ability to view all traffic on the WSN.
- Interference to the normal communications of the WSN is not of concern to the attacker. Traffic analysis will be carried out by attacker, who only deduce the monitored objects' location and sink node using information such as transmission time of packet and frequency [6].
- The attacker is unaware of or does not to possess encryption key.

(b) Cluster based Routing for Achieving Privacy

In order to achieve energy-controlled sink node privacy, a node clustering routing algorithm that results in *n* order nodes that have related observable traffic statistics and therefore confusing the location of the sink node is proposed. The procedures that the WSN takes when put into operation to route traffic are as follows: Cluster Head (CH) election and cluster formation, and select a subset of the CHs to function as broadcast CHs. The clustering technique is shown in Figure 2.

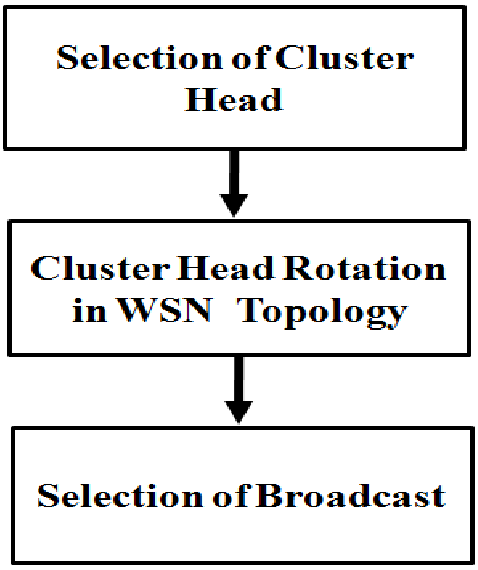
Selection of Cluster Head
Cluster Head Rotation in WSN Topology
Selection of Broadcast

Figure 2: Clustering technique procedures

(c) Sink Node Privacy

The purpose of developing this algorithm is to make sure that at least s other nodes in the wireless sensor network (WSN) have identical traffic data as the sink node. Let S be the set of all nodes in the WSN and let the total number of nodes denoted by i. In this work, $i = 100$ nodes; therefore:

$$S = \{s_1, s_2, \cdots, s_i\} \quad (1)$$

Cluster Head (CH) is the set of nodes that functions just like CHs. The sum of CHs is denoted by j and is given by:

$$CH = \{ch_1, ch_2, \cdots, ch_j\} \quad (2)$$

Let the set of the nodes that serve as cluster members be represented by CM. The sum of the number of cluster members is represented by k:

$$CM = \{cm_1, cm_2, \cdots cm_k\} \quad (3)$$

After the final iteration of CH selection, all nodes in the network are either CHs or cluster members CM. Representing this expression using set notation gives:

$$S \equiv CH \cup CM \quad (4)$$

Such that

$$i = j + k \quad (5)$$

Each s_i in S becomes a component of CH or CM :

$$s_i = ch_i \in CH \text{ or } s_i = cm_i \in CM \quad (6)$$

The set CH is then ordered by the residual energy within every node:

$$CH_{RE} = \{ch_{re1}, ch_{re2}, \cdots, ch_{rej}\} \quad (7)$$

The set of nodes that serves as broadcast cluster heads (CHs) is denoted by BCH and is a subset of the cluster head. Therefore, the sum of the broadcast CHs is represented by l :

$$BCH = \{bc_1, bc_2, \cdots, bc_l\} \quad (8)$$

where $BCH \subseteq CH$.

Every broadcast CH is chosen or selected in based on the maximum energy remaining: $bc_1 = ch_{re1}, bc_2 = ch_{re2}$ and so on. A broadcast cluster head transmits any data it receives to all of its cluster members (CM) as well as to the next hop CH. The overall number of nodes broadcast to is represented by α:

$$\alpha = \sum_{i=1}^{l} CM(bc_i) \quad (9)$$

The anonymity factor (that is factor that determines privacy) of the sink node is represented by PF and is given by:

$$PF = \frac{1}{\alpha} \quad (10)$$

There is always a change in the number of CM that belongs to each broadcast CH at any time the cluster heads are rotated. In order to calculate the PF, the average value of the cluster members broadcast is taken across the simulation expressed as:

$$PF = \frac{1}{average(\alpha)} \quad (11)$$

(d) Simulation Parameter and Flow Diagram

The values of the parameters used for simulation in MATLAB are shown in Table 1.

Table 1: Simulation parameters

Parameter	Value
No of sensors	100
Area	100m by 100m square
Sink node coordinate	(x,y) = (25m, 75m)
Probability of node to becoming a CH (P_{opt})	20%
Transmit power	5.0×10^{-9}W
Receive power	5.0×10^{-9}W
Processing power	5.0×10^{-9}W
Initial Energy of sink node	2.0 J
Initial Energy of Each node	2.0 J
Traffic generation messages	5,000 to 20,000
No of threshold nodes	20

Results & Discussion

This section presents the outcome of the simulations carried out in MATLAB Simulink environment. In the simulation carried out in this paper for wireless sensor network (WSN) sink node anonymity, each sensor in the network can elect or choose to become a cluster head (CH) with a given probability p when network is set up. However, there is no optimal number of CHs for a WSN. In this work, the probability of a sensor node to become a CH was taken from 0.1 to 0.5. This was demonstrated by carrying out simulation to determine which value will ensure optimal performance with most of the CHs selected. Having obtained the probability that offered the most promising performance to be 0.2; further simulation was conducted for different generated traffic (5000 to 20000) to determine the sink node privacy preservation performance.

The privacy of the sink node which is called anonymity of the sink is presented in this section. The anonymity factor is determined in terms of the number of nodes broadcast to as stated in Equation (9). The results obtained in terms of four simulation trials conducted for the various messages are presented in Tables 2 and 3 and their simulation plots including the probability plot for validating the anonymity factor that will give the most desired security to sink node are shown in Figures 3 and 5.

Table 2: Total number of nodes broadcast to for each simulation trial and messages

Messages	Total number of nodes broadcast to with respect to the number of simulation trials				
	1	2	3	4	Average
5000	21.000	21.000	20.000	23.000	21.250
10000	20.000	29.000	20.000	26.000	23.750
15000	24.000	21.000	23.000	22.000	22.500
20000	25.000	25.000	30.000	26.000	26.500

Table 3: Total number of nodes broadcast to and anonymity factor for each simulation trial and messages

Messages	Average number of nodes broadcast to	Anonymity factor
5000	21.250	0.047
10000	23.750	0.042
15000	22.500	0.044
20000	26.500	0.038

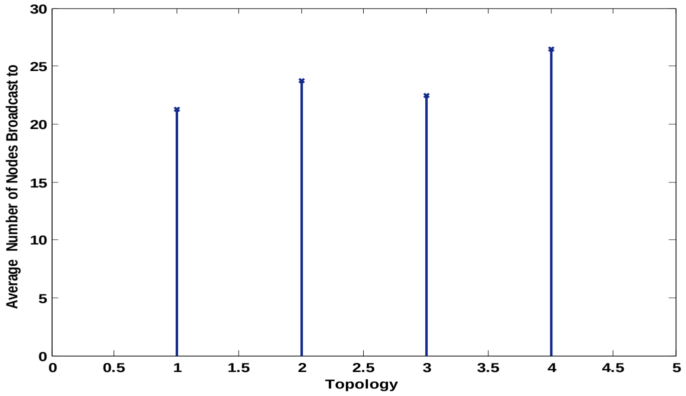

Figure 3: Average number of nodes broadcast to for all four simulation trials

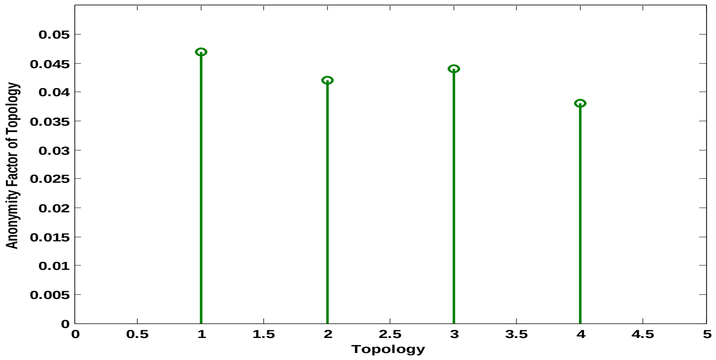

Figure 4: Anonymity factor for all four simulation trials

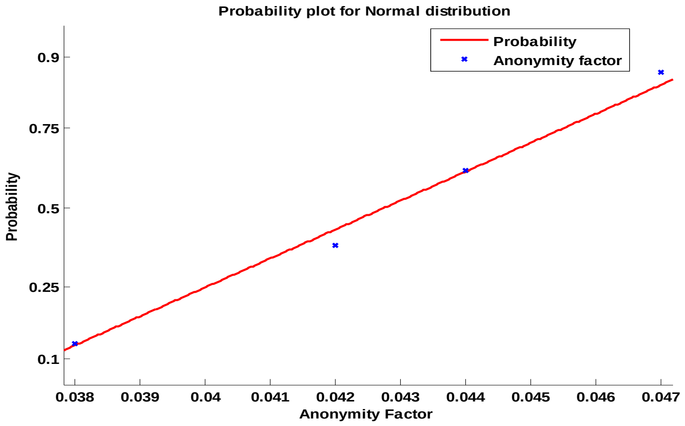

Figure 5: Probability plot for normal distribution of anonymity factor

A general look at the results obtained revealed variation in terms of the messages and does not show any trend of convergence to a number of nodes broadcast to or divergence from a number of nodes broadcast to as messages increase as shown in Figure 3. In the same way, there is no trend in convergence or divergence in the anonymity factor over the different messages as shown Figure 4. A look at Table 2 shows that the number of nodes broadcast to ranges from 20 to 30 and this surpasses the lower threshold of 20 nodes. Furthermore, a critical look at Figure 3 reveals a slight increase in the average number of nodes broadcast to with increase in messages (that is traffic volume). This slight increase in number of nodes broadcast to as messages increases invariably translates into a small decrease in the anonymity factor as messages increase in the WSN topology as shown in Figure 4.

In order to validate the sink node privacy, the result obtained for anonymity factor was further analysed using probability plot for normal distribution (of the MATLAB software) to ascertain which of the values of the anonymity factor actually provide the most accurate sink node privacy as shown in Figure 5. A look at Figure 5 indicated that out of the four values of the anonymity factor obtained, two of the values (0.038 and 0.044) fall in the straight line curve of the distribution while the other two (0.042 and 0.047) fall off the line. Thus, the two values that fall in the line are taken as the best fit and their average (that is 0.04) was chosen to represent the value of the anonymity factor of the WSN algorithm developed in this paper.

Therefore, the simulation results discussed so far have revealed that variation exists for four simulation trials conducted with respect to the traffic volume across the WSN topology. There is remarkable consistency in the results obtained. For instance, the value of the anonymity factor of the sink node in the WSN for each simulation trial is within 0.04 and this value is in conformity with the average value of the anonymity factor obtained in terms of the probability plot for normal distribution, which is also 0.04 and this confirms the consistency of the results. Also, what this means is that for any given simulation trial of the WSN topology; it can be said that for a hacker or an attacker carrying out traffic analysis of the developed network, it will have a probability of less than 4% of finding the sink node on his first attempt at any time he is searching for the sink node sensor.

Conclusion

A model and routing algorithm has been developed for sink node privacy preservation in Wireless Sensor Network (WSN) security. The developed topology and routing algorithm for WSN was validated through simulation experiments conducted in MATLAB. A remarkable consistency was observed from the result obtained in the sense that the value of the anonymity factor of the sink node in the WSN for each simulation trial was within 0.04 and this value was in conformity with the average value of the anonymity factor obtained in terms of the probability plot for normal distribution, which was also 0.04 and this confirmed the consistency of the results. A crucial parameter for realizing sink node privacy is energy efficiency of the node. This is because the energy of nodes in sensor networks ensures that reliable communication among nodes is achieved with less cost when properly managed. In order to enhance the security of the network, an algorithm that is capable of hiding the location of the sink node must be implemented while ensuring efficient energy management. However, in this study, the performance of WSN was only analysed in terms of sink node privacy.

References

[1]. Mehta, K., Liu, D., & Wright, M. (2012). Protecting Location Privacy in Sensor Networks against a Global Eavesdropper, *IEEE Transactions on Mobile Computing*, 11(2), 320–336.

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

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

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

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

[6]. 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

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

[8]. 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

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

[10]. 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.

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

[12]. 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.

[13]. 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.

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

[15]. 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.