# Multiple Techniques To Preserve Location Privacy of Sink in WSN

Venu H.D.[a],Chinnaswamy C.N.[b]

[a]*PG Student,National Institue of Engineering,Mysuru,India*
[b]*Associate Professor,National Institute of Engineering,Mysuru,India*

**Abstract**

Wireless Sensor Networks (WSN) are getting to be essential subject in research zone in view of its applications in critical regions like military, human services, savvy homes ,ecological observing and so forth., WSN is made out of a great many modest sensor nodes which are having the capacity of sensing, processing and communication. These sensors are having minimal effort on account of its low memory ,low calculation power, limited scope of correspondence capacity. In a large portion of the WSN applications, sensors are left unattended so security in these applications are vital in light of the fact that gate crasher may harm the sensor and get the critical information in order to do suspicious activities. One of the attack is Sink hole attack where foe or assailant tries to draw sensed data with the mean to counteract base station or sink node from accepting a total sensing information from nodes. Henceforth, attacker gets entire detected data from system and accomplish its objective. Along these lines, to overcome from this assault we need to track these sort of assaulted nodes in the system furthermore attempt to sidestep this in future. In this paper, we are proposing three techniques like Ring based technique, Random walk of sink and Multi sink approaches to hide the location of sink from attacker. Simulation results demonstrate these three techniques, Simulation is carried out using simulator NS3.

*Keywords*: Wireless Sensor Networks(WSN), Base Station (BS) , Base station Location Anonymity and Security Technique(BLAST), Sink location Privacy Preserving Protocol(SLPRP),Software Defined Networking(SDN)

## 1. INTRODUCTION

Wireless Sensor network comprises of an arrangement of topographically dispersed sensor nodes, which constantly screen their environment and forward the detecting information to a base station through multi-hop routing. These systems utilize radio communication as a media for transmission which make them powerless to various sorts of attacks. We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en masse to monitor and affect the environment. Sensor networks often have one or more points of centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. In some previous work on sensor network routing protocols, base stations have also been referred to as sinks.

Base stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop class processors, memory and storage, AC power, and high bandwidth links for communication amongst themselves. However, sensors are constrained to use lower-power, lower bandwidth, shorter-range radios, and so it is envisioned that the sensor nodes would form a multi-hop wireless network to allow sensors to communicate to the nearest base station. A base station might request a steady stream of data, such as a sensor reading every second, from nodes able to satisfy a query. We refer to such a stream as a data flow and to the nodes sending the data as sources.

Since the base station forms the bridge between the sensor and the user, a complete sensor network or a part of it can be rendered useless if the base station or the sink node is taken down. This situation makes the base very sensitive and creates a single point of failure, thereby making it a priority when it comes to protecting location privacy. We focus on protecting the base station in this paper. Energy being a primary concern in WSNs, it is important to take care of the energy consumption while devising a method to protect the privacy. We also need to keep the delay as low as possible to make sure that the data is still useful when it reaches the base station.

Sinkhole attack [1] is considered as one of the serious assaults that is propelled by a compromised node to occupy the system activity far from the intended activity, Through this system sinkhole node endeavours to attract all system movement to itself. From that point it modifies the data packets or drops the packets noiselessly and finally decimate the system. A sinkhole assault causes a genuine risk to sensor systems.

Sinkhole assaults (see Fig. 1) commonly work by making a malicious node look particularly attractive to neighbour nodes regarding the routing algorithm. Due to either the genuine or envisioned good quality route through the malicious node, it is likely each neighbouring node of the foe will forward data packets for a sink through the foe, furthermore propagates the engaging quality of the route to its neighbours. Viably, the enemy makes a extensive "effective reach", pulling in all traffics bound for a sink from hubs a few hops far from the malicious node. So all the sensed data are collected by malicious node which is under the control of attacker. He may alter or drop the data packet and may destroy the whole network.

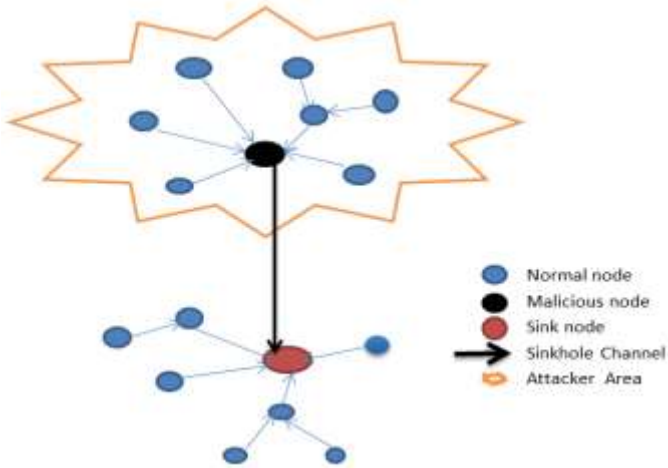


Fig. 1: Sink Hole Attack

The base station is kept by the sinkhole attack from accomplishing complete and precise sensing data, and hence it is brought about a vital risk which is basic for wireless sensor systems. Actually, this happens due to the unprotected remote connections, the organization of the sensors in open territories, what's more, the frail calculation and battery control.

Privacy in wireless sensor networks is divided into data oriented privacy and context-oriented privacy as shown in figure 2. Data oriented privacy is a privacy of the data contained in the packets. It can be provided by encryption of the data and authentication process can be applied, it can be divided into data aggregation and data query. Data aggregation may be done by computing mean, standard deviation, variance, etc. the context oriented privacy such as the location of the source or the sink can be deduced by analysing the network traffic and examining the routing function. Context-oriented privacy is classified into location privacy such as a source location and receiver location privacy and temporal privacy. Location privacy must be provided in WSNs. Here, our focal point is the sink location privacy in WSN.

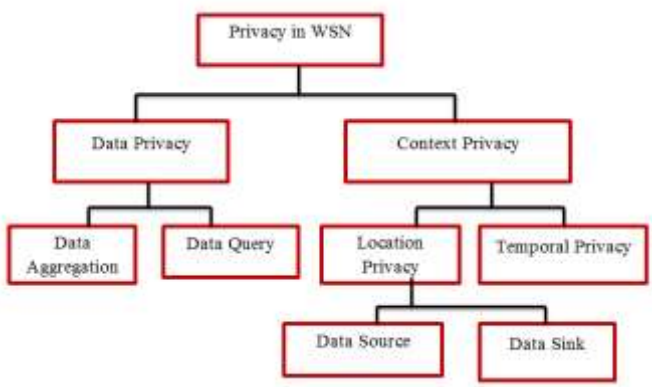


Fig 2:Classification of Privacy in WSN

The attacker can locate the sink location by using packet tracing attack and traffic analysis attack . The attacker first tries to use traffic analysis attack. An attacker locates the sink position by examining the network traffic. As neighboring nodes of sink forward, a larger volume of data compared to nodes present far away from the sink. The attacker can easily understand the presence of sink near the particular node. After that, the attacker may use packet tracing to locate the sink because it may use frequency modulation techniques to perform hop-by-hop check towards the sink. In this paper, our focus is on studying the defense measures against the traffic analysis attack.

We will first describe the attacks that could compromise the sensor location privacy.

*Attacks*

There are two kinds of attacks to compromise the location privacy or contextual privacy in a WSN: the Traffic Analysis Attack and Packet Tracing Attack . These attacks can be carried out either by a local adversary or a global adversary. A local adversary means that there is a single mobile attacker which has to move around to hear packets and interpret the direction of traffic to locate the base station. A global attacker can hear all the transmissions in the network. This is possible by deploying an adversarial network over an existing WSN through which the adversary can instantly hear the packets with minimum delay.

*Traffic Analysis*

In this type of attack, the adversary observes the traffic rate at each location. We know that, nodes nearer to the base station generate traffic at higher rates than nodes far away from the base station as they have to forward the packets from farther nodes. The adversary can take advantage of these traffic characteristics to find the physical location of the base station and compromise the network. This attack takes long time before becoming effective as the adversary needs to stay at each location and assess the traffic.

*Packet Tracing*

In this type of attack, the adversary does not wait at a location to analyze the traffic. Instead, it finds the next transmitter of the packet and moves along with it. In this way, the adversary works its way hop-by-hop from source to the base station. Thus, the adversary moves one hop with the transmission of every packet. This attack is more efficient than the Traffic Analysis attack as the adversary keeps getting closer to the base station without waiting at a particular location. The above two attacks can be implemented more quickly and effectively by a global attacker. Our technique concentrates more on the local adversary through the blast nodes. It also offers a decent level of privacy against a global attacker.

## 2.RELATED WORK

Location privacy in WSNs has gained enough interest in recent years. Methods for location privacy against local adversary are usually based on injecting fake packets, creating fake sinks, routing packets along a random path, decorrelating transmission times by choosing random timings for transmission, or a combination of these techniques. Controlling transmission rates and injecting dummy data into the network are usually used against a global attacker.

A technique that uses random walk is proposed in [2] where each node chooses with a probability P the next hop from its neighbours which are nearer to the base station and with a probability (1 − P) from those neighbours which are farther away from the base station. As the adversary can find the trend of traffic flow in this technique when there are many sources, they try to secure the network by introducing fake packets to maintain equal traffic rate throughout the network, thereby having an overhead. DEFP [3] also creates fake packets to confuse the adversary. Here, nodes generate fake packets as soon as they hear a real packet in their neighbourhood and the technique is further improvised by creating hotspots by increasing the generation rate

of fake packets in few selected areas.

Data aggregation is a technique that could maintain equal traffic rates throughout the network. A technique is proposed in that uses data aggregation to maintain equal traffic rates. But it is not possible to obtain data at a particular location for which they propose an option of operating the network without aggregation when required. But, in order to maintain the traffic rate, each node has to wait for a long time before it can send its data. This also requires injection of fake packets which consumes energy.

A technique to protect sink location privacy without delay and fake packet injection is proposed in [4]. This technique requires the source to send the packet along multiple paths and without any destination address and with a specific TTL value. This technique has a major problem of the base station not getting the packet. A technique has been introduced in [5] that protects both the source and the sink nodes. This technique uses fake sinks, fake sources and dummy packets to protect the identity of both the source and the sink. Though actual packets are routed along the shortest path, it uses resources creating fake sources and sinks and also in generating and forwarding fake packets.

The techniques that deal with global adversary concentrate on maintaining equal traffic rate throughout the network. A technique is given in [6] that collects data from the network periodically so as to maintain the same traffic rate. Since this consumes more energy, the authors propose an alternative to create fake sources that keep changing over time thereby offering a trade-off between energy and privacy. Authors of [7] and [8] proposed techniques to defend against global attacker, but only for the source protection.

In the rest of this paper, we will discuss the various techniques for location privacy of sink in WSN.

## 3.TECHNIQUES TO HIDE THE LOCATION OF SINK

### *A. Ring Based Technique*

As shown in Fig 3, first form one secure ring containing WSN nodes and sink within the network, Select one node as master node in the ring other than sink node. send the unicast packet from source node to master node. Master node broadcast this packet within the ring, it will reach all the nodes in the ring, Sink within the ring finally get the packet and attacker is not able to find out which is the sink because traffic is same in all the nodes within the ring.

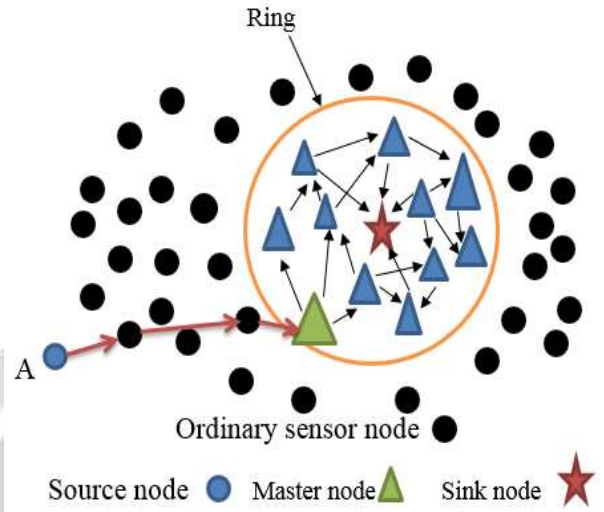


Fig.3: ring Based Technique

The network is divided into two sets of nodes, namely ordinary nodes and ring nodes. The ring nodes are in a ring or circular region. Somewhere in this region is the real base station (need not be at the centre). Each ordinary node has a transmission range of tx and each ring node has a transmission range of K × tx, where K can be any value such that the product stays under the maximum possible transmission range of the sensor. The product K × tx is set to be the diameter of the ring . A node can chose the next hop node from its neighbours based on their distance from the destination.

When a sensor node has a packet to send, it randomly routes the packet towards the sink and when it reaches one of the special nodes (it is the edge of the ring in our set up), the packet is flooded in a controlled manner. Flooding is done within the diameter of the ring. This ensures that the packet is received by the base station while still keeping its location safe. After numerous transmissions, the adversary could find all the nodes in the ring, since flooding always starts on the edge of the ring. After this, the adversary cannot make any further progress in narrowing down the scope of the region.

The sink can be anywhere within the ring. Implementing such a scheme does not require any special ring nodes in the ring. We just need a circular area of nodes marked with a specific role, such that when one of these nodes receives a packet, it will flood it with a pre-defined TTL. In the initial routing phase to the ring, a directed random path is used, where each node chooses the next hop randomly from its near hop list. The near hop list of a node consists of all its neighbours which are nearer to the base station than itself.

The Source A randomly chooses a blast node B from the ring, Then, the packet is routed from A to B through the shortest path between them. The node B now blasts the packet with a transmission range of K * tx which is the diameter of the protection ring. This covers the whole ring and also some extra nodes outside the ring. The actual base station can be located anywhere inside the ring. To the adversary, any node in the ring could be the base station.

In the initial phase of routing the packet from a source to a random blast node, we use the shortest path between them. We may use a random directed path to increase the privacy. But, since the destination is randomly chosen each time, the path is going to be different each time. Even after the adversary estimates the

presence of ring after many transmissions, it cannot go any further. We chose the shortest path to reduce the delay.

Now, a global adversary can trace the ring quicker than a local adversary as it simultaneously gets the information from all over the network. But even the global adversary cannot predict the actual location of the base station within the ring. We can defend strongly against a local adversary as it is takes a long time for it before it determines the ring of blast nodes using the traffic trend.

*B. Random Walk of Sink Technique*

As shown in Fig 4. , Source node sends the sensed data packet to intermediate nodes then Sink node at location say 1 receive the source packet. Sink will move to different location say 2 then Source node again sends the next sensed data packet to intermediate nodes and Sink node at location say 2 receive the source packet. Since Sink location is different for every packet ,it is difficult for the attacker to get the packet.

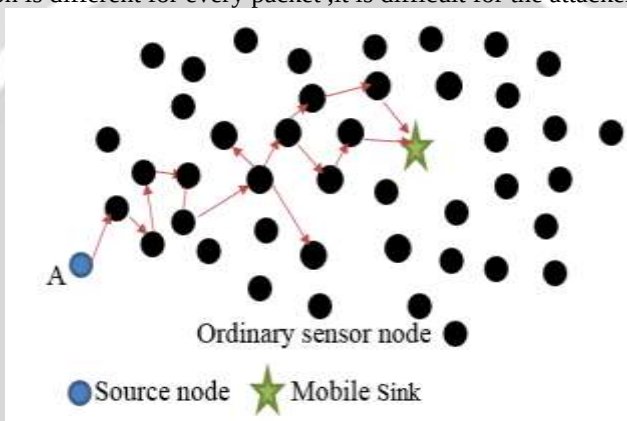


Fig.4: Random Walk of Sink Technique

*C. Multiple Sink Technique*

As shown in Fig 5 , Source node sends the sensed data packet to intermediate nodes, then create one more fake sink in the network. Source node also sends data less packet to fake sink. fake sink will get the data less packet from the source. Real sink will get real packet from the source. Now attacker is confused which is the real sink, hence achieved location privacy of sink.

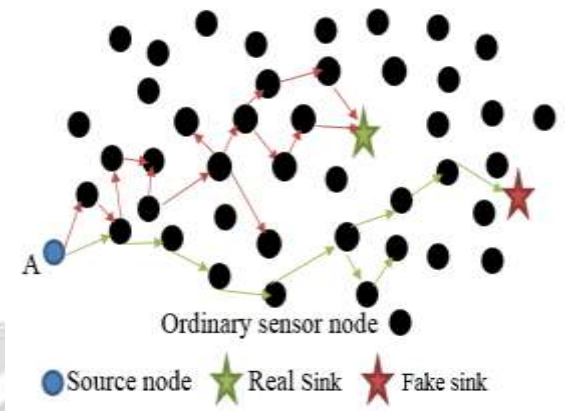


Fig.5: Multiple Sink Technique

In the first step, we are considering the network with multiple sources and sink present in the network. The routing protocol use is DSR protocol. The intermediate node or SLPRP nodes are responsible for fake packet generation. When a source wants to send the packet to the sink node, the SLPRP node generates fake packets and send it to the fake sink. The intersection nodes send fake packets for every real packet to the fake sinks. The real packets are sent using the DSR protocol so that it simply reaches the sink using shortest path. The fake packets don't contain any useful information. It can be simply used to take an adversary to the wrong path. As the adversary will be confused with a real and fake path, so the safe time will be increased.

## 4. EXPERIMENTAL RESULTS

In this section, we plan implementation framework of proposed algorithm using latest version 3.23 of NS-3

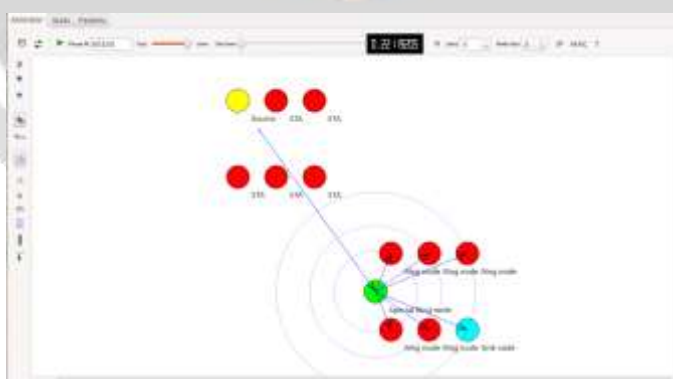

Fig.6: Ring Node Technique

Initial Network configuration in Ring technique is shown in Fig. 6, yellow color node is Source node, green is Special ring node, sky blue color node is Sink node and Red color node is other WSN nodes. first Special ring node or master node will inform all other ring nodes that I am the special ring node and you will get packets

from me only. Then Source will send unicast packet to master node, then master node will broadcast that within the ring, finally sink will receive it ,so attacker won't get the location of sink because traffic is same in all nodes in the ring.

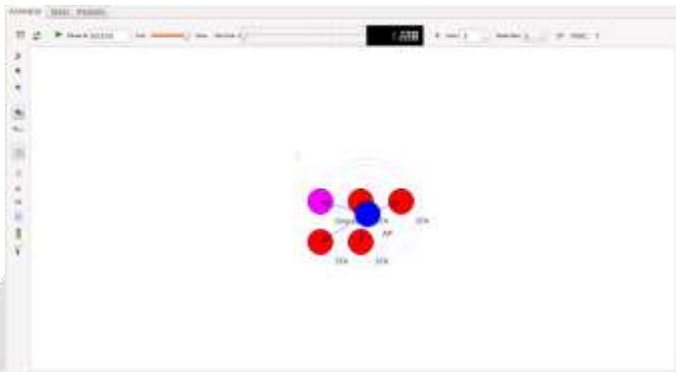

Fig.7: Random Walk Technique

Initial Network configuration in Random Walk technique is shown in Fig. 7, Pink color node is Source node, blue color node is Sink node and Red color node is other WSN nodes. Source node will broadcast the packet which is sensed in the environment to the WSN network, all nodes in the network will receive the packet including Sink. Sink node after receiving packet from source node will randomly change the location, so attacker won't get the location of sink since it is different for every packet.

Fig.8: Multi Sink Technique

Initial Network configuration in Multi sink technique is shown in Fig. 8, Pink color node is Source node, blue color node is Real Sink node, green color node is fake sink and Red color node is other WSN nodes. Source node will broadcast the packet which is sensed in the environment to the WSN network, all nodes in the network will receive the packet including Real and fake sink. Source node also send data less packet in the network, it will reach the fake sink not the real sink, real data packets will reach only real sink, since traffic is same in both sink, attacker won't get real sink easily. Random Walk mobility strategy is applied to multi sink, to strengthen the multi sink strategy.

## 5. PERFORMANCE ANALYSIS

The performance of all proposed techniques including energy, end-to-end latency and number of reported sink hole detection will be analyzed in this section.

### *A. Energy Consumption*

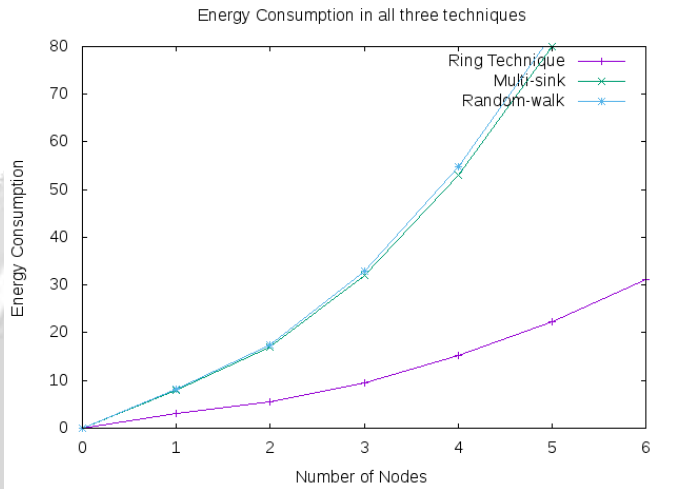


Fig.9: Energy consumption

Ring Technique has less energy consumption because broadcasting of packet is only with in the network, not with entire network as in Random Walk and Multi sink Technique which are having more energy consumption as shown in Fig 9.

### *B. end-to-end latency*

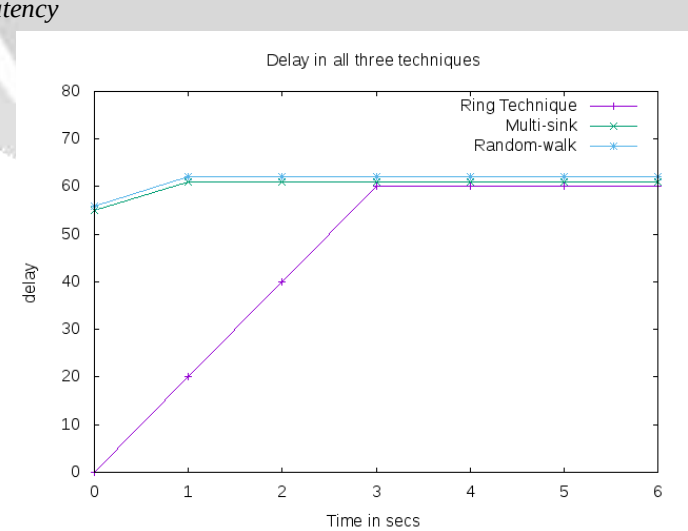


Fig.10: End-to-End latency

Ring node technique as initially more delay because it will take time to set up the ring, Random Walk and multi sink technique has less delay because there is no extra set up with in the ring.

*C. Number of reported sink hole detection*

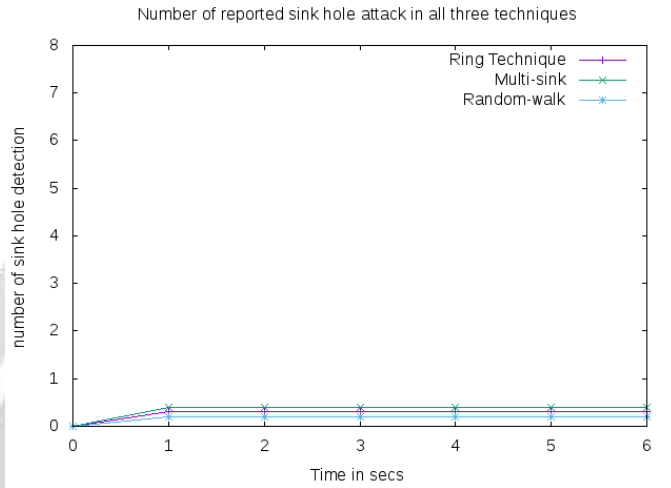


Fig.11: Number of reported sink hole detection

Random- Walk has less Sink hole detection because location is different for each packet, Multi-sink technique has more detection because probability of getting real sink in the network is possible and Ring Technique has less probability compared to multi sink.

## 6. CONCLUSION AND FUTURE ENHANCEMENT

In WSNs, sink-node gathers data from surrounding nodes and forwards to outside world via a gateway. Sink-node, which is the bridge between deployed sensor network and outside world, has a vital role in sensor network operations. Therefore, its location information must be hidden from any attacker. To protect BS location privacy against local and global adversary, we discussed Ring, Multi Sink and Random Walk Technique. Energy Consumption is more in Random Walk and Multi Sink Technique compared to Ring Technique.

Our work also motivates further research on reducing Energy Consumption in Random Walk and Multi Sink Techniques. They can also research on proposing new techniques based on our ideas.

**REFERENCES**

*[1] S. Ahmad Salehi; M. A. Razzaque; Parisa Naraei; Ali Farrokhtala;"Detection of sinkhole attack in wireless sensor networks",2013 IEEE International Conference on Space Science and Communication (IconSpace),pp.361-365*

*[2] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 7, no. 10, pp. 3769–3779, 2008.*

*[3] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm2005. First International Conference on. IEEE, 2005, pp. 113–126.*

*[4] E. Ngai, "On providing sink anonymity for sensor networks," in Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. ACM, 2009, pp. 269–273.*

*[5] H. Chen and W. Lou, "From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks," 2010 International Conference on IEEE*

*[6] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in Network Protocols, 2007. ICNP 2007. IEEE International Conference on. IEEE, 2007, pp. 314–323.*

*[7] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic," in in sensor networks, The ACM Conference on Wireless Network Security WiSec,2008.*

*[8] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008, pp.51–55.*

*[9]Kiran Mehta, Donggang Liu and Matthew Wright;"Protecting Location Privacy in Sensor Networks against a Global Eavesdropper,", IEEE Transaction on Mobile Computing, Vol. 11, NO. 2, February 2012.*

*[10] Venkata Praneeth Varma Gottumukkala; Vaibhav Pandit; Hailong Li; Dharma P. Agrawal, "Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks", 2012 IEEE International Conference on Communications (ICC) ,pp.6705 - 6709*

*[11]Abhishek R. Malviya; Balaso N. Jagdale;"Location privacy of multiple sink using zone partitioning approach in WSN", 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp.449 – 454*

*[12] Yawar Bangash; Lingfang Zeng; Shijun Deng; Dan Feng;" Lpsdn: Sinknode location Privacy in WSNs via SDN Approach",2016 IEEE International Conference on Networking, Architecture and Storage (NAS), pp.1 – 10*

*[13] Juan Chen; Zhengkui Lin; Xiaojiang Du;"Protecting sink location against global traffic monitoring attacker",2016 International Conference on Computing, Networking and Communications (ICNC),pp.1-5*


IJARIIE