TECHNIQUES TO PRESERVE THE LOCATION OF SINK IN WIRELESS SENSOR NETWORKS.

Lohitha KN[1], C.N Chinnaswamy[2]

Aditya raj[1], Samarth S Malya[1] Laxmish Prakash Shetty[1],

[1] *UG Students, Dept. of ISE, National Institute of Engineering Mysore, Karnataka, India.*

[2] *Associate Professor, Dept. of ISE, National Institute of Engineering Mysore, Karnataka, India.*

ABSTRACT

A wireless sensor network (WSN) is a computer network consisting of small space-occupying distributed autonomous devices called as sensors. These small sensors are used to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants at different locations. The development of wireless sensor network communication through sensors lead to one of major issue - Privacy. Since the communication patterns involving sensors could possibly be exposed to global adversary. Many protocols such as encryption algorithms can provide content-oriented security but context-oriented information generally remains insecure. Such context-oriented information such as the locations of monitored objects and data sinks or data source location can be can be deduced and used by an adversary for wrong purpose. However, number of techniques are there to deal with local eavesdropper who can only observe network communication in a small area but these techniques are remains insecure against global eavesdropper. This paper formalizes the different location privacy preserving schemes for wireless sensor networks.

Keyword: *Wireless Sensor networks, source node, sink node, location privacy, eavesdropper, adversary*.

1. INTRODUCT ION

WSN (wireless sensor network) has become a vital subject for research because of its many critical applications [4]. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas. These various applications of WSNs include environment monitoring, security, health monitoring, medical diagnosis, smart building, smart roads, smart lighting and forest fire detection etc.

Wireless sensor networks (WSNs) consist of a large number of small space-occupying nodes that can sense, collect, and transmit information to other nodes in network. WSNs comprises of different sensors which collect the general or sensitive data like identity of a person or the status of a communication, health information of a person or social and financial status of a person or area of some field like battlefield. These applications often include monitoring of sensitive data such as an army's movement in the battlefield or location of a person.

There are endless possibilities where WSNs can be used. One of these applications is tracking and monitoring. Therefore, security of such information is most challenging aspect of WSNs. WSN faces many constraints like computation capability, memory, limited energy, limited transmission range etc. These constraints make the security in wireless sensor networks a challenging task.

One of major security challenge that WSN faces is privacy.

1.1 WSN Security Goals

Privacy in WSNs are basically categorized in two categories:

(i) Content-based privacy or Data privacy

(ii) Context-based privacy.

Different types of privacy issues in wireless sensor networks is shown in Fig [5].

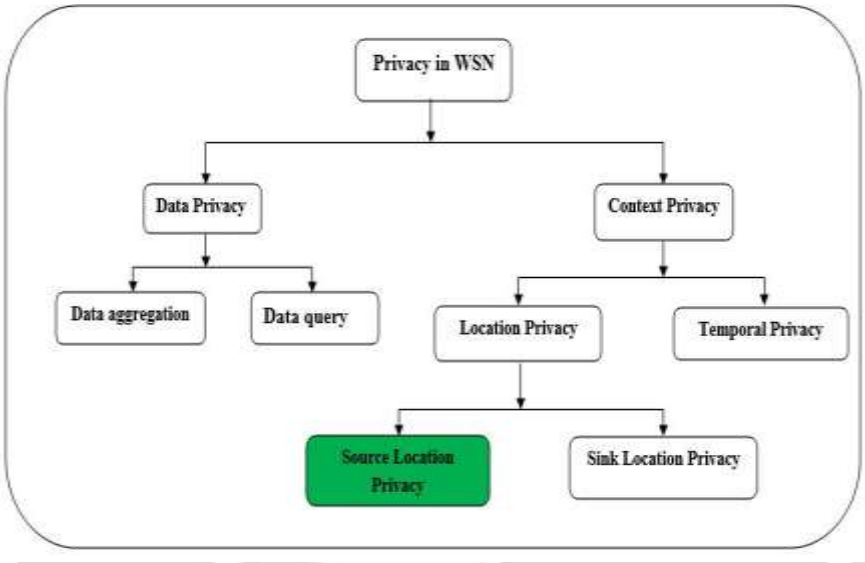

Fig-1: Privacy Issues in WSN.

Here we pay consideration on a few security requirements identified with WSN:

Data privacy: Content-oriented privacy (Data-oriented privacy) is concerned with the attack related to data. Any intruders or adversary should not learn the content of packet which is being transmitted in the sensor network. It is the ability to hide message from global adversary.

1. Data confidentiality: It ensures that the given message should not be understood by anyone other than the desired recipients. Encryption of data is one way to achieve that.

2. Data integrity: Data confidentiality can prevent taking hold of data by malicious nodes; however, it cannot stop data from being altered by unauthorized persons. Data integrity ensures that the message will not be altered during communication by any malicious nodes or global adversary.

3. Data authentication: This is the determining the reliability of message's origin. The receiver node should verify whether the information is received from an authenticated node.

4. Data availability: It ensures desired data are available all the time during the entire communication even in case of security attacks or system failure.

5. Self-Organization: A wireless sensor network is a typically an ad hoc network, thus every sensor node network should be independent and flexible enough to be self-organizing and should be flexible according to different situations.

6. Time Synchronization: In order to consume less power, a sensor may be turned off for some period of time.

7. Secure localization: A wireless sensor network should be able locate each sensor in the network to accurately and automatically.

8. Authentication: Authentication ensures that only authorized sensors can take part in communication between the sensors.

9. Data freshness: No old data should be deliver to the receiving node.

Data privacy requires a strong cryptographic algorithm Such as public key cryptography or private key cryptography in WSN to hide message from global adversary.

Contextual-oriented privacy: Contextual oriented privacy is concerned with the ability of adversaries to learn information from observations of sensors and communications within the network without having any access to the content of messages.

Furthermore Context-oriented privacy can be divided in subclass as,

(i) temporal privacy and (ii) location Privacy.

In this project work, we mainly concentrate on the location privacy preservation of sink node which is a type of location privacy.

1.2 Location Privacy Preservation of Sink

The attacker can deduce the location of sink by examining the traffic analysis in a network. These attacks can be carried out either by local adversary or global adversary. A local adversary is one who analyze the traffic in the small area by moving around the packet and find out the direction of communication. A global adversary is the one who can analyze all the traffic in a network and interpret the direction of each communication. This can be achieved by deploying the fake sink in the WSN as a part of network. Global adversary can analyze all the traffic through this fake sink deployed by the adversary.

ATTACKS: Attacks in WSN can be carried out by two methods:

I. Traffic analysis attack: Traffic analysis is a one of the most common type of attack technique. In this type of attack, attacker analyze the communication patterns between nodes in WSN network. Traffic analysis attack intercepts messages to deduce information from communication patterns. It can be performed even when the messages are encrypted and attacker is not authorized to decrypt the message. The attacker observes a number of messages for long period and tries intercept nature of message and communication. Attacker store all the information about the message and communication between the nodes. The more attacker Know about communication the more probability that the attacker gets to deduce the location of Sink node. But this type of attack requires a long period of time to attack since attack needs to analyze all the transmission and communication between nodes to find out the communication patterns [3].

II. Packet sniffing: This type of attack is more efficient than Traffic-analysis attack strategy. In Packet sniffing attacker analyze data stored in the packet, Sensitive data such as location of source node or location of destination node (which is generally sent with packet) can be deduced if the data is not encrypted. one other way is attacker hold the packet and moves with packet as packet gets delivered to other node means attacker moves along with packet and by keeping information about packet's route attacker might reach to the source node. This type of attack is more effective since attacker does not need to wait for the communication pattern rather attacker moves with packet and can trace the sink location by tracking path of packet.

2. RELATED WORK

WSN has become a vital subject in the research work because of its various applications. Although WSN faces some constraints like computation capability, limited memory, limited energy, limited transmission range etc. These constraints impose security risk in wireless sensor such as privacy. Location privacy preservation of sink is based on sink simulation, false packet injection, backbone flooding and location privacy routing etc. All these techniques are designed and simulated through ns3 simulator and performance evaluated.

In this paper we will discussed about the all 4 techniques to preserve the location of the sink in wireless sensor networks.

3.TECHNIQUES TO PRESERVE THE LOCATION OF SINK

A. SINK SIMULATION:

One method of location privacy preservation of sink is sink simulation. In sink simulation, fake sinks are established in sensor network to confuse the global adversary. The fake sinks are simulated within the communication range of real sink.

Consider A wireless sensor networks which consists multiple nodes. A subset of these nodes is considered as fake sinks and are simulated within the range of real sinks. when packets are transmitted to the other sensor nodes, sensors do not make any distinction between real and fake sinks. Packets are sent to both the real and fake sinks. Both real sink and fake sink get the packet with the equal probability p.

To achieve sink simulation, at least one fake sink is simulated in the communication range of real sink. Wireless sensor network should have two fake sinks as far as possible, because if fake sinks are too close, attack on one fake sink might destroy another fake sink as well.

When an event is detected, the source nod transmits the packet to the fake sinks in the network. So, the entire fake sinks receive the report about the event. Fake sinks broadcast the packet locally to the real sink using various routing protocols. So, it is must that the real sink should be in the communication range of at least one of the fake sink. Since fake sink send packet to real sink locally, global adversary might believe that the real sink can be in the communication range of fake sink, thus it may be confusing for an adversary to find out the location of real sink.

B. FAKE PACKET INJECTION:

The basic idea of fake packet injection is to use for multiple paths for transmitting the packets and make it difficult for the global adversary to trace the route of packet. In fake packet injection, real packets are sent to the real sink and fake packets are sent to the fake sinks and some other random chosen destinations or sinks. Fake packets are generated to confuse global adversary since adversary might treat fake packet as the real packets and will spend more time and effort in tracing the route of fake packets. One question arises if fake packet generates the same traffic same traffic such as real packet, are the nodes are energy efficient and which nodes are responsible for the fake packet injection. Usually Intersection of multiple shortest path from base station to sink are responsible for the fake packet injection. Real packet choses shortest path from source to sink and travel along it. Fake packets are packet with no useful content and are generated by source. Fake packets are generated just to confuse the global adversary and waste adversary's time and efforts. Fake packets travel to sink or any other destination through the intersection nodes. Traffic of fake packet in network depend on different situations.

In fake packet injection, every intermediate node and source has different states as following [1]:

(a) Every sensor has a counter and a timer, and their value are initialized to 0. Every sensor receives packet from its immediate neighbor nodes.

(b) As soon as sensor receive packet from its neighbor, its counter is incremented by 1.

(c) Sensor routes the packet according to the its routing table. Now step (a) is repeated till counter reaches its threshold value or timer is expired

(d) When counter value reaches its threshold value or the timer is expired, the intersection node start injecting fake packets to fake sinks and some random chosen destinations.

(e) The intersection node resets its counter and timer.

Fake packet arises three situations: (a) in first situation, if the first intersection node is not found, then only real packet is routed along the routing path. If an attack is made on real packet, attacker might be able to track the first interaction node. (b)When a packet arrives at the first intersection node, as soon as counter reaches its threshold value or the timer expires, the intersection node start injecting fake packets to the fake sink or some randomly chosen destinations. The number of fake packet injected by intermediate node is equal to the number of real packet. (c)The third is the stage after a packet leaves the first intersection node, second intersection node receives fake packets for

every real packet. Sending fake packets for every real packet is reduces traffic and does not allow the adversary to store the direction information.

C. BACKBONE FLOODING:

The idea behind backbone flooding is to create the backbone, it is created by finding out minimum number of sensors that are needed to flood a packet so that whole network can receive it. This backbone will be utilized to relay both real data packets and fake data packets. We assume an attacker could not distinguish a fake data packet from a real one. At any instant of time, a number of data packets, either fake or real, are flowing in the backbone. Fake data packets can be generated at any time with some probability by a sensor and be flooded for a random number of hops. The flooding of real data should be able to reach at least one access point. It is preferable for a real data packet to be relayed a random number of hops. Access points (data sinks) can reside at any place in the network. They may serve as backbone nodes or may simply attach to the backbone. An access point silently reads the data destined to itself. Regular sensors are either backbone sensors or neighbors of some backbone nodes.

D. LOCATION PRIVACY ROUTING:

In this method, each sensor divides its neighbor into two lists: a closer list consisting of neighbors who are closer to the sink node, and a further list consisting of neighbors that are further from the sink node. Privacy of the sensor node can be defined as delivery of event information only for legitimate users such that no other parties can either analyze the traffic patterns and estimate the behavior nor decipher the content. In order to protect the content, various data encryption methods are employed in wireless sensor networks (WSNs) and abundance of research are being carried out in this particular field. Compared with data privacy, contextual privacy has not acquired much attention in WSNs environment. If an adversary may be able to estimate the behavior of network and locate the source node with contextual information like traffic patterns, transmission speed etc. without requiring to decrypt the data payload. An adversary employs backtracking algorithm to trace the source node, where it follows the traffic in the sensor networks operating in multi hop fashion. This traffic patterns between different hops in WSNs are analyzed by attacker to infer immediate sender and followed through to find the location of a source generating the message.

4. IMPLEMATATION AND EXPERIMENTAL RESULTS

We are taking the following steps to implementing the four techniques using the latest version 3.26 of NS-3

Step 1: we create a Wireless sensor network have 1 sink node, 1 fake sink node and 20-30 sensor nodes use.

Step 2: fake sink node only randomly changes the position and other all nodes are stationary nodes (fixed position) not movable use consent position mobility model and set simulation are is 500X500.

Step 3: next implement attack for SINK SIMULATION, FALSE PACKET INJECTION and BACKBONE FLOODING.

Step 4: next implement LOCATION PRIVACY ROUTING protocol implement to minimize the traffic direction information that an adversary can retrieve from eavesdropping.

Step 5: run the simulation.

Step 6: plot the results are Latency and Event detection.

We are set up the all working environment for the ns-3.26 after that compiling the code. once get successful compilation we run the animator and simulate the all techniques in animator.

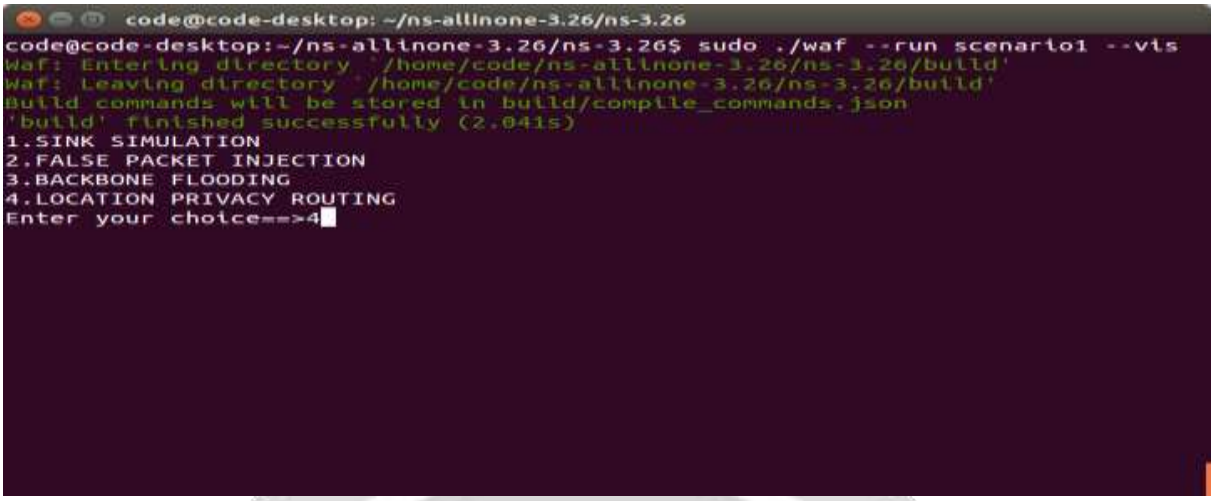

Fig -2: Successfully build and run the code.

we create a Wireless sensor network have 1 sink node, 1 fake sink node, 2 attacker nodes and 30 sensor nodes use.

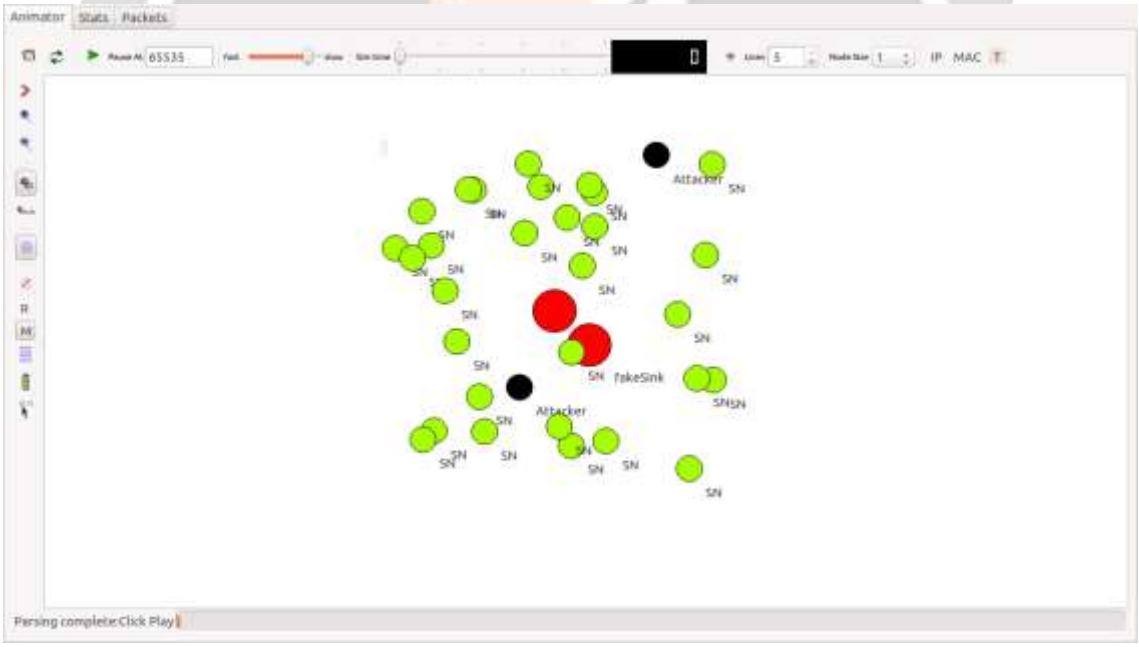

Fig – 3: Creating the wireless sensor network.

Initial configuration of network for creating wireless sensor network shown in fig-3. we are creating the wireless network it contains one sink node (SN-Red color), one fake sink (fake sink -Red color), two attacker nodes (Attacker -Black color) and 30 sensor nodes (SN-Green color).

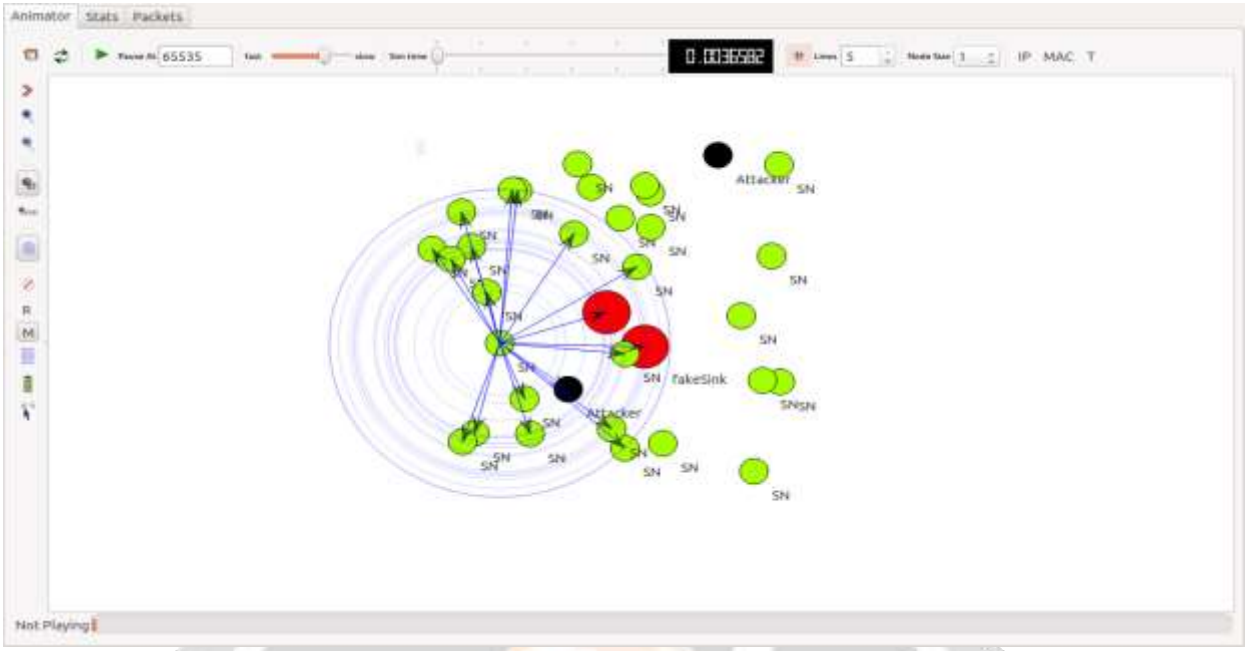

Fig – 4: Simulation results of all 4 techniques.

Initial network configuration for Sink simulation, False packet injection, Backbone flooding and location privacy routing is shown in fig 4, fake sink node only randomly changes the position and other all nodes are movable use Random mobility model. In case of sink simulation, we established the fake sinks for the real sinks and in false packet injection create the false packet which are send to the fake sink and real packets are send to the real sink. Backbone flooding is to create the backbone, it is created by finding out minimum number of sensors that are needed to flood a packet so that whole network can receive it. This backbone will be utilized to relay both real data packets and fake data packets. We assume an attacker could not distinguish a fake data packet from a real one. At any instant of time, a number of data packets, either fake or real, are flowing in the backbone. LOCATION PRIVACY ROUTING protocol implement to minimize the traffic direction information that an adversary can retrieve from eavesdropping.

5. CONCLUSION AND FUTURE ENHANCEMENT

The main aim of wsn is to meet the challenging requirements such as energy utilization, scalability etc. Sink, which is a connecting link between the network and the end user has to be well maintained. So, privacy of the sink becomes an important issue. In our project we have implemented four techniques regarding hiding the location of the sink namely sink simulation, false packet injection, backbone flooding and location privacy routing. In future, area of energy consumption for these techniques has to be overlooked precisely.

6. REFERENCES

[1] Protecting the sink location privacy in wireless sensor networks , Lin Yao • Lin Kang • Pengfei Shang •Guowei Wu , Received: 18 September 2011 / Accepted: 29 December 2011 / Published online: 28 April 2012

[2] Protecting Location Privacy in Sensor Networks against a Global Eavesdropper, Kiran Mehta, Donggang Liu, Matthew Wright ,Member, IEEE

[3] Multiple Techniques To Preserve Location Privacy of Sink in WSN,1. Venu H.D,PG Student,National Institue of Engineering,Mysuru,India.2.Chinnaswamy C.N. Associate Professor,National Institute of Engineering,Mysuru,India

[4] Location Privacy in Sensor Networks: An Approach for Prevention From Adversaries, 1. Pediredla Srilatha, 2. Dinesh Reddy,Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India

[5] Source Location Privacy Using Fake Source And Phantom Routing (FSAPR) Technique in Wireless Sensor Networks,Pradeep Kumar Roy, Jyoti Prakash Singh, Prabhat Kumar and M. P. Singh,National Institute of Technology Patna, Bihar, India

[6] Protecting Location Privacy in Wireless Sensor Networks against Eavesdropper, 1. Seema Goswami, 2.Prof. Nidhi Chandrakar, 3. Prof. Somesh Dewangan ,Computer Science And Engineering(Information Security),Disha institute Of Management And Technology,Raipur, India

[7] Enhancing Source-Location Privacy in Sensor Network Routing ,Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk,Wireless Information Network Laboratory (WINLAB),Rutgers University, 73 Brett Rd., Piscataway, NJ 08854.

[8] AN EFFECTIVE SCHEME OF LOCATION PRIVACY PRESERVING IN MONITORING SYSTEM FOR WSNs , 1. K. Chaithanya Jyothi ,Student, M.Tech (CSE), Anadapuram , Al-Ameer College of Engineering and Technology, VIZAG, A.P, India

2. V. Srinivas , Asst.Professor, (CSE), Anadapuram , Al-Ameer College of Engineering and Technology, VIZAG, A.P, India

[9] THE PROBLEM OF GLOBAL EAVESDROPPER IN WIRELESS COMMUNICATION IS SOLVED BY GI , Harsha C.Kunwar , Shreya Pandey , Department of Computer Technology , GHRP, Nagpur, Maharashtra,India.

[10] Software Defined Wireless Sensor Networks Security Challenges , 1. Tebogo Kgogo, Bassey Isong ,Computer Science Department North-West University, Mafikeng, South Africa, 2. Adnan M. Abu-Mahfouz ,Meraka Institute , Council for Scientific and Industrial Research (CSIR) Pretoria, South Africa

[11] Privacy Enhancing Technologies for Wireless Sensor Networks , Chi-Yin Chow, Wenjian Xu and Tian He

[12] Survey On Location Privacy Preserving Schemes In Wireless Sensor Network , Revati A. Parate,Pragati Patil Girish Agarwal, ABHA GAIKWAD PATIL,college of Nagpur

[13] IMPROVED DEVELOPMENT OF ENERGY EFFICIENT ROUTING ALGORITHM FOR PRIVACY PRESERVATION OF SINK IN WSN 1.Pallavi Saxena, Scholar, E&C Department, NITTTR, Chandigarh, India , 2.Dr. Kanika Sharma ME,Associate Professor, E&C Department, NITTTR, Chandigarh,India