ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# To Enhance Schema on both source and sink location privacy against local eavesdropper on multiple mobile Sources in WSN

Gurwinder Singh
M.Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
AP, M.Tech Computer Science,
Department of CSE

***Abstract:*** WSN is fundamental arrangement of different and devoted sensors. These sensors observe and record the physical condition of the surroundings and than manage the collected information at a central location. The open features of wireless communications allows an adversary to detect the location of a source or sink. Finally the adversary capture them by eavesdropping on the node's transmissions and tracing the path followed by the packets in the network. Thus the location privacy of both the source and sink becomes an important concern in such networks. Earlier researches focus only on the location privacy of the source or sink independently. In this paper, the attacker identifies the hot spot location. It gets the location and id information of all nodes within its range through location based DREAM protocol. It attacks and blocks their communication actions. Our proposed protection scheme provides the attack free surroundings in presence of attacker and also improves the network performance.

***Keywords:*** sensor node, location privacy, eavesdropper, sensor networks, network security

## I. INTRODUCTION

WSN (Wireless Sensor Network) is the broadly used network of sensors that are circulated and autonomous. They observe physical and environmental circumstances such as sound, temperature, humidity and pressure and send this data through the network to a main locality. Its development was motivated by many military applications like battlefield supervision. These networks are used today in many user and industry applications, such as business process monitoring and control, machine health monitoring, etc.

It uses the wireless links for communication among the sensor nodes. Therefore, it is said to be open in nature. Nodes can be easily compromised in this type of network because of its openness. So this may lead to many security problems. An enemy may try to attack the network in order to get some information. For this, it may compromise the sensing nodes of an event to get direct information from them or may try to compromise the intermediate nodes in the network. The worst thing it may do is to attack the sink node itself which is the central point of the complete network data. This sort of attack can make the sink a single point breakdown for the whole network. The WSN network is built of thousands of nodes. Each node is connected to one or more sensors. Every node has several parts like a microcontroller, a radio transceiver with an antenna, an energy resource such as a battery and an electronic circuit for interfacing with the sensors. A sensor node may vary in size. Cost and size restrictions result in subsequent limitations on resources such as computational speed, memory, communications bandwidth and energy.

The sink node is the most important part in the sensor network. All the sensors send data to this node. It can be highly sensitive as in case of network deployed in the war zone where it can be carried by some soldier himself. If the location of this node is exposed to the opponent, the life of that soldier can be at huge risk. Therfore it is very important to provide the location privacy to the sink node. Location privacy is of critical security concern. Lack of location privacy may expose important information about the traffic passed on the networks. Secrecy of the information can be ensured by encryption, but it is more difficult to effectively deal with the location privacy. The sensor nodes consist of inexpensive and low-power radio devices. They are intended to work for lengthy time periods. Replacement or recharging of battery may be not possible. So cryptographic algorithms may not be quite suitable for these type of networks. This makes location privacy a really difficult job.

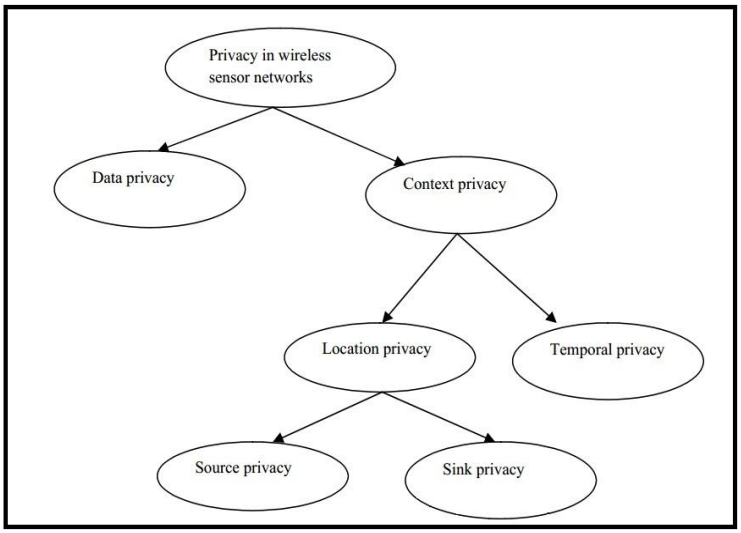


Figure 1. Privacy in WSN.

The enemy may attack on nodes to get the sensed data. There are two types of attacks:

1) *Local attack*: Extra nodes are added into the network or the existing nodes are compromised to gain access to the information.
2) *Global attack*: The whole system structure is created by the adversary over the existing system to acquire entire network state.

### A. *Characteristics*

1) Open environment.

2) Prone to different attacks.
3) Capability to deal with failures.
4) Limited resources like memory, battery life and processing ability.
5) Scalability.
6) Information flows from nodes towards central point and than moves toward a base station called sink for processing.
7) Ability to face harsh environmental conditions.
8) Self configuring.
9) Self organizing node.
10) Communication failures.

## II. PREVIOUS WORK

During the past years, researches focus on location privacy protectin of source or sink separately.

In [1], four schemes are proposed to protect the location privacy of source and sink. They are named as forward random walk, bidirectional tree, dynamic bidirectional tree and zigzag bidirectional tree. These schemes are also implemented on TOSSIM platform.

Kamat [2] proposes a technique to protect source location privacy. The technique is called phantom routing. This technique prevents the attacker from attacking the source node. Ozturk [3] also proposes the method to provide source location privacy. They modify the sensor routing to protect the location of source. Wang [4] introduces phantom routing with locational angle scheme to protect source location privacy for path selection in the network.

Mehta [5] presents two techniques for source location privacy named as periodic collection and source simulation which are much effective. In [6], Deng provides two approaches to secure the network from adversaries. Firstly, the multiple base stations will have multiple paths and secondly, anti-traffic analysis is done in the network to avoid unwanted traffic.

Jian [7] proposed a technique called LPR (Location Privacy Routing protocol) which controls the traffic of the network to prevent the adverseries from attacking the nodes. Ngai [8] proposed a new method for protecting sink location. It states that sinks moves accross some random paths and collects information from nodes. So the attackers cannot predict location and movement of the sink node.

In [9] SLPP was introduced. Reason for introducing this was to protect the sink location privacy. In this technique, fake messages were injected to the network. These fake messages helped to protect the location privacy. In [10], Xi proposes a technique named as greedy random walk. It is a routing protocol that prevents the attacker from getting the information regarding location of the source node. Hencce it provides source location privacy and secure the source node.

So the earlier researches proposes techniques to provide source and sink location privacy independtly. They do not aim to protect the source and sink nodes respectively.

## III. PROPOSED SCHEME

The aim of proposed scheme is to provide the source location privacy against hotspot locating attack in Wireless Sensor Network. In this paper, we had provided privacy against the attack by misguiding the attacker and sending him the deviated location information and false identity of the sensor nodes. In the proposed work, the adversary deploys the monitoring nodes in the WSN; we will called them as attacker in our entire work. The attacker continuously monitors the traffic of particular area of the entire network. The attacker collects the traffic information which includes the unique identity of the node, its location (x y coordinates), time at which the information is last updated and the speed of the mobile node. It collects this information of mobile nodes through DREAM protocol. On the basis of this information, it attacks the nodes by sending the false reply of route existence from sender to receiver and drops all the data packets.

In order to protect the source node from the attacker, the protection scheme has been applied. In protection scheme, all the nodes are aware about the behavior of attacker in the network. Now, whenever attacker uses DREAM protocol to know the information of the nodes in its range, all the nodes send their deviated location and false identity of the node to misguide the attacker. Therefore, the entries in the location table of attacker contains false information of the location and identity of the node. Now, whenever the attacker tries to attack the source node on the basis of entries in its location table, it does not succeed in doing so because it attacks on the deviated location of the node and hence the source node gets protected from the attack. It attacks somewhere else in the network other than the destined node. In this way, the data packets have been sent successfully from the source to the sink.

## IV. PROPOSED ALGORITHM

The proposed algorithm of security scheme given below misguides the attacker and provides secure data delivery in network.

Initialize
S: Sender Nodes
Ss: Sink Node
Attack Type : Hot Spot Location Attack
Attacker Uses: Dream Protocol (for location and Capturing)
Normal Routing: AODV
Prevention: Location and Id Updating
Step 1: Begin
Step 2: Source Node detects the event
{
Step 3: Source Node S Search Sink Ss Node for Message Transfer
Step 4: If (Ss found and Attacker present network)
Capture Location and id of S node using Dream
Target to Source S
}
Else If (Ss found and Source S send updated Location and ID info and Attacker present network)
{
Capture Location and id of S node using Dream
Target to Source S
Target not found
Safe Data send to Sink Ss
}
Else
{
Normal Data Delivery to Ss sink Node
}

Step 5: Stop

## V. RESULTS ANALYSIS

In this section the analysis of simulation results are mentioned with the scenario of normal routing, in case of attack and when protection scheme is applied.

### A. *Routing Load Analysis*

The routing packets are required in network to find the destination and confirm the path in between source and destination. The destination is validating the request packets then after that the data packets in network is delivered. This graph represents the routing packets analysis in case of attack and protection scheme. This graph illustrate that in case of attack about 1700 packets are deliver in network but on the other hand in case of protection scheme about 6500 routing packets are deliver in network. The less amount of routing packets delivery provides the better performance in network. In case of attacker or hunter very few packets are send in network but in case of protection the packets quantity is more. The attacker aim is to identify the node ID in network and after that attacker convey false reply of route existence to destination. The attacker is identifying the location of source nodes and drops the data packets in network. The proposed deviated location and node identification (ID) scheme is provides the attacker free environment and secure path for data delivery.

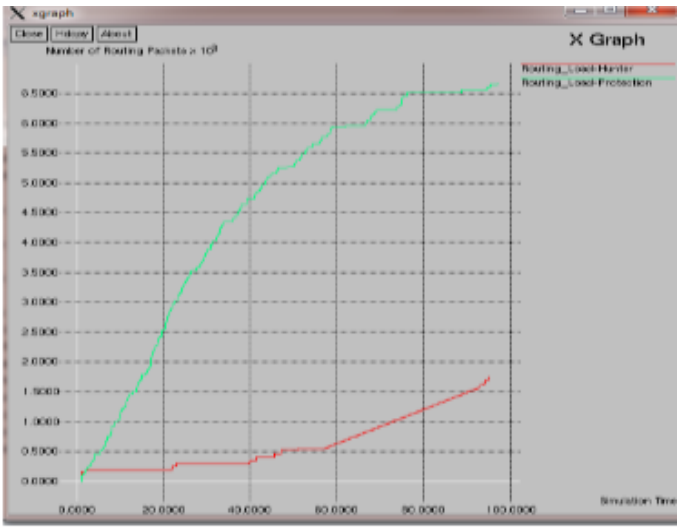


Figure 2. Routing Load Analysis.

### B. *Attacker Loss Analysis*

In network, the aim of attacker is to damage the network and degrades it's performance time to time in network. In this research, the attacker has targeted the nodes on the basis of their location and node ID in network. The attacker has identified the location of node through the location table and then targets the source node. The attacker has identified the actual position and state of node and then drops all data packets that had originated from the source node. In this graph, the analysis of packet delivered to the sink node has been mentioned in the presence of attacker. It is described as how much amount of data packets has been lost in a given simulation time. This graph has illustrated the data loss in network in presence of hunter and evaluated the loss of data.

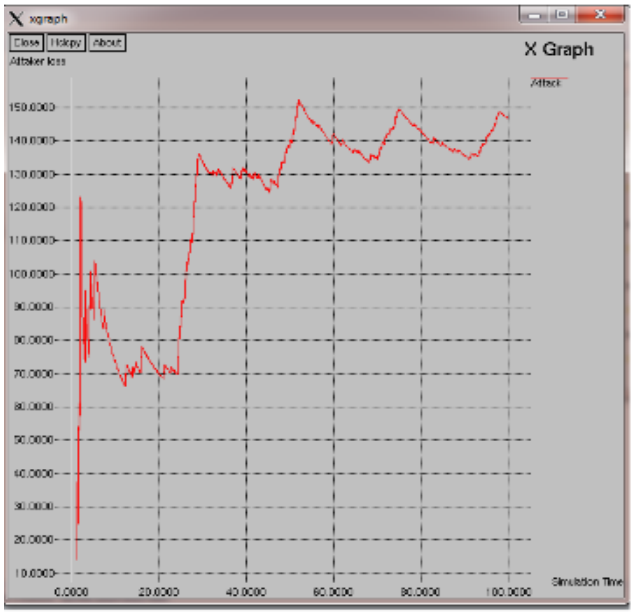


Figure 3. Attacker Loss Analysis.

## VI. CONCLUSION

Security is another unique characteristic of WSN and it is a fundamental concern in order to provide protected and authenticated communication between sensor nodes in critical applications, such as military or healthcare. In WSN, physical security of sensor nodes is not guaranteed as they are usually deployed in remote and hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. In order to optimize the conventional security algorithms for WSN, it is necessary to be aware about the constraints of sensor nodes. In this research, the Attacker identifies the hot spot location and it has the location and id information of all nodes within its range through location based DREAM protocol and it attacks and also blocks their communication activity in network. Our protection scheme provides the attack free environment in presence of attacker and it also improves the network performance.

## VII. REFERENCES

[1] Honglong Chen, Wei Lou, "On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks" Elsevier, 2014.

[2] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, "Enhancing source-location privacy in sensor network routing" IEEE, 2005, pp. 599–608.

[3] C. Ozturk, Y. Zhang, W. Trappe, "Source-location privay in energy constrained sensor network routing" ACM, 2004, pp. 88–93.

[4] W. Wang, L. Chen, J. Wang, "A source-location privacy protocol in WSN based on locational angle" IEEE, 2008, pp. 1630–1634.

[5] K. Mehta, D. Liu, M. Wright, "Location privacy in sensor networks against a global eavesdropper" IEEE, 2007, pp. 314–323.

[6] J. Deng, R. Han, S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks" IEEE, 2004, pp. 637–646.

[7] Y. Jian, S. Chen, Z. Zhang, L. Zhang, "Protecting receiver-location privacy in wireless sensor networks" IEEE, 2007, pp. 1955–1963.

[8] E.C.H. Ngai, I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks" ACM, 2009.

[9] B. Ying, D. Makrakis, H.T. Mouftah, "A protocol for sink location privacy protection in wireless sensor networks" IEEE, 2011.

[10] Y. Xi, L. Schwiebert, W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks" SSN, 2006.