Protection of Source and Sink in Wireless Sensor Networks

Prabhjot Kaur,Mandeep Kaur

ABSTRACT - In wireless sensor networks messages are sent from source to sink, but it sometime becomes a risky communication way because of presence of eavesdropper. During transfer of packet or message from source to sink an eavesdropper may attack on the network and creates problem for the sender or receiver, as the eavesdropper may trace the path and detect the location of source or sink very easily. Because of this security is always remained a concern topic in wireless sensor networks. Different techniques introduced time to time for the protection of source and sink in wireless sensor networks. I n this paper we have also introduced a scheme for the location privacy. This technique especially effective when eavesdropper will try to locate the location of source or sink by using DREAM protocol. In this scheme deviate location information and false identity of sensor nodes is provided to the eavesdropper which can confuse the attacker and protects our source as well as sink.

Index Terms— Wireless, Source, Sink, Eavesdropper, Privacy, Data collection, monitoring.

1 INTRODUCTION

Wireless sensor networks consist of numerous small nodes that collect and spread the information for many different types of applications. It is made up of number of sensor nodes that are self organized to carry out tasks such as mobile object monitoring and environmental sensing. Because they use wireless communications which can be accessed by anyone who wishes, it is not difficult to trace the location of sender and receiver. This is usually guaranteed by using methods of encryption and authentication[3].

The nodes in these networks having identical capabilities and energy in a network is called homogeneous network [8]. These types of networks can be again classified into flat and hierarchy topology. In the flat topology that the sensors close to the static sink consumes more energy than the sensors at the margin of the network.

The drawbacks of flat topology can be overcome by using hierarchical topology i.e., clusters. In this, the group of nodes that forms the lower layer and the cluster heads at the higher layer [4]. Cluster head, which collects data from the lower layers and then forwards it to the sink. Cluster head can acts as an aggregation point. Since the cluster head is collecting data from lower nodes, it consumes more energy than other nodes. So, the sensor nodes can be rotated dynamically to avoid the energy consumption.

The Heterogeneous networks having small number of resource rich nodes and large number of resource limited basic nodes. The resource rich nodes are having powerful transceivers and batteries. The resource rich nodes can acts as cluster heads. The resource limited basic nodes having limited communication capabilities.

Mobile Data Gathering is a technique that consists of one or more Mobile Collectors (MC's) [4]. Mobile collector is a device equipped with powerful transceiver and high battery power. It gathers the data in short-range communications. MC roams over the sensing field to collects the data while moving or pause at some points on its moving path from the sensors. To attain the maximum energy saving, a mobile collector must travel the transmission range of each sensor node in the field. It helps the mobile collector to collect the data packets in a single hop. The path of the mobile collector in the sensing field may be random or planned. The mobility of the collector reduces the energy consumption in the network.

Every sensor communicates directly with the sink is called single-hop relay [7]. It requires large transmit power and may be infeasible in large geographic areas. Sensors that serve as relay for other sensor nodes are known as multi-hop routing in wireless sensor networks. Data packets are forwarded to data sink via multi-hop relay among sensors. Energy consumption is more while forwarding the data packets in multi-hop. To achieve the uniform energy consumption, the Single Hop Data Gathering Problem (SHDGP) is used [2]. The mobile Data Gathering algorithm is used to find the minimal set of points in the sensor network. It serves as data gathering points for mobile node [4] [8].

In some applications, the sensor nodes are deployed to monitor different areas. In such applications, the network may be disconnected. In those applications, the sensors cannot forward data to sink via wireless links. A mobile collector can be used to collect the data. Mobile collector is a

device equipped with powerful transceiver and high battery power [4].

Recent advancement in wireless communications and Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low-cost Wireless Sensor Networks (WSNs), which are made up of a number of sensor nodes that are self-organized for various applications, such as mobile target detection [2], earthquake monitoring [3], and habitat monitoring In these applications, sensor nodes are deployed to detect the existence of an interested event, such as the appearance of a rare animal. The sensor nodes that detect the occurrence of the interested event will send the detection information to a sink (or base station) by multi-hop wireless communications. Such kind of systems is called event collection system, which is one of the important applications in WSNs.

1.1 Data Collection Techniques

The data collection technique is used to collect the aggregate data from the sensor node to the sink node. The main objective of the data collection process is to reduce the delay and improves the network's lifetime. There are various techniques used to collect the data from source node to sink node.

First, all the sensors are static and then the network is considered as static network. The static sensor node forwards the data to the sink by one or more hops [9]. So, the sensor located nearer to the sink gets depleted soon.

Second, the hierarchy form of data collection. The nodes can be categorized into lower layer and higher layer. The nodes in the lower level layers are homogenous sensor nodes. The nodes in the higher layer are more powerful than the nodes in the lower layer. The higher layer nodes are called as cluster heads. The hierarchy topology is also called as clusters.

Third, Mobile Collector is used to collect the data periodically. A mobile data observer is used to collect the data dynamically. The nodes that can be located closer to the data observer can upload the data directly. The nodes that can be located far away from the observer can forward the data by relaying [9].

Single Hop Data Gathering problem (SHDGP) and mobile Data Gathering are the two approaches that can be used to increase the lifetime of the network. Single Hop Data Gathering Problem (SHDGP) is used to achieve the uniform energy consumption. The mobile Data Gathering algorithm is used to find the minimal set of points in the sensor network. It serves as data gathering points for mobile node.

Due to the open characteristic of wireless communications, it is not difficult to attack wireless sensor networks with the goal of either obtaining confidential data or simply disrupting the normal operations of the WSN applications [6]

To protect the location it is essentially to protect the end-to-end location privacy rather than merely protect the source or sink location privacy. Thus, the end-to-end location privacy protection is a crucial contextual privacy problem in WSNs.

In this paper, we propose one end-to-end location privacy protection scheme to deliver messages from source to sink, which can protect against local eavesdropper that might break the location privacy of a source or sink, i.e., the end-to-end location privacy. In this scheme the false information is stored in the table of every node so that attacker get deviated information about the path and start following the wrong path which can protect the source and sink.This scheme is effective only in case of DREAM protocol.

1.2 Dream Protocol

DREAM protocol stands for Distance Routing Effect Algorithm for Mobility. This protocol uses the distance effect [2] i.e. greater the distance between the nodes, slower the nodes appear to be moving with respect to each other. The routing tables are used to keep the location of neighbor node every node contains the information about the next node in the routing table.

DREAM protocol is a restricted flooding communication protocol used in unstructured architectures. Each node may maintain a location table about the position of all nodes of the network and frequently floods a location packet, called control packet, to update the position information maintained by its neighbors. Each location packet submitted by a node A to other nodes to update their location tables contains A's coordinates along with its speed and the time the location packet was transmitted. DREAM uses the principle of distance effect in which the location tables update frequency is determined by the distance of the registered nodes. In other words, the closer to another node, the more updates sent to this node. The frequency of sending a control packet is adjusted based on the moving speed of the source node S.

When the source node S wishes to send a message to a destination node D, it starts by looking for its location table and retrieves information about its geographical position. If the direction of D is valid, S sends the message to the all one hop neighbors in the forwarding zone determined by that direction. If no location information is available for D, then a recovery procedure must be executed by flooding partially or entirely the network in order to reach D. When a node A receives the message, it checks first if it is the node

destination. If this is the case, it sends an acknowledgement to the source node. Otherwise, A repeats the same process by sending it to all one hop neighbors that are in the direction of D. Each of these nodes, in turn, repeats this process, if possible, until D is reached.

To determine the forwarding zone in the direction of the node D, the source node S calculates the expected zone which contains D. Figure 2 shows an example of expected zone, i.e., the circle around the position of D. The radius r of this zone is set to $(t_1 - t_0)v_{max}$, where t_0 is the timestamp of the position information that S has about D, t1 is the current time, and v_{max} is the local known speed that the node D may travel in adhoc network. After determining the expected zone, the node S defines its forwarding zone which is the region enclosed by an angle whose vertex is at S and whose sides are tangent to the expected zone calculated for D and then sends the packet, destined for D, to all its neighbors in the forwarding zone.

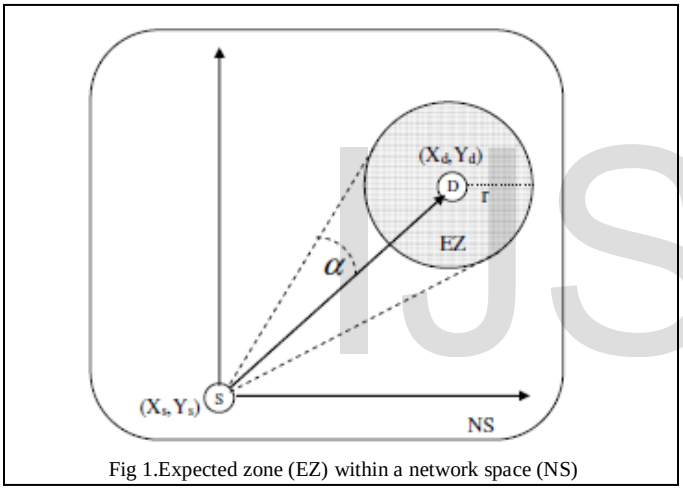

Fig 1.Expected zone (EZ) within a network space (NS)

In DREAM, exchanging nodes' coordinates instead of exchanging complete link state or distance vector information helps reducing the occupied bandwidth. Moreover, since DREAM uses the distance effect principle described above, it can perform well in dynamic mobile ad hoc networks.

2. PROPOSED SCHEME

The aim of proposed scheme is to provide the source location privacy against hotspot locating attack in Wireless Sensor Network. In this thesis, we have provided privacy against the attack by misguiding attacker by 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 contain 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.

2.1 Proposed Algorithm

The proposed algorithm of security scheme is given the whole steps misguide the attacker in 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

3 Results

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

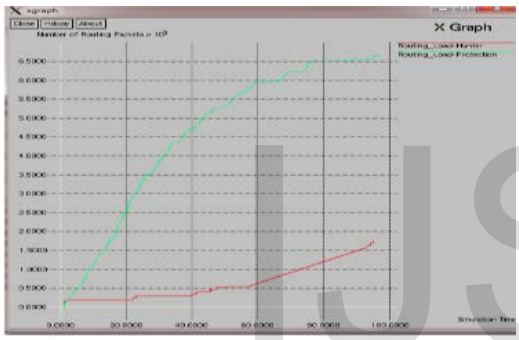

Fig 3. Routing Load Analysis

3.1 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.

3.2 Attacker Loss Analysis

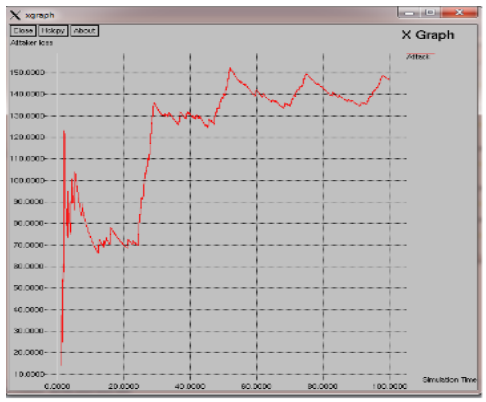

Fig 4.Attacker Loss Analysis.

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.

4 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 granted 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.

ACKNOWLEDGMENT

I highly grateful to the Director, Global Institute of Management and Emerging Technologies for providing this opportunity to carry out the present work. I am also thankful to Ms. Mandeep Kaur(Assistant Professor in Computer science department,GIMET) who has been of great help in conclusion of present work.

REFERENCES

[1] Milan Erdelj, "Mobile wireless sensor network architecture: Applications to mobile sensor deployment" 2013.
[2] Martin Lukac, Igor Stubailo, Richard Guy, Paul Davis, Victor Aguilar Puruhuaya, Robert Clayton, Deborah Estrin, "First-class meta-data: a step towards a highly reliable wireless seismic network in Peru" ACM, April 2009.
[3] Pavlos Papageorgiou, "Literature Survey on Wireless Sensor Networks" 2003.
[4] Ms. Rubia, Mr. Sivan Arul Selvan, "A Survey on Mobile Data Gathering in Wireless Sensor Networks - Bounded Relay" IJETT, Volume 7, Number 5, Jan 2014.
[5] Aarti Arjun Andhale, Prof. B.N. Jagdale "Light Weight Security Protocol for Wireless Sensor Network's (WSN)" IJERT, Vol. 3, Issue 1, January 2014.
[6] ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTOR WEN, DAVID E. CULLER, "SPINS: Security Protocols for Sensor Networks" ACM, September 2002.
[7] G. UMA, A. DINESH, "Sequential Based Hypothesis Testing in Wireless Sensor Networks" GRA - GLOBAL RESEARCH ANALYSIS, Volume 2, Issue 11, Nov 2013, ISSN No 2277 – 8160.
[8] Bhavna G. Pise, Prof. Nikita Chavhan, "Energy Efficient Data Gathering in Wireless Sensor Network" IJCSMC, Vol. 3, Issue. 4, April 2014.
[9] Narendran M, Prakasam P, "MOBILITY BASED ENERGY UTILIZATION IN WIRELESS SENSOR Network" IJETCAS, 2014.
[10] S. Girija, Mr. S. Arunmozhi, Mr. S. Anbazhagan, "Performance Analysis of Energy Utilization in Static and Mobility Relaying in WSN" IJSETR, Volume 4, Issue 3, March 2015.
[11] A. Abitha, S. Sujatha, A. Stephy, "Efficient Data Gathering With Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks" IJETT, Volume 18, Number 3, Dec 2014.
[12] Honglong Chen, Wei Lou, "On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks" Elsevier, January 2014.
[13] Pavitha N, S.N. Shelke, "Providing Source and Sink Location Privacy against a Global Eavesdropper in Sensor Networks: a Survey" International Journal of Research, Vol-1, Issue-6, July 2014.
[14] M. Bakhouya, J. Gaber, M. Wack "Performance Evaluation of DREAM Protocol for Inter-vehicle Communication" GSEM/SeT Laboratory, UTBM 90010 Belfort, France, 2009