Position Defensing In Sensor Network Using Virtual Objects

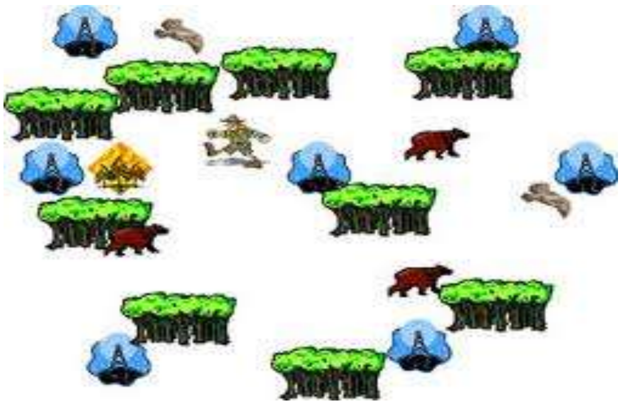
Anju Jayan, Jenopaul P
Department of Electronics and Communication Engineering,
PSN College of Engineering and Technology,
Tirunelveli, Tamil Nadu, India,

Abstract— In sensor network, it is relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the location information. After studying the adversary's behaviour patterns, we present certain steps to prevent this problem. Many protocols for sensor network security provide confidentiality for the content of secret information which usually remains exposed. Such information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Encounters on these components can significantly undermine any network application. Offered techniques defend the leakage of location information from a partial adversary who can only observe network traffic in a small field. However, a stronger adversary is realistic and can defeat these obtainable techniques. This paper first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. The paper then proposes techniques to provide location privacy to source-location and data sinks . These techniques provide trade-offs between solitude, communication cost, and latency. We demonstrate that the anticipated techniques are efficient and effective for source and sink-location privacy in sensor networks by the analysis**.**

1.INTRODUCTION

A wireless sensor network (WSN) is a collection of small randomly dispersed devices that provide the ability to monitor physical and environmental conditions and to cooperatively pass their data through the network to a main location . Sensor networks are often used in applications where it is not practical to set up wired networks. Some of the examples are wildlife habitat monitoring, security and military surveillance, and target tracking etc.

In the case of military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence. Abuse of secret information can cause monetary losses or hazard human lives. To protect such information, researchers provide classic security services. Though these are critical security requirements, they are insufficient in many applications. The way by which sensors communicating can, by themselves, reveal a great deal of secret information, which can disclose the location information of critical components in a sensor network. For example, in the Panda-Hunter scenario, a sensor network is deployed to track endangered giant pandas in a forest. Each panda has an electronic check that emits a signal that can be detected by the sensors in the network. A sensor that detects this signal, then sends the location of that animal to the destination with help of intermediate sensors. An attacker may use the transfer of data between sensors and the data sinks to locate and then capture the monitored pandas. In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g., base stations) . Acknowledging the locations of the nodes during the communication with sensors may allow the enemy to precisely launch attacks against those animals and this may cause the network damage.



Location privacy is, thus, very important, especially in adverse environments. Decline to protect such information can completely subvert the intended purposes of applications in sensor networks. To prevent the adversary from determining the physical locations of source sensors and sinks the Location privacy measures are needed, .The limited energy lifetime of battery may cause problems while communication. Therefore it should be energy efficient. The energy consumption of our protocols are measured by the cost of communication.

Providing location privacy in a sensor network is challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. time, frequency can be used for the traffic analysis and to analysis the position details. Sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the information's between sensor nodes . here we should find another way to provide position privacy that accounts for the resource limitations of sensor nodes.

Now a days, a number of privacy-preserving routing techniques have been evolved for sensor networks. But most of those techniques are made to protect against attackers which are capable to attack on a small part of the network. A highly provoked adversary can easily attack on the entire network and defeat these schemes. For example, the attacker can use his own set of nodes to monitor the messages in the target network. . This is especially true in a military or industrial spying context, where the adversary has strong, potentially life-or-death, incentives to gain as much messages as possible from observing the traffic in the target network. If the attacker has a global knowledge about the network then it is easy to monitor the positions of nodes. For example, a region in the network with high activity should be close to a intermediate node , while a field where the packets evolved should be close to a controlled object. In this paper, we have targeted on techniques that are used for the privacy preserved, secured communication against the attacker. The contributions in this paper are given below.

We consider an assumption that the attacker has the entire knowledge about the network. Under such an assumption and we apply an analysis based on Steiner trees to estimate the cost for the bit communication.

We provide the first case on how to significantly measure position privacy in sensor networks. We then apply the results of this study to evaluate our proposed techniques for location privacy in sensor networks. These include two techniques that prevent the leakage of position details —and two techniques that provide position privacy. Our analysis show that these approaches are efficient and effective.

2.EXISTING APPROACHES

Position privacy has been an active area of research in recent years. In position-based services, a user may want to retrieve position-based data without revealing her location. Techniques such as k-anonymity and private information retrieval have been developed for this purpose. In pervasive computing, users' location privacy can be adjusted by detecting the wireless signals from user devices . Random delay and dummy traffic have been suggested to mitigate these troubles. Position privacy in networks also falls under the general framework of position privacy. The adversary monitors the wireless transmissions to conclude positions of critical infrastructure. However, there are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their working time. another one, a sensor network is often quantitatively larger than the network part in smart home and benefited living applications.

In Source-location privacy, early work in protecting the position of monitored objects sought to increase the safety period, i.e., the number of messages sent by the source before the object is located by the attacker. The technique like flooding has the node which act as a source and it will send packet through many number of paths to a sink, making it difficult for an adversary to trace the source. Generation of fake packets creates fake sources whenever a sender analyses the sink that it has real data to send. The fake senders are away from the real source and merely at the same distance from the sink as the real sender. Phantom single-path routing achieves position secrecy by making every packet walk along a random path before being delivered to the sink. The technique like entrapment by cyclic loops creates circular paths at various places in the network to make the attacker fool by following these loops repeatedly and thereby increase the assurance period. However, all these techniques assume a attacker of local knowledge who is only capable of eavesdropping on a limited area. A global eavesdropper can easily break these techniques by locating the first node starts the transfer of messages with the base station.

Recently, several techniques have been proposed to deal with global attackers. There were techniques that propose to use proxies to make the network traffic such that the attackers cannot infer the locations of monitored objects. Another technique is proposed to reduce the latency of real events without reducing the position privacy under a global attacker. This technique ensures that the adversary cannot analyses the actual traffic from statistical analysis.

In Sink-location privacy, there are technique to protect the positions of sinks from a local attackers by hashing the ID field in the packet header. In , it was shown that an adversary can track sinks by carrying out time correlation and rate monitoring attacks. To prevent these two kinds of attacks, there were some techniques like multiple-parent routing scheme, a controlled random walk scheme, a wrong path scheme. In redundant hops and fake packets are added to provide secrecy when data are sent to the sink. However, these techniques all assume that the attacker has only a local knowledge about the network. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify the region where a high number of transmissions are there, to locate the sink. We, thus, focus on privacy preserving techniques made to defend against a global attacking.

3.NETWORK AND ADVERSARY MODEL

Sensor networks are in the current researches. There are many categories in sensors that have been and continue to be developed. These range from very small, inexpensive, and resource-poor sensors. Applications for networks include many forms of monitoring, such as environmental and structural monitoring or military and security surveillance. In this paper, we consider a analogue network model. In this network model, all sensors have roughly the same computing capacity, sources for power, and expected lifetimes. This is a common network behavior for many applications today. It is well studied and provides relatively correct analysis in research as well as simple arrangement and maintenance in the field.

We can use our research in to a variety of sensor platforms, most sensors run off battery power, especially in the kinds of likely hostile environments that we are studying. in this, each sensor has a limited time and the network should be made in order to power reserved. It has been demonstrated that sensors use more power for the transmission and reception of messages. Thus, we focus our evaluation on the amount of transmission overhead incurred by our protocols. For the kinds of sensor networks that we envision, we expect highly actuated and well-funded attackers whose objective is to leak the secret information such as the position of monitored objects and sinks

Here the network will monitor the objects which will be fussy in nature. These can be guard, robots etc or certain animals in the extinction listed. If the position of these were known to an attacker then these things will get attacked for the profit of this attacker. The intermediate nodes are also very important which will act as the gateways in between the multi hop networks. And also if there occurs any problem to the intermediate nodes then this can cause permanent damage to the whole networks. It is easy for an attacker to compromise the intermediate nodes,if the node become compromised then it will become easy for the attacker to take all the information from the node because in most of the transmission the messages will not be encrypted. In the case of military operations also this can become a problem, so the position information should be kept secretly.

In this paper, we consider global agent. For a actuated attacker it is very easy for attacker the whole networks in a fast and effective way and to sense all the positions of the objects. There were some ways such as snooping and it will be at a price of $25.It is actually a higher cost .so for a position it will worth the cost and trouble. In the case of snooping, due to short radio ranges the snooping nodes need to deploy a huge number of nodes. In practical it is difficult .So here we consider the first option as practical.

Rather than the case of collecting the information about the traffic the attackers can sense the objects which they need by deploying the nodes taking an object will be difficult because it is not easy to differentiate the background with the real object. For example observing a panda will be tough then analyzing a packet of datas.So to avoid these types of problems we can install. For example, recognizing a panda is much harder a sensor node in every objects which can be sense time to time. If the attacker takes a direct attacking path then it is successful for us to defense.

4.PRIVACY EVALUATION MODEL

Here we are introducing a model for the position privacy of analytical components in sensor networks. In this the attacker will deploy a snooping network and with the help of this it will target the position of the network. Here we consider a scenario in which the attacker knows about all the transmission in the networks and in the practical case it is not need to know when the packet is sent. A rough estimate of the location will be better for the attacker to analyses traffic. And also here we consider a worst case scenario that is the attacker knows about the sent time of the packet and the node where it is received. This indicates that each sensor i is an view point, and a tuple ði; t; eÞ is available to the adversary by observing each packet e send by node i at time t. The actual useful information available to the attacker is ði; tÞ. We assume that the operation here starts at time t ¼ 0

Main aim of the attacker is to locate the source and the destination of the objects by the method of snooping. The main innovation of the attacker will be the spacial temporal correlated packets which will be in each of the communication sequence.. As long as the attacker have the knowledge about the routing protocol then it is easy to find the traffic sequence in whole.

For the defender, it is must to create a dummy sequence first in addition with the traffic which leads to the communication. . Clearly, there is a trade-off between the position privacy and the communication overhead. In this section, we develop a theoretical study of this trade-off. In the case of certain sensor nodes it is difficult to access by the attacker. By the physical access the node becomes compromised. Having a collection of compromised sensors in the network will provide an merit to the attacker. However, we assume that an attacker does not compromise sensor nodes. We will find solutions to the problem of providing position privacy despite nodes being compromised in future work. We assume that we can protect the sensed objects if we can prevent the leakage of the position of sensors which act as the source. We use the terms objects and sources interchangeably in this paper.

We now describe our privacy type in detail. We will first describe a privacy type for sender-position privacy and then extend it to include receiver-position privacy. A network which consist of sensors are given to certain applications that can be examined as a graph G ¼ fV ,Eg where the set of vertices V is the union of the set I of sensor nodes and the set of sinks. A group of sensors will act as the node which is of source. The set E of edges includes all direct communication links between sensor nodes .In the point in time, from the global eavesdropper's point of view, the network can be considered to include a set SP (i.e., the protected sources), a set SA (i.e., the sinks where the data is sent), and a set of sensors that transfer data between sources and sinks. The attacker will attack on the entire network with the intention of physically positioned objects. We model each view of the attacker as the symbols ði; tÞ, which gives that a data has been given by a node i and viewed by the attacker in a certain interval t. Let Oi;T be the set of all observations collected by the attacker about node i by time T. Thus, at time T, the knowledge that an attacker can obtain from attacking on the entire target network is OT ¼[i2I Oi.

The objective of the attacker is to check a set ST I of possible sources, i.e., sensor nodes in whose range the attacker expects to find things at time T. Actually sometime the attacker will not believe that the alone observation ði; tÞ indicates the presence of an object. The presence of an object should make a trace, which is a set of observations over the lifetime of the network up to time T. By this it is concluded that there will a path of communication between possible position sources and the destinations.. Correctly, for each source i 2 ST , there must exist a subset of sinks K .SA and a set of observations Ai ;K and OT that could be exactly given because of the transfer of information from the nodes i (based on observing an object) to the sinks in K. Those set of observations are called as the trace of candidates.. In other words, a candidate trace is actually a group of nodes which is in the observation of the attacker and it will the result of the sensor giving information to the base station.

An effective way of measuring position privacy is to check the attackers accuracy in finding the sources. Here the attacker should find the nodes were he can have his interest. In this we are forced to assume that the attacker knows about the routing protocol and thereby he can reach to the real sources. The sensing range will occupy the sensing nodes which can be easily identified by the attackers (ST).We can find the area covered by the sensors. Since the sensors have the same sensing radius and the of set ST. Intuitively, the larger the size of ST, the more uncertainty the attacker will have about the position of real sources. We assume that the sensors in ST are equally likely to be sensors. The probability of any sensor node in ST being a sensor that is the source can,, be estimated by jSP j jST j . Hence, we formally define the location privacy of our system as b =¼ X jST j1 jST j log2 jSP j jST j ¼ log2 jST j jSP j.

In the following, we explore the relationship between the height of secrecy and the amount of transfer of information overhead. To minimize transfer information overhead, we should lower the communication required to produce all the candidate traces in the network.

Here first we are solving our given type to know about the policies that have applied and the position privacy that is in the networks. . In this the communication .The sensor nodes will communicate at the end of each interval i.e., at time f; 2. . . ; i ; . . .. In the nodes it can receive all packets and cant send more than one at a time. A sensor node can receive all the packets targeted to itself and will send no more than one packet in any time interval. In the case of receiving more than one dummy packets it will move one to save the communication price. As the communication price increases the value of delta also increases.

5.Privacy-Preserving Routing

In this part, we present the privacy-preserving techniques for protecting the position information of monitored objects and intermediate nodes. We are considering that the communication in between the sensors is encrypted so that it will appear a random model to the attacker.

Here ,we present two methods to provide position privacy to monitored objects in sensor networks, by the periodically collecting the data and by the simulation of the node which act as the source. . The periodic collection method achieves the high secrecy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery abeyance. The source simulation method provides practical trade-offs between secrecy, communication overhead, and abeyance.

The previous methods fail against a attacker with the global knowledge. The main reason is that the presence of a actual object will make difference in the traffic pattern at the place where we can find the objects. This can help the attacker to know about the change happened. To avoid this we send packets periodically and independently from each nodes at a frequency whether there is an actual data or not.

The periodically collecting method provides the highest position privacy in the network .It is possible that the object can be anywhere in the region at the time T,we know that for any i 2 I, there exists a candidate trace Ai;K €OT with fpðAi;KÞ ¼ i for K SA. This indicates that ST ¼ I. Hence, we have b = ¼ log2 jST j jSP j ¼ log2 N jSP j,.

It is clear that the communication in the sensor networks will be more costlier than the computations. And in the case of privacy preserving technique, its energy consumption will be measured by the communication used for hiding the traffic carrying actual data..Since the network starts operation at time 0, the total number of data packets transmitted in the network can be estimated by ðT NÞ=. Certainly, a small indicates a large amount of additional traffic for our periodically receiving method. This indicates then this cannot put the real time applications.

Here first we will consider the topology generation module. In fig 1 this the nodes are arranged in the flat grid topology. In this the node indicated by red is the base station. Since we have considered a panda hunter scenario the white color indicates the panda in the forest. The all other green color is the sensor nodes which are kept in the forest. Each and every node will transmit the signal to the base station. In this the node number 29 is nearer to the panda and so it will send the data to the base station that the panda is nearer to the 29 th node.The attacker can easily get the data if he is nearer to the node 29 and he can leak the position information here.

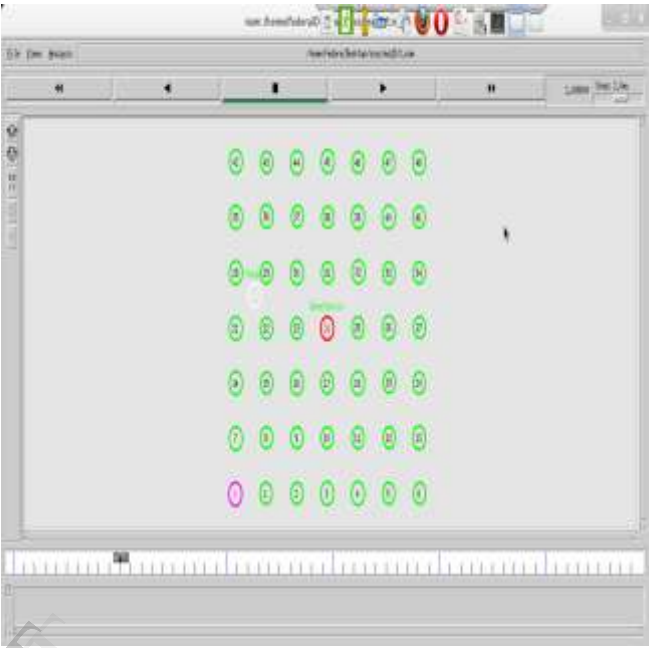


Fig 1

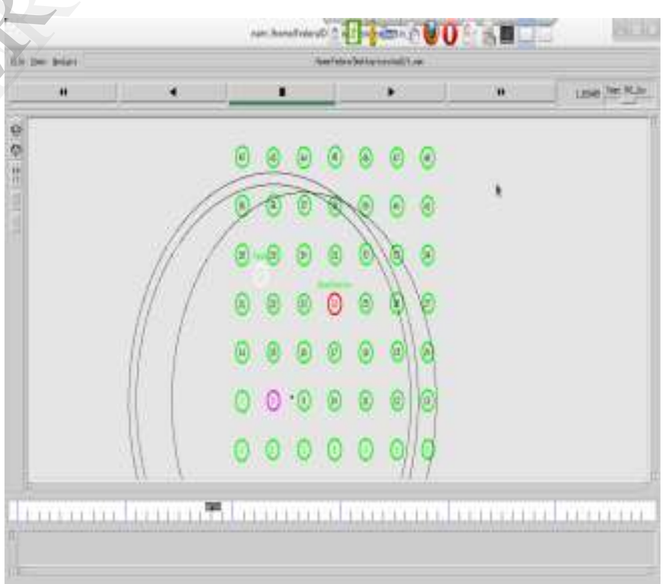


Fig 2

The fig 2 shows the transmission of datas from the nodes to the base station here.In the case of the topology generation ,it will calculate the distance between the nodes before deploying the nodes here.the arrangement of the nodes here will be like this.the above is the transfer of information from each and every nodes to the base station .

In the case of the collection of data's in the periodic manner ,each and every node will send packets in an independent and periodic manner .So the aim is to fool the attacker. Every node will send packets in the periodic manner then it will become difficult to the attacker to analyze which is the original data and which is the fake one. Here in fig 3 and 4 explains the periodic manner of data are given.

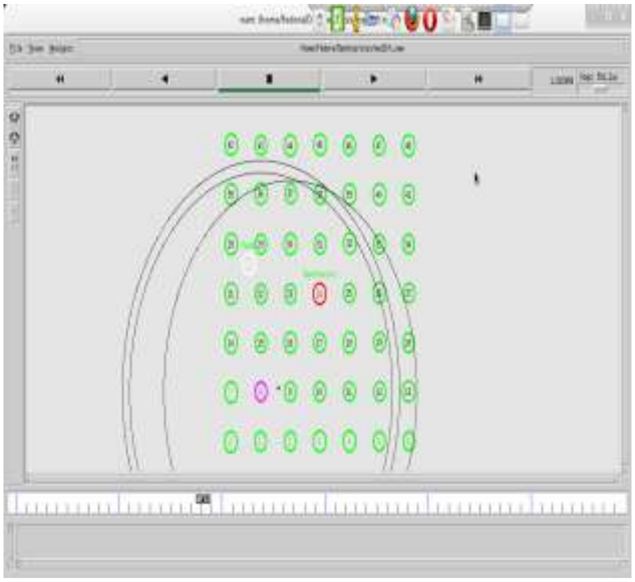


Fig 3

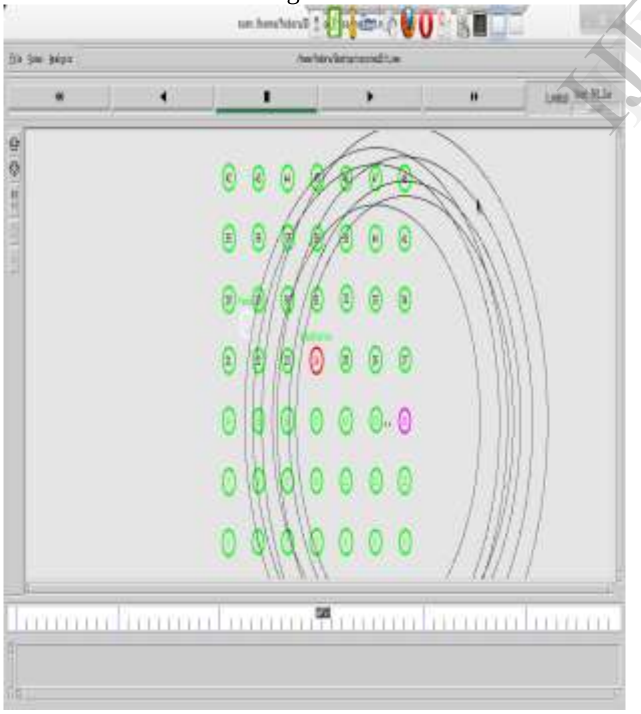


Fig 4

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid

[3] BlueRadios Inc., "Order and Price Info," http://www.blueradios. com/orderinfo.htm,

.

[4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree,"

[5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy