International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Protecting Location Privacy in Sensor Networks against a Global Eavesdropper Using Fake Objects and Fake Sink

Priyanka A. Linge[1], Prof. S. K. Pathan[2]

[1]Department of Computer Engineering Savitribai Phule, Pune University, India

[2]Department of Computer Engineering Savitribai Phule, Pune University, India

Abstract: ***Sensor Networks are employed in several applications e.g. habitat monitoring, military tracking. Whenever sensor networks are used to monitor sensitive objects the privacy of objects location becomes important issue. To safeguard such necessary info, goodly effort in sensor network security has targeted on providing security services like integrity, confidentiality, accessibility, and authentication. These security necessities aren't sufficient in case of location privacy application. The contextual info may be disclosed by the communication patterns of sensors itself. In WSN, sensor data is distributed from sensor node to sink node. This data is sent using comparatively fixed path. The bound traffic patterns are created during this procedure that is analyzed by attacker to search out the placement of either source sensor or sink node. Once attacker is aware of the placement of either source sensor or sink node he will establish the spot of object. Suppressing or hiding the location of object becomes necessary if it's representing a sensitive entity like soldier or an endangered species. Source sensor location privacy and sink location privacy are necessary tasks in an order to stay object safe. During this paper we've got used location privacy techniques together to safeguard the source sensor and sink, successively to safeguard the article from being disclosed. Sensors are low power devices. Very little power is employed for the sensing operation however the most power of sensor is used for transmission and reception of the packets or messages, so communication overhead should be reduced. In this paper we've got targeted on the technique that uses the less variety of packets to cover the location of source sensor and sink and in turn hides location of object.***

Keywords: WSN, location privacy, sink node, object

1. Introduction

Wireless sensor networks accommodate a large number of sensor nodes that incorporates a capability of sensing computing and communication. Applications built using sensor networks can be divided into data gathering and tracking applications or object tracking applications [[1]. In data gathering applications sensor nodes are made to measure the specific environmental variable periodically. These sporadically taken records are sent to base station for additional process. Examples are temperature gathering sensors and smoke detective sensors. In tracking or trailing applications environment is continuously monitored for the presence of signals that are accustomed determine object being tracked. E.g. tracking objects like an automobile. Once sensor nodes are trailing sensitive object like soldier or endangered species the location privacy of objects become a vital issue. The presence of object is reportable by sensor node to sink node. Once these objects are reportable by sensor to sink through sensor network, the path taken by packets creates a trail leading back to source that makes attacker easier to urge data concerning the location of object.

Privacy in sensor network are often categorized into content privacy and context privacy [2]. Content oriented privacy is restricting the attacker from reading the contents of the transmission which is achieved using various cryptographic methods. Though the content privacy is assured, hunter is able to extract the data of object monitored in sensor networks. Contextual privacy on the other hand is bothered with ability of hunter to urge data from examination of sensors and communication pattern. This process can be done by attacker, without accessing the contents of the packets or messages. To search out the position of the object adversary uses the routing path of the packet or communication pattern.

When a sensor networks are used to monitor the precious assets or the sensitive objects, the location privacy in sensor networks becomes necessary. Example watching the movement of soldier in battle field and report the position to the headquarters.

A panda hunter model delineate in [3] can make the location privacy scenario clear. In panda hunter scenario, sensors nodes are deployed within the field. These sensors deployed to track the panda. Whenever a panda moves within the field, its location is sensed by close sensor and these sensor nodes send the message to the base station or sink node. This model assumes that the attacker can eavesdrop on the communication between sensors. Although the communication between sensors is encrypted and hunter will not see the contents of the message still he can analyze path of messages. We've got assumed here that hunter has deployed his own snooping network to watch the transmission of packets in target network. We do not assume that attacker precisely locates the object, only rough idea of event happening is enough for attacker. We are considering the scenario within which hunter will monitor all transmission events in sensor network.

2. Related Work

Location privacy is split into source location privacy and sink location privacy. If source sensor isn't protected the adversary can figure out the sensor node in whose range the item is and successively the adversary can capture the location of the item.

If sink location isn't protected then it's possible that adversary can apprehend the locations of all the objects in the network.

Following are some existing techniques for source location privacy.

P. Kamat et al[3] has given a Fake packet generation Technique. Sender initially notifies a couple of real message to sink and then fake sources are created. These fake sources send the fake messages to the sink at identical time once source sends real message to sink. This creates uncertainty for attacker to spot a source. It's conjointly given a phantom single path routing. This method relies on each flooding and single path routing. In this each packet takes a random path before aiming to the sink. This method increases the safety period of the object.

Yi Ouyang, ZhengyiLe[2] has proposed a Cyclic Entrapment Method(CEM) for location privacy. Loops of sensors are created before the sources send any messages to base station. These loops are preconfigured for sending fake messages.

C. Ozturk, Y. Zhang, and W. Trappe[4], has represented a flooding technique. In this technique source sends a message to base station using various paths. As source uses varied paths for message, it becomes tough for adversary to search out the object location.

Mehta et al[5] has proposed a way Periodic collection. Periodic collection is explained as follows. If object is present in some space the communication pattern therein space changes. Eavesdropper notices these changes that facilitate him to search out the location of object. To resolve this drawback answer is to create communication pattern independent of real object i.e. each sensor node in network ought to send message to the bottom station even though it don't have a data to send. Figure shows the strategy periodic collection.

Following are some existing techniques for sink location privacy.

Jing Deng, Richard Han [6] has proposed some techniques like controlled random walk, multiple parent routing, random fake path and hot spots to beat these attacks. In controlled random walk, random walk of packets is performed into the multi hop route i.e. packets are made to traverse multiple hops in network towards the sink. In, multiple parent routing technique packets is forwarded to at least one of its parents that makes patterns less distinguished just in case of routing messages towards the sink. In random fake path, fake paths are set up to confuse attacker from following the sink. In hot spots [7] technique multiple areas of high activity are introduced to confuse it with base station.

Mehta et al [5] has projected a way Sink Simulation for sink location privacy. During this theme multiple candidate traces square measure created towards the fake sinks. Fake sinks square measure simulated within the field to stay the important sinks safe. Fake sinks can receive the traffic as that of the traffic received by the important sinks.

3. Proposed System

3.1 Proposed System

In projected system we've got combined 2 techniques to cover the situation of object as well as sink. we've got used fake objects[5] and fake sink together[5]. Sensor network will work when some sensor nodes are not working. However if some sink isn't operating the sensor network can collapse. Therefore it's necessary to use these techniques together. Once real object is close to the sensor it conveys this to the sink node using packet. Attacker has its own sensor network to analyze the sensor network used by commander and may see the changes in communication pattern and may establish the location of object. However we are using fake objects here, once sensor has info regarding the important object fake object conjointly sends the packet to the base station. This confuses the adversary regarding the presence of real object. Conjointly we've got fake sink deployed. In periodic collection all the sensors send the packets to the sink node even when only one sensor has object in its range. In this method the overhead is very high. And if in periodic collection methodology if we deploy fake or dummy sink to safeguard the important sink the overhead would be far more.

Sinks are necessary elements of sensor network so protecting sink also becomes necessary. Sink is that place wherever high activity of packets takes place, as a result of all packets are sent to the sink by sensor nodes for processing. Failure of few sensor nodes may be tolerated. However failure of sink node results in the failure of complete sensor network. We are able to use a fake sink within the field. Whenever any sensor nodes send packets to the sink node, they conjointly send the packets to the fake sink node. By making fake traffic in field we are able to confuse attacker regarding the position of sink. Proposed system is represented in figure1.

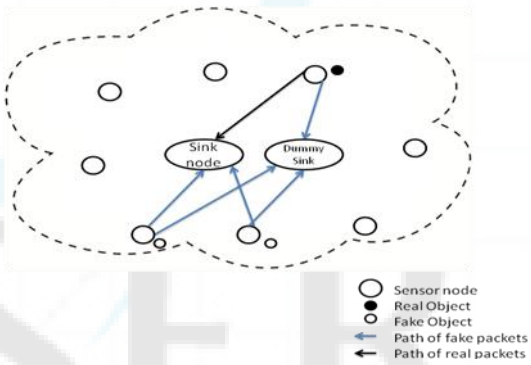


Figure 1: Proposed system

When we use dummy or fake sink to safeguard the sink within the field and the number of fake sinks are significantly more; the huge amount of traffic is generated. In this case we must always cut back the fake sinks accordingly. Actually in real time this sort of situation don't arise because large no of sensors are deployed to track small set of objects. So the amount of overhead in periodic collection remains additional (as the number of sensors is more) than that of the overhead in the fake objects methodology.

3.2 System Architecture

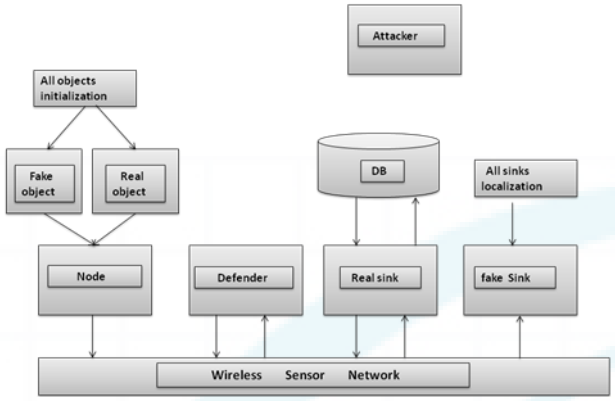


Figure 2: System architecture

System architecture consists of defender or commander who wants to defend the system from the attacker, sensor node, sink node, objects and database as shown in figure 2.

3.3 Algorithm

1. Initialize the sensor network.
2. Initialize the real and fake objects and sinks in the network.
3. Sensors having real object in its range will send the real packet to the real as well as fake sink node.
4. Sensors having fake objects in its range will send fake packet to the real as well as fake sink node.
5. Packets are decrypted at real sink node. The information is sent in the database.
6. Generation of report.

3.4 Mathematical Model

Sensor network can be viewed as graph G={V, E} where V denotes the set of vertices which denotes sink as well as sensor nodes. Source sensor (i.e. Sensor nodes having object in its range) is a small subset of V. Set E denotes all direct communication links.

$V = \{ S_e, S_a \}$

Where S_e denotes sensor node and S_i denotes sink node.

$S_e = \{ S_{ei}, S_{eo} \}$

Where S_{ei} denotes sensor nodes not having objects in its range and S_{eo} denotes sensor nodes having objects in its range. Sensor nodes having objects in its range are also called as source sensors.

S_{eo} is again divided in source sensors containing real objects S_{eir} and source sensors containing fake objects S_{eif}.

Adversary will eavesdrop on network to find the objects. The observation of adversary can be stated as (i, t) where i= sensor id who sent the packet at time t. O_{iT} be the set of all observations of attacker over time T about node i only. Information collected by adversary over entire network is

$O_T = \text{U } O_{i,T}$

where i belongs to V which is set of all sensor nodes including sink.

The objective of attacker is to know the set S_{eir} C V of source sensors. S_{eir} = set of sensor nodes in whose range the real object is expected to present at time T. The presence of an object must generate a trace, set of observation i.e. trace shows path between sensor node and sink node. S_a set of all sink nodes. We can say that for each source i, which belongs to set S_{eir}, there must be a subset of sinks K C S_a and also set of observations $A_{i,K}$ C O_T that are generated due to communication from node i to sink K. Such set of observations is called as candidate trace. We can also define Candidate trace as any subset of attacker's observation that could be the result of source sensor sending packet to the base station. For attacker to check whether a set of observation is a candidate trace we have a pattern analysis function

$f: 2^{Ö}{}_t \rightarrow I \text{ U } \{\phi\}$

$Ö_T$= set of all possible observations $Ö_T$={(i, t)} . This pattern analysis function is used to output the ID of possible source sensor. If the set of observation is candidate trace otherwise it returns ϕ .

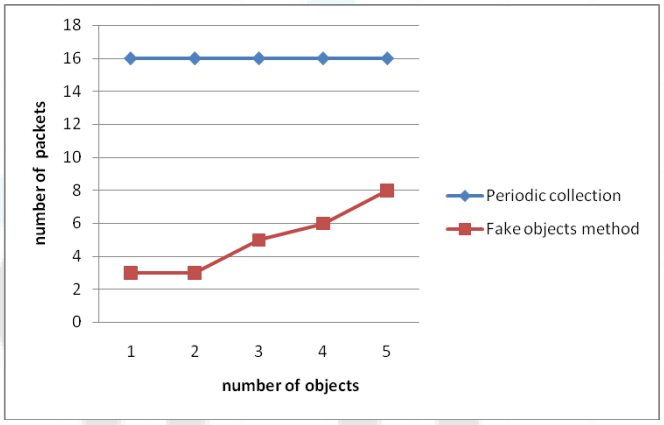
Using the pattern analysis function will have

S_{eir}={i/Ɔ $A_{i,K}$ C $O_{T,}$ K C S_a, (i= $f(A_{i,K})$)}.[kiran mehta]

But as we are using fake objects to prevent real object the pattern analysis function will return

S_{eir} U S_{eir} .

4. Results



Here results are obtained between the number of objects and number of packets produced to keep the object safe. From the graph we can see that the number of packets used in periodic collection is graeater than that used in fake objects method.

5. Conclusion

Here we have seen why location privacy is needed. Necessity of location privacy in some areas is of high importance. While protecting location of object keeping overhead less is also important concern. In this paper we have used two location privacy techniques in combination in an order to keep both

object as well as sink protected. There are varieties of directions that worth studying such as method which still provide location privacy when subset of sensor nodes is compromised by attacker.

References

[1] Siddharth Ramesh, "A Protocol Architecture for Wireless Sensor Networks"
[2] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks" Proc. Int'1 Conf. World of Wireless, Mobile, Multimedia Networking(WoWMoM'06), June 2006
[3] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing, " Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05), June 2005.
[4] C. Ozturk, Y. Zhang, and W. Trappe, "Source- Location Privacy in Energy-Constrained Sensor Network Routing, " Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.
[5] Kiran Mehta, Donggang Liu, Member, IEEE, and Matthew Wright, Protecting Location Privacy in Sensor Networks against a Global Eavesdropper. IEEE Transactions on mobile computing, vol.11, no.2 February 2012.
[6] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.
[7] J. Deng, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks, " Pervasive and Mobile Computing J., Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

Author Profile

Priyanka Linge is student of Master in Engineering [Computer Networks] Department of computer Engineering, Smt. Kahsibai Navale College of Engineering, Savitribai Phule Pune university, Pune, India

Prof. S. K. Pathan is Professor at Department of computer Engineering, Smt. Kahsibai Navale College of Engineering, Savitribai Phule Pune university, Pune, India