Mitigating Hotspot Locating Attack in Wireless Sensor Network

Basavarajeshwari[1], M. Jitendranath[2], I Manimozhi[3]

M. Tech, CNE, CMRIT[1]

Associate Professor, CSE, CMRIT[2]

Professor and Dean, CSE, CMRIT[3]

Abstract: ***In wireless sensor network monitored objects can be located by using traffic analysis techniques. Whenever sensors are used to monitor sensitive objects, the privacy of monitored objects' locations becomes an important concern. In case of hotspot locating attack, it becomes easier for the adversaries to locate the area from which large numbers of packets are originating called as hotspot, causing the inconsistencies in the network. In this paper we develop a realistic adversary model which can monitor multiple parts of the network and can analyse the traffic in those areas. Next we propose a cloud based privacy preserving scheme by creating fake traffic of irregular shape which provides an efficient mechanism to protect the source node's location in addition to that we also generate the fake event at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network. Next we are introducing the concept of context aware location privacy where the sensor nodes are having the ability to perceive the presence of adversary in their vicinity in order to transmit data packets in more energy-efficient manner. Simulation and analytical results demonstrate that our scheme can provide stronger privacy protection***

Keywords: Anonymity, Context privacy, Context awareness, Fake event, Source location privacy preserving scheme.

1. Introduction

Wireless sensor network consist of small, multifunctional and resource constrained sensors. Their low cost provides a means to deploy large arrays of sensors in a variety of conditions performing military and civilian tasks. Each sensor node acts as information source from which sensed information is collected. Advances in wireless network technologies have enabled a new generation of massive scale sensor networks suitable for a range of commercial and military applications. Whenever sensor node detects an object it may be soldier in military application and endangered animal in case of habitat monitoring it reports that event to the sink which is a powerful data collection unit. In this paper we consider habitat monitoring application where the sensors are used to monitor the pandas, for example a WSN have been deployed to monitor the pandas by the save-the-panda organisation. The sensors periodically sense the information of their presence and activities and the sensed data is reported to the sink. However, WSN are located in large and open areas so that providing physical boundary or attending each sensor node becomes almost impossible. While the information is sent from source to the sink through the transmission link, the adversaries can eavesdrop on the wireless medium and can locate the source nodes by making use of traffic information to hunt the pandas. Therefore it is essential to preserve the source node's location because of the easiness of locating pandas and their furs large market value.

There are two privacy threats which can be classified as content privacy and contextual privacy. In the case of content privacy threat adversary can observe and manipulate the packets sent over the sensor network the packets may corresponds to the actual sensed data or may contain sensitive lower layer control information. The content privacy threat can be can be countered by encrypting the packets content and using pseudonyms instead of real identities. Contextual privacy deals with the protection of the context associated with the measurement and transmission of sensed data. The general contextual information such as the location of the message originator, the time at which message is generated etc are sensitive and must be protected. Even if the packets are strongly encrypted the act of packet transmission itself reveals the sensitive information to the adversary.

The existing privacy preserving schemes can be classified as routing based and global adversary based schemes. Routing based schemes uses an adversary model which can monitor very small area in the network and whose monitoring area or overhearing capability is similar to that of the transmission range of a sensor. In this scheme adversary starts from the sink and back traces the hop by hop movement of the packets to locate the origin of the transmitted packets. Routing based scheme uses a mechanism in which packets are sent through different routes instead of single route to preserve the source location privacy. In such scheme it is infeasible for the adversary to trace back the packets from sink to the source as the packets are sent through different routes so that adversary can't receive the continuous flow of packets. However, if the adversary's overhearing range is larger than the sensor nodes' transmission range, the probability of capturing a large ratio of the packets sent from a source node to sink increases significantly.

In the global adversary based scheme the adversary has the capability to monitor the every radio transmission and the links between them. In this scheme it is it is assumed that adversary can monitor the entire network which is unrealistic in large areas. Adversary is having global view of the network means that the attacker can locate pandas without the use of network transmissions.

In this paper, we will first study the hotspot phenomenon, in which large number of packets originates from a small area causing incongruity in the network traffic. The hotspot can be formed when the monitored object for example panda's in high density spend some time in an area due to the availability of food, water or shelter. Next we will develop an adversary model which is having partial view to the network. Adversary model consist of monitoring devices located at different observation points in network, which tries to collects the information like co-ordinates of the sending nodes, the packets content and at which time packet is sent etc. we will study the hotspot attack in which adversary tries to locate the pandas by analysing the traffic information collected by the monitoring devices. Adversary uses the traffic analysis techniques such as time correlations, packet correlations and nodes sending rates to locate the hotspot. Finally we propose our novel scheme in which we create a cloud of fake traffic in addition to that we also generate the fake event at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network to contravene the incongruity in the traffic pattern caused by hotspot to obfuscate the source node within the group of nodes. Here to reduce the energy consumption of transmitting nodes we are using Context-Aware Location Privacy (CALP) approach. CALP takes advantage of sensor nodes' context-awareness in order to detect the presence of a mobile adversary in their surroundings so that packets are routed in a more efficient and privacy preserving manner. The solution aims to anticipate the movements of the attacker in order to minimize the number of packets he is able to capture and analyse, hence reducing the likelihood of the attacker finding the source. Moreover, the protection mechanism will be in operation only when the attacker is moving in the field. Since the network is expected to be free from threats most of the time, the use of CALP translates into a significant reduction of the incurred overhead.

2. Related Works

Location privacy plays very important role in both wired and wireless network. Onion routing [5] technique is used to provide the anonymous communication by hiding the identities of the user.

The scheme in [6] [7] [8] hides the nodes network/MAC address for anonymous communication in mobile adhoc network. The schemes in [9] [10] uses fake packet injection to preserve the location privacy of the sink, where each node is distributed with equal incoming and outgoing number of packets so that the location of the sink is protected.

In [11], deng et al. proposed a scheme in which traffic analysis attacks can be overcome by sending packets at constant rate and are randomly delayed to hide parent-child relationships.

In [2] and [12], routing based schemes are proposed where information is sent through different routes so that back tracking attack is not possible. In this scheme each packet takes random walk to random nodes before it is sent to the destination. However the scheme fails if the adversary overhearing range is more than the sensor nodes transmission range, once the packet is captured in the route, the attacker can know the direction of source node, which reduces the complexity for the attacker to back track the packet to the origin.

Wang et al [13] present a scheme where a weighted random stride routing breaks the entire routing into strides so that time of back tracing the packet to the source is maximised.

Global adversary based schemes [3] [4] assumes that the adversary can monitor the entire network's traffic and each node has to periodically send packets and dummy packets are sent if there is no actual event, so that attacker cant differentiate between real and fake traffic.

In [14], context aware location privacy is used to know the location of the attacker in order to transmit data packets in a more energy-efficient and privacy-preserving manner.

3. Network and Threat Models

This section describes the formal models and assumptions that will be used in this paper.

3.1 Sensor network model

The wireless sensor network consists of sink and large no of sensor nodes deployed in the monitoring area which are having the capabilities to detect a panda. The source node and sink are stationary. The sensor nodes have limited battery power, computation capacity and limited network communication bandwidth. Each sensor node is equipped with sensing device, data processing and communicating components.

The sink has sufficient computation and storage capabilities to perform the functions: 1) broadcasting beacon packets to bootstrap our scheme. 2) Collecting the data sensed by the sensor nodes. Pandas have embedded radio frequency tags and when sensor node senses a panda, the node is called source node which sends event packet to the sink.

3.2 Adversary Model

When the information is sent from source to the destination the adversary can eavesdrop on the channel and can locate the source of the information to determine the location of panda and hunt them. The adversary distributes the number of monitoring devices in the interested region to collect the traffic information in these areas but it cannot monitor the entire network. The adversary is passive and does not involve with the active attacks to remain hidden from the network operator. Each monitoring device consists of spectrum analyser and antenna. The attacker can intercept the packet and can measure the angle of arrival and received signal strength to determine the location of the node. The attacker knows

the location of the sink and can monitor its traffic as it is the destination of the event packets.

4. Hotspot Locating Attack

A hotspot is caused, when from small area large numbers of packets are sent from sensor node which causes irregularity in the network so that attacker makes use of these inconsistencies in the network to hunt the pandas. The following algorithm is used by the attacker to search the panda

Algorithm 1 Hotspot Locating Attack

Start
Monitor the network
Analyse the data gathered
While (does not identify the hotspot), do
Eavesdrop on the communication link by changing the observation point
If hotspot is identified search for pandas
Else
Change the location of the monitoring device
End

The information collected by the adversary in the monitoring phase consist of < Pi, Xi, Yi, Ti> where Pi is the content of the packet, (Xi, Yi) is the co-ordinates of the packet sending sensor node and Ti is the time at which packet is sent.
The traffic analysis techniques such as content correlation, time correlation and packet sending rates are used by the adversary to locate the hotspot in addition to that adversary can know that whenever it receives packets from sensor nodes whether it is fake or real the adversary can conclude that there is a hotspot in the network so that the attacker can hunt the pandas by visiting the expected places like near pond or river etc.

5. Proposed Privacy Preservation Scheme

5.1 Deployment Phase

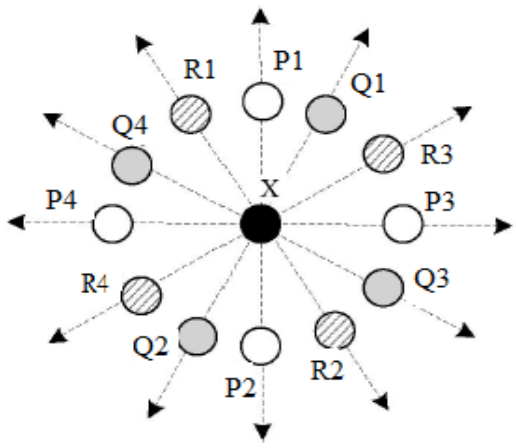

Figure 1: Grouping of Single Hop Neighbours

Each sensor node A is loaded with a unique identity IDA, a shared key with the Sink KA, and secret key dA that is used to compute a shared key with any sensor node using identity based cryptography (IBC) based on bilinear pairing.

5.2 Bootstrapping Phase

After the deployment of the network and before it starts collecting the data the following steps are performed

- Informing the sink about the location of the sensor nodes.
- Fake source node and fake event generator node assignment and finding the shortest route to the sink
- Forming groups that involve in the cloud creation

The sink broadcast the beacon packets, when sensor node receives the packets adds its identity to that and again broadcast the packet. Thus each node can know the shortest route to the sink, in the first received beacon packet. Using localisation techniques the sensor node determines its own location and informs the sink through the shortest path.

To assign the fake source node and fake event generator nodes the node P broadcasts the fake node request packet which contains the maximum number of hops the packet should be propagated. Each node adds its identity and broadcasts the packet if the number of hops is fewer than hmax; otherwise, it unicasts Fake Nodes Request Reply (FREP) packet to node P, containing the identities of the nodes in the route. Node P receives multiple FREP packets containing different routes with maximum number of hops of hmax. It chooses a group of nodes at different number of hops and unicasts the Fake Node Assignment Packets (FASS) to assign them as fake source nodes to its packets. Next, each node groups its single-hop neighbours to send the packets in different directions as shown in figure 1.

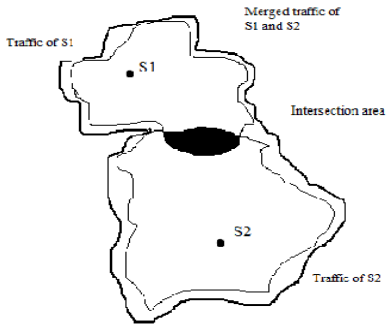

Figure 2: Merged cloud

5.3 Transmission of Sensed Data

In this phase a real source node sends an event packet anonymously to a fake source node to send to the Sink. Simultaneously, a cloud of fake packets is activated to protect the source node's location. In order to make it infeasible to infer a source node's location by analyzing the traffic-analysis information collected from the monitored areas, the nodes of the cloud send fake packets to add randomness to the traffic pattern to

- Make the transmission of the event packet from the real source node to the fake one indistinguishable
- Make the source node indistinguishable by analyzing the packet sending rates of the cloud's nodes.

Instead of using a single path or a single fake source node, the real source node transmits packets through different paths to different fake sources to prevent the linkability between the real and fake source nodes and make packet back tracing infeasible. If the adversary cannot distinguish the traffic belonging to the individual clouds, the clouds can be merged into a larger cloud as shown in figure 2, because the adversary will see the nodes of the merged cloud send one packet in a time interval. Merging of clouds is an important property for hotspots because clouds are very likely intersected which can significantly reduce the number of fake packets and boost privacy protection.

To generate the fake event, the fake event generator nodes are configured to generate the fake event at particular time intervals, here the fake event generator nodes generates the fake event and sends anonymously to fake source node and from there it is sent to the sink. The sink can know whether the message is coming from the real source node or fake source node. The advantage of generating fake event is that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network.

5.4 Context Aware Location Privacy

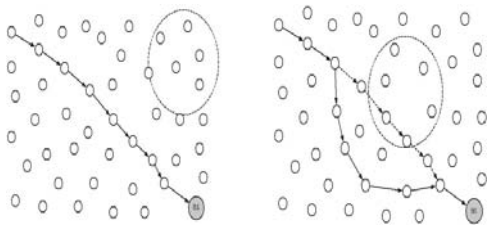

Figure 3: Route adopted according to the presence of adversary

The underlying idea of CALP is to anticipate the movements of the attacker in order to decrease the number of packets he might capture and thus reduce the probability of the attacker finding the source node. To that end, it is necessary to take advantage of the ability of sensor nodes to perceive the existence of moving objects in their vicinity. Upon the detection of such an event, nodes react by broadcasting a route update message to its neighbouring nodes. This message might be forwarded several hops from the position of the attacker and thus it allows sensor nodes to modify their routing tables in order to circumvent the region under the control of the adversary.

Upon the detection of an adversary in the proximities of the network, the privacy preservation mechanism is triggered. The sensor nodes noticing the presence of an adversary inform their neighbouring nodes about this situation in order to prevent packets from traversing the area where the adversary is located. The path is taken based on the presence of the attacker as shown in figure 3.

6. Simulation Results

The experiments were carried out using NS-2 as the simulation tool NS-2 is a discrete event network simulator which provides a detailed model of the physical and link layer behaviour of a wireless network. The scenario is set up in a topology of 3000 m X 3000 m area, where 5000 nodes are randomly deployed.

The Sink is located at the centre. The nodes' radio transmission radius is 50m, and the monitoring devices' overhearing radius is ε_v x50 m. The network has one hotspot that is randomly located and fixed during each simulation run, and the number of source nodes in the hotspot is 35. The number of monitoring devices is Nm. The simulation parameters are listed in table 1

We consider two metrics called the detection probability and the false positive probability. The detection probability is the probability that the adversary can locate the hotspot during the simulation time. It is measured by the number of times the adversary could locate the hotspot to the total number of runs. The false positive probability is the probability that the adversary falsely identifies an area as a hotspot. It is measured by the number of times the adversary falsely identifies an area as a hotspot to the total number of times the adversary suspects that an area is a hotspot. The decrease of the detection probability and the increase of the false positive probability are indicators for providing high-privacy protection for the hotspot.

The simulation results given in Tables 2 and 3 demonstrate that the false positive probability decreases and the detection probability increases when the monitoring devices' overhearing radius increases.

In our scheme, the powerful adversary who has a large number of monitoring devices with large overhearing radius will not locate hotspots. We found that in the runs that the adversary could be close to the cloud, he could not conclude information about the location or the direction of the hotspot in the cloud.

We have also plotted the graph showing that as the number of fake sources increases in the network the cloud size also increases as shown in figure 4, and increase in the number of fake source nodes also results in the consumption of more energy as shown in figure 5.

7. Conclusion and Future

In this paper, using realistic adversary model we have introduced a novel hotspot locating attack, and we also proposed a novel scheme for preserving the location of the hotspot by creating traffic of fake packets and sending packets through different routes and packets appearance is changed at each hop. We also generate the fake event at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network. Our simulation results

have shown that the proposed system is more efficient than routing based and global adversary based schemes.
In our future work, we will try sophisticated approaches to locate hotspots with low false positive probability. We will use computer-based image recognition algorithms in addition to the proposed traffic-analysis techniques. In other words, we will use these algorithms to locate hotspots in the traffic-pattern image created by the traffic analysis techniques.

Table 1: Simulation parameters

Parameter	*Value*
Number of nodes	5000
Network size	3000m X 3000m
Number of hotspot	1
Sensor nodes in the hotspot	35
Sensor nodes transmission range	50m
Attackers hearing range	ε_r X 50m
Location of sink	Center
Number of monitoring devices	Nm
Event transmission rate	1/30 sec

Table 2: False Positive Probability

Scheme	Nm	4			8		
	ε_r	1	2	4	1	2	4
Shortest Path		0.22	0.18	0.08	0.14	0.09	0
Phantom	Hw=4	0.24	0.15	0.1	0.12	0.07	0.01
	Hw=8	0.32	0.23	0.18	0.2	0.1	0.05
Our Scheme		1	0.98	0.93	0.97	0.92	0.9

Table 3: Hotspot Detection Probability

Scheme	Nm	4			8		
	ε_r	1	2	4	1	2	4
Shortest Path		0.71	0.78	0.92	0.82	0.93	0
Phantom	Hw=4	0.41	0.47	0.6	0.5	0.73	0.8
	Hw=8	0.32	0.43	0.59	0.45	0.69	0.79
Our Scheme		0	0.04	0.1	0.05	0.13	0.21

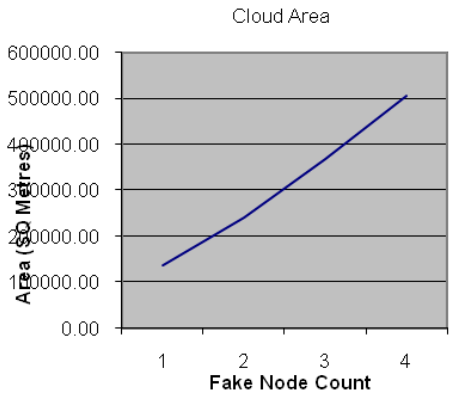

Figure 4: Cloud area Vs Fake node count

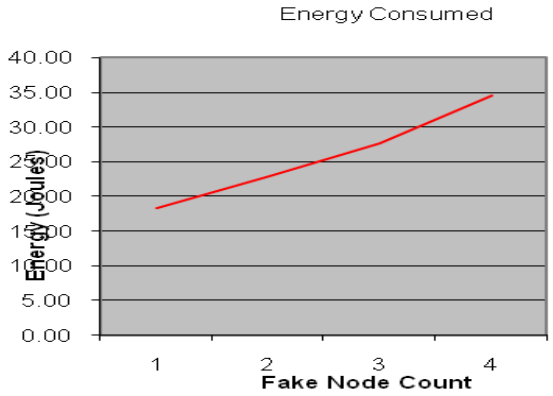

Figure 5: Cloud area Vs Energy Consumed

References

[1] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE "A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 10, October 2012

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source Location Privacy in Sensor Network Routing," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '05), pp. 599-608, June 2005.

[3] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks," Proc. IEEE INFOCOM '08, pp. 51-59, Apr. 2008

[4] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks," Proc. First ACM Conf. Wireless Network Security (WiSec '08), pp. 77-88, Apr. 2008

[5] C. Karlof and D. Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures" In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.

[6] M. Mahmoud and X. Shen, "Lightweight Privacy Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks," Proc. IEEE INFOCOM '11-Int'l Workshop Security in Computers, Networking, and Comm. (SCNC), pp. 1006-1011, Apr.2011.

[7] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[9] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Networks," IEEE Trans. Wireless Comm., vol. 7, no. 10, pp. 3769-3779, Oct. 2008.

[10] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting Receiver-Location Privacy in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.
[11] J. Deng, R. Han, and S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," Proc. Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm), pp. 113-126, Sept. 2005.
[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04), pp. 88-93, 2004.
[13] H. Wang, B. Sheng, and Q. Li, "Privacy-Aware Routing in Sensor Networks," Computer Networks, vol. 53, no. 9, pp. 1512-1529, 2009.
[14] Ruben Rios and Javier Lopez "Exploiting Context-Awareness to Enhance Source-Location Privacy inWireless Sensor Networks" The Computer Journal, Vol. 54 No. 10, 2011

Author Profile

Ms Basavarajeshwari is presently doing Master of Technology in computer networks and engineering in CMR Institute of Technology, Bangalore Karnataka. She obtained the Bachelor of Engineering degree in computer science and engineering from Rural Engineering College, Bhalki, Karnataka, India in the year 2011.

Mrs. I Manimozhi is presently working as Associate Professor, CMR Institute of Technology, Bangalore

Dr. M. Jitendranath is double doctorate in Electronics and Computer Science Engineering and working as Professor and Dean of Research in Computer Science Engineering department in CMRIT, Bangalore. He has published 35 papers in the area of Mobile ad hoc Networks international journals.