IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. V (Mar.-Apr. 2017), PP 80-83
www.iosrjournals.org

Protecting Location Privacy in Sensor Networks against a Global Eavesdropper

Radhika Shetty D. S. [1], Roopa G K[2]
[1]*Computer Science and Engg., Vivekananda College of Engg. & Technology, Puttur, India*
[2]*Computer Science and Engg., Vivekananda College of Engg. & Technology, Puttur, India*

Abstract: *While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can defeat these existing techniques. This paper 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 two techniques to provide location privacy to monitored objects (source-location privacy)—periodic collection and source simulation—and two techniques to provide location privacy to data sinks (sink-location privacy)—sink simulation and backbone flooding. These techniques provide trade-offs between privacy, communication cost, and latency. Through analysis and simulation, will demonstrate that the proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.*
Keywords: *Global Eavesdroppers, Location Privacy, Protection in WSN,WSN*

I. Introduction

A wireless sensor network (WSN) typically consists of a large number of small, multifunctional, and resource constrained sensors that are self-organized as an ad hoc network to monitor the physical world. Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking.

For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. Location privacy is, thus, very important, especially in hostile environments. Failure to protect such information can completely subvert the intended purposes of sensor network applications[1]. Since communication in sensor networks is much more expensive than computation, we use communication cost to measure the energy consumption of the protocols.

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. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have imited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. We need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes. This paper focus on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic

II. Existing Approaches

T.Wang in his work **"Supporting Anonymous Location Queries in Mobile Environments with Privacy grid" [2]** proposed K-anonymity to protect location privacy. His work focused on methods to provide query results with minimum for K users, so it is hard to infer privacy information of individual users.

P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk in their work "**Enhancing Source-Location Privacy in Sensor Network Routing"[3]** proposed to increase the safety period, i.e., the number of messages sent by the source before the object is located by the attacker. This scheme provides decent privacy against a local eavesdropper.

The flooding technique proposed by **C. Ozturk, Y. Zhang, and W. Trappe**, in their work **"Source-Location Privacy in Energy-Constrained Sensor Network Routing"[4]** used flooding technique which has the source node send each packet through numerous paths to a sink, making it difficult for an adversary to trace the source. However, the problem is that the destination will still receive packets from the shortest path first. The adversary can thus quickly trace the source node using backtracking.

Cyclic entrapment proposed by **Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon** in their work "**Entrapping Adversaries for Source Protection in Sensor Networks,"** [5]creates looping paths at various places in the network to fool the adversary into following these loops repeatedly and thereby increase the safety period. **Yang** in his work **"Towards Event Source Un observability with Minimum Network Traffic in Sensor Networks"[6]** proposes to use proxies to shape the network traffic such that global eavesdroppers cannot infer the locations of monitored objects.

Shao in his work "**Towards Statistically Strong Source Anonymity for Sensor Networks"[7]** proposed to reduce the latency of real events without reducing the location privacy under a global eavesdropper. This technique ensures that the adversary cannot determine the real traffic from statistical analysis.

The work mentioned in survey has a common problem. All these techniques assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify the region exhibiting a high number of transmissions to locate the sink. We, thus, focus on privacy preserving techniques designed to defend against a global eavesdropper.

III. Protecting Location Privacy

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. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. We need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes. This paper propose two techniques that hide the locations of monitored objects periodic collection and source simulation and two techniques that provide location privacy to data sinks, sink simulation and backbone flooding.

3.1 Source Location Privacy

This section presents two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency.

Periodic Collection

The primary reason is that the presence of a real object will change the traffic pattern at the place where the object resides. This allows the global eavesdropper to easily find out where the change happens. An intuitive solution is to make the traffic pattern independent of the presence of real objects. To achieve this, we have every sensor node independently and periodically send packets at a reasonable frequency regardless of whether there are real data to send or not.

Specifically, each sensor node has a timer that triggers an event every Ω seconds, as well as a first-in-first-out (FIFO) queue of size q for buffering received packets that carry real data reports. When the timer fires, the node checks if it has any packets in its queue. If so, it dequeues the first packet, encrypts it with the pair wise key it shares with the next hop, and forwards it to that node. Otherwise, it sends a dummy packet with a random payload that will not correctly authenticate at the next hop. Since every sensor node only accepts the packets that correctly authenticate, dummy packets do not enter the receiver's queue. When the queue at a sensor node is full, it will stop accepting new packets.

Source Simulation

Though the periodic collection method provides optimal location privacy, it consumes a substantial amount of energy for applications that have strict latency requirements. It is clearly not well suited for real-time applications. For this purpose, we propose to create multiple candidate traces in the network to hide the traffic generated by real objects. In general, we expect that this number is much smaller than the size of I. In the source simulation approach, a set of virtual objects will be simulated in the field. Each of them will generate a traffic pattern similar to that of a real object.

Source simulation works as follows: before deployment, we randomly select a set L of sensor nodes and preload each of them with a different token. Every token has a unique ID. These tokens will be passed around between sensor nodes to simulate the behavior of real objects. For convenience, we call the node holding a token the token node. We also assume that the profile for the behavior of real objects is available for us to create candidate traces.

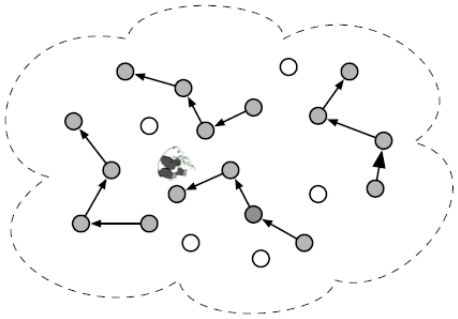

Figure 1: Simulating virtual objects in the field

After deployment, every token node will emit a signal mimicking the signal used by real objects for event detection. This will trigger event detection in the local area and generate traffic as if a real event was detected. The token node will then determine who in its neighborhood (including itself) should run the next round of source simulation based on the behavior profile of real objects. The token will then be passed to the selected node. The delivery of the token between sensor nodes will always be protected by the pairwise key established between them.

3.2 Sink Location Privacy

This section presents two privacy-preserving routing techniques for sink-location privacy in sensor networks: sink simulation and backbone flooding. The sink simulation method achieves location privacy by simulating sinks at specified locations, and the backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks.

Sink Simulation

In sink simulation, fake sinks will be simulated in the field. Each of them will receive traffic similar to the traffic received by a real sink. To achieve this, we make no distinction between fake and real sinks when sensors send packets.

During deployment, we place real sinks and select locations where fake sinks are to be simulated. A subset of the sensors will be used as fake sinks. It is also required that each real sink have a fake sink simulated in its communication range. We will only send messages to the fake sinks and have all fake sinks perform a one-hop broadcast of the message, ensuring full concealment of the real sink locations.

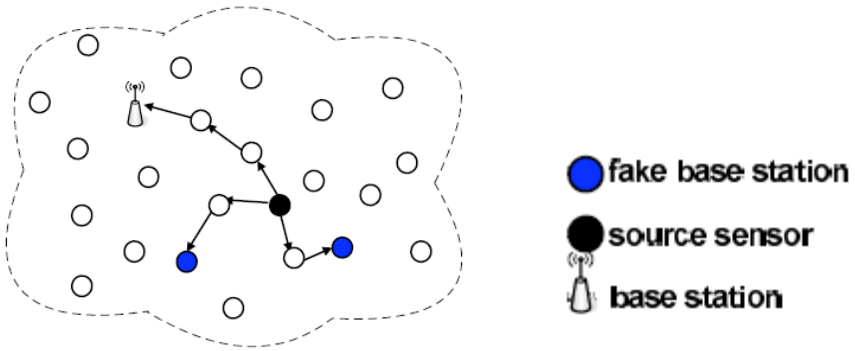

Figure 2: Destination simulation approach

Backbone Flooding

In backbone flooding, we send packets to a connected portion of the network, the backbone, instead of sending them directly to a few sinks. The packets are only flooded among the backbone members, the sensors that belong to this backbone. As long as the real sinks are located in the communication range of at least one backbone member, they can receive packets from any source in the field. Clearly, for a global eavesdropper, the sink could be anywhere near the backbone. We assume that the backbone is created soon after the network is deployed and that the adversary does not eavesdrop until the backbone is created.

IV. Conclusions

Prior work that studied location privacy in sensor networks had assumed that the attacker has only a local eavesdropping capability. This assumption is unrealistic given a well-funded, highly-motivated attacker. We formalized the location privacy issues under the model of a global eavesdropper, and show the minimum average communication overhead needed for achieving certain privacy. We also presented two techniques to provide location privacy to objects and destinations against a global eavesdropper. Analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks

References

[1]. 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, February 2012.
[2]. T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l Conf. World Wide Web (WWW '08), 2008.
[3]. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing" in Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS), June 2005.
[4]. C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN), October 2004.
[5]. Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06), June 2006.
[6]. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards Event Source Unobservability with Minimum network Traffic in Sensor Networks," Proc. ACM Conf. Wireless Network Security (WiSec '08), 2008.
[7]. M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor networks," Proc. IEEE INFOCOM, 2008.