IJSEAT International Journal of Science Engineering and Advance Technology

Privacy Preserving from global eavesdropper in Wireless Sensor Network Using Routing Technique

Himasri.P[1], M.v.b.Chandhra sekhar [2],
[1]Student of M.Tech (CSE) and [2]Asst.Prof in Department of Computer Science Engineering,
AITAM, Tekkali, Srikakulam

Abstract:
Various sensor network security schemes care for the content of messages, while the related information is left defenceless by divulge the location of the monitored objects. Preserving location privacy is essential and one of the largely challenging problems in lots of mission crucial sensor network applications. Previous solutions are principally designed to defend privacy from regional attackers who eavesdrop on traffic in a petite region at a moment. However, they can be effortlessly defeated by abundantly motivated global attackers that be able to trace the entire network's communication proceedings. Although a few topical privacy solutions are proposed adjacent to global attackers, they experience from significant communication transparency as they inject dummy traffic or send messages in a globally synchronized method. As a result, they devour a lot of energy to maintain a required privacy level that craft the network lifetime diminutive. We propose an energy-efficient source location privacy preserving solution, handle the Energy Efficient Location Privacy method beside global attackers (E-LPG). E-LPG hides inventive source locations through a spatial scatter of messages with stealthy wormholes and owing to a temporal scatter using random setback when endorsed With a imperfect number of wormholes, E-LPG can accomplish a high privacy level lacking incurring further communication overhead. We evaluated the effectiveness and efficiency of E-LPG owing to theoretical analysis and general simulations. We have shown that E-LPG also generate dramatic synergistic consequence when used among other privacy schemes accompaniment.

Keywords—*Wireless Sensor Networks, Privacy, location privacy, Eavesdropper, Probabilistic algorithm, Resiliency.*

I. Introduction:

Privacy is one of the largely imperative problems in wireless sensor networks owing to the open disposition of wireless communication, which assemble it very easy for opponent to eavesdrop. Privacy in sensor networks is alienated into two categories: *content privacy*, which disquiet with the comfortable of data packets, and *transactional privacy*, which converge on information about the traffic description (such as carrier message rate, frequency and routing) [1]. Although content privacy can be guard by strapping encryption and authentication mechanisms, sensor networks endure from malicious traffic examination. In this paper, we swot up the problem of location privacy.

A wireless sensor network typically consists of a large number of resource-constrained sensors, e.g. MICA2 motes, and a single base station (BS), e.g. PC-caliber gateway [2]. BS is used to manage and monitor the behaviour of sensor nodes. The failure of BS will lead to collapse of the entire sensor network. An adversary would be eager to locate BS and perform further physical attack. Imagine a sensor network used for military purpose, BS collects information of the battlefield from sensors. If the location of BS is exposed to the enemy, this information channel will probably be destroyed. Thus, BS demands ultimate protection on its location privacy.

There are generally two ways for an adversary to locate BS: *traffic-analysis* and *packet-tracing*. The idea of traffic analysis is that sensors near BS forward a greater volume of packets than sensors further away from BS [2]. An adversary is able to deduce the location of BS based on the traffic densities of various locations. By packet-tracing, an adversary infers a transmission link when he overhears two consecutive packets transmitted by adjacent nodes. Then he performs hop-by-hop tracing towards BS. Packet-tracing attack is more efficient than traffic-analysis attack for the adversary [3]. Therefore, we focus on the countermeasures against the packet-tracing attack. The entire lifetime of a wireless sensor network can be divided into two kinds of operational phases: *topology discovery* and *data transmission* [4]. Most previous work deal with the location privacy in the data transmission period.

However, they ignore the potential threats involved in the topology discovery period. Here we propose an anonymous topology discovery mechanism to eliminate the potential threats in the first period. Besides, we apply fake packet injection to protect the location privacy of BS in the data transmission period. Different from previous fake packet injection approaches, we consider the optimization issue and introduce an intelligent injection scheme to enhance the privacy strength. With the above

two countermeasures, we present a complete solution for the location privacy of BS throughout the entire lifetime of wireless sensor networks. The residue of the paper is controlled as follows. Section II summarizes related work, followed by the statement of models in Section III. In Section IV anonymous topology discovery is described in details. Section V introduces the intelligent fake packet injection scheme. Section VI presents the results of experiments, and then we draw the conclusion in Section VII.

II. Background And Related Works:

location privacy possesses gained a lot more attentions. According to the difference connected with objects protected, previous studies can be divided in two kinds: preserving source location solitude and safeguarding sink position privacy. The main element idea connected with protection is always to confuse your adversary as well as conceal the important location connected with BS in redundant bogus information, including fabricating bogus sources/sink randomly walk as well as fake packet injection. Kamat et 's. designed some sort of routing process called Phantom routing to protect the location privacy connected with source nodes. With Phantom routing, packets randomly walk into a virtual source before the normal delivery. However, Phantom routing cannot protect your receiver's position privacy properly. Additionally, randomly walk prolongs your delivery latency. Deng et 's. proposed Differential Forced Fractal Propagation (DEFP) versus traffic evaluation attack for the location privacy of BS. Multi-path direction-finding and bogus message propagation are released into DEFP. But this specific work concentrates on the traffic-analysis strike, which is not a more suitable measure to have an adversary. Jian et 's. designed the location privacy direction-finding protocol (LPR) to protect the receiver's location]. LPR combines both randomly walk as well as fake packet injection. On the other hand, random stroll brings more packet hold up, and bogus packet injection in LPR is completely random, with no consideration connected with optimization matter. Deng et 's. address the challenge of the best way to hide the location of the bottom station within a sensor network. Techniques connected with multi-path direction-finding and bogus message injection are released. However, the effort concentrates for the traffic-analysis strike, which determines the bottom station's location through the measurement connected with traffic charges at different locations. We have remarked that the traffic-analysis strike takes for a longer time time to identify a receiver compared to packet-tracing strike. The simulation ends up with Section Versus will demonstrate how the method won't perform properly in defending against the packet searching for. Deng et 's. propose another way of protecting the bottom station versus traffic-rate evaluation attacks. The transmission times from the packets are generally randomly delayed so that you can hide your traffic pattern plus the parent-child relationship under a clear traffic pace model. However, this strategy introduces more delay pertaining to delivering packets within a sensor network. Nezhad et 's. considered your privacy problem throughout the topology discovery period as well as proposed an distributed strategy for network topology discovery to protect the destroy location solitude. However, this process has a higher complexity as well as brings more load in order to sensor communities. Privacy matter is widely explored in the field of database, communities, data mining and also other field. Plenty of techniques are generally proposed pertaining to privacy preservation including: Cryptographic protection, Kanonymity. These methods are use to protect data whenever it flows in one node in order to other your figure 1 demonstrates the distinction of solitude preservation troubles in Wi-Fi sensor network [5]. With Phantom direction-finding, packets randomly walk into a virtual source before the normal delivery. However, Phantom routing cannot protect your receiver's position privacy properly. Additionally, randomly walk prolongs your delivery latency.

Figure 1 Classification of the privacy preserving problems for WSN**.**

III. Providing Source And Sink:

Location privacy can be defined as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. In short, control of location information is the central issue in location privacy. Privacy in smart environments has traditionally been related to what is known as social privacy, which refers to the ability of collecting and analysing user data without explicit consent. However, the privacy problem in WSNs has been broadened to embrace network privacy aspects. In this scenario, an attacker might analyse the network

operation in order to retrieve information about the network itself and the data being collected. In the case of social privacy, the owner of the network is usually the privacy perpetrator because height collects user data when the user interacts with the environment. In the network privacy case, the adversary is an outsider who takes advantage of a sensor

Network deployed for legitimate purposes in order to obtain information which was not intended for him. Pai et al. [3] show how much information can be obtained from the network and the environment being monitored by simple observation of the network traffic.

1. The frequency range might reveal the sensor platform being used. In addition, carrier frequency can help to determine the owner of the network, since different frequency bands are assigned for different purposes and organizations.
2. The transmission rate at which messages are being delivered is a good indicator of the quantity and the nature of the events being monitored. The occurrence of events triggers the delivery of messages to the base station. Also, the non-occurrence of events might be an indicator of sensitive information.
3. The size of the packets provides information about the type and precision of the data being collected. In particular, the use of some data aggregation protocols might produce privacy breaches because the nodes receiving a message incorporate their own sensed data into the packet payload, thus increasing the size of the packets. This feature can help an adversary to infer the proximity to the base station.
4. The communication pattern might reveal the network topology. In order to extend battery lifetime, messages are usually transmitted in the shortest path between the source and the destination. Adversaries can take advantage of this knowledge to find out the location of important nodes in the network such as the base station or the sources of messages. Another consideration about privacy in WSNs is made by Kamat et al. in [4]. They suggest that not only the occurrence of an event is important but that also the time at which this event takes place. This concept is named as temporal privacy. In mobile asset monitoring scenarios if an adversary is able to make an association between the time and position of the events being monitored, then he will be able to predict future behaviours. For example, in military scenarios, being in possession of such information can be tremendous advantage in developing more effective plans of attack. Consequently, a large amount of contextual information can be gathered by simply observing the messages being exchanged by the nodes during the network operation. Several techniques have been proposed in the literature for protecting location privacy against global eavesdropper. In location-based services, a user may want to retrieve location-based data without revealing the location.

IV. Problem Definition

Inside previous exploration and research, there assume how the global eavesdropper does not compromise sensor nodes. Even so, in process, the world-wide Eavesdropper may be able to compromise a subset on the sensor nodes from the field and also perform site visitors analysis along with additional expertise from insiders. This specific presents useful challenges for you to methods. But it takes time to the observations made by the adversarial network to succeed in the enemy for analysis and response. Studying the impact connected with such “delayed” analysis and reaction will be another useful research course. And the vast majority of techniques add more energy consumption.

V. Proposed Work:

Much like this analyze we identify some dilemma in problem identification area and that is present within the almost all of the previous methodologies. The major objectives to operate on that area should be to develop a much better techniques when it comes to location privacy against global eavesdropper, energy intake and time taking on the observations of the adversarial network to achieve the foe for evaluation and response. We will certainly propose any enhanced strategy in expression of Better location privacy against eavesdropper using less power consumption and less time come to the observations of the adversarial network to achieve the foe for evaluation and response.

VI. Conclusion:

Prior approaches on location privacy in sensor networks are mostly designed against local attackers and thus, can be easily defeated by highly motivated global attackers. Although a few solutions against global attackers have recently been proposed, they inject fake traffic and/or send traffic in a synchronized manner in order to confuse global attackers and thereby suffer from significant communication overhead and latency. We have presented the Energy Efficient Location Privacy Scheme against Global Attackers (E-LPG) that effectively and efficiently preserves source location privacy. E-LPG uses a limited number of stealthy wormholes to enhance privacy in sensor networks. Wormholes provide a spatial scatter of traffic using hybrid link architecture without incurring any extra communication overhead. We also employed random delays of traffic for a temporal scatter when the applications allowed a controlled amount of delay in message delivery. We have analytically quantified the source location privacy level of our

approaches, and shown how to control the level of uncertainty with a limited budget. We have evaluated the efficiency and effectiveness of E-LPG through extensive simulations with various parameters. E-LPG can be used complementarily with other privacy schemes, and we have shown E-LPG produces dramatic synergistic results in improving privacy when used with a fake traffic injection scheme. As for future work, we are investigating strategic wormhole deployment schemes that improve network resilience and performance while providing location privacy.

VII. Reference

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,—Wireless Sensor Networks: A Survey,‖ Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, —Supporting Anonymous Location Queries in Mobile Environments with Privacygrid,‖ Proc. Int'l Conf. World Wide Web (WWW '08), 2008.

[3] BlueRadios Inc., —Order and Price Info,‖ http://www.blueradios.com/orderinfo.htm, Feb. 2006.

[4] B. Bollobas, D. Gamarnik, O. Riordan, and B. Sudakov, —On the Value of a Random Minimum Weight Steiner Tree,‖ Combinatorica, vol. 24, no. 2, pp. 187-207, 2004.

[5] H. Chan, A. Perrig, and D. Song, —Random Key Predistribution Schemes for Sensor Networks,‖ Proc. IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.

[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, —Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks,‖ Proc. Int'l Conf. Dependable Systems and Networks (DSN '04), June 2004.

[8] 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.

[9] L. Eschenauer and V.D. Gligor, —A Key-Management Scheme for Distributed Sensor Networks,‖ Proc. ACM Conf. Computer and Comm. Security (CCS '02), Nov. 2002.

[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan,—Private Queries in Location Based Services: Anonymizers are not Necessary,‖ Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.

[11] H. Gupta, Z. Zhou, S. Das, and Q. Gu, —Connected Sensor Cover: Self- Organization of Sensor Networks for Efficient Query Execution,‖ IEEE/ACM Trans. Networking, vol. 14, no. 1, pp. 55- 67, Feb. 2006.

Authors:

Paidisetty Himasri is a student of Computer Science Engineering from Aditya Institute of Technology And Management, Tekkali, Presently pursuing M.Tech (CSE) from this college.