Location Privacy against Traffic Analysis Attacks through Mobile Sinks using Trust Value Computing

Nithya Joy
Department of
Computer Science & Engineering
Rajagiri School of
Engineering & Technology
Rajagiri valley, Cochin,
India

Biju Paul
Department of
Information Technology
Rajagiri School of
Engineering & Technology
Rajagiri valley, Cochin,
India

ABSTRACT

We propose a method which provides location privacy against traffic analysis attacks. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be described as the passive attacks that try to deduce the traffic pattern based on the eavesdropped information. They launch an active attack according to the achieved information about the nodes and synchronizing the cooperation of distributed components. Base station location privacy is the important term that is combined with two important concepts defined above .The proposed location privacy method is designed in order to remove the local adversary effect, sinkhole attack and Sybil attack. The network mix ring concept helps in local adversary effect while we have designed mobile sinks against sink hole attack. The Sybil attack is prevented by the trust value computing. In this paper we present our proposed technique with the small experimental setup that helps in further simulation of the technique.

General Terms

Design, Security, Experimentation

Keywords

Location Privacy, Traffic Analysis Attacks, Wireless sensor networks.

1. INTRODUCTION

Wireless sensor networks are considered to be one of the most fully fledged area in the field of research. Since the installation can be done at low price with the easy deployment of the sensor nodes. Wireless sensor networks are wireless asymmetric networks that consist of large number of small resource constrained sensor nodes which communicate over short distances and a small number of relatively powerful base station. Sensor nodes are organized a sensor nodes and aggregator nodes. Sensing node is responsible for sensing data and aggregator node helps to process data from sensing nodes and send results data to a base station. A base station is used to collect data from the entire sensor network and reports the data to an end user. They help in maintaining the network by broadcasting control messages.

The concept of network security is holding equal importance as the WSN as they are susceptible to various attacks due to the simplicity of sensor nodes; dynamic network topology and open medium for communication .Major type of attacks are aiming at the availability of data than the physical integrity of nodes. Traffic analysis attacks[1] are one of the major issues concerned with the security of data passed through the network . Traffic analysis attacks deduce the information from the nodes in a passive manner by monitoring the various parameters of wireless communication. These attacks mostly aim at deducing the location of the nodes mostly the sink node so that the data can be attacked more easily. Once the location have been detected they launch an active attacks such as DoS attack which is considered to critical to the data transferring through network.

The location privacy can be classified as base station location privacy and source location privacy. There are several papers that hold different methods against source location privacy while base station privacy holds equal importance. In this paper we are concerned about the base station privacy. The base station privacy is hampered more when it is located at a definite node remaining static.

The rest of this paper is organized as follows. In section 2, we review some related works. In section 3, we propose some preliminaries, such as base station privacy and attack model. In section 4, we describe the main idea in detail. It includes proposed scheme against three major traffic analysis attacks. And then the experimental setup for the simulation is shown in section 5. Finally, in section 6, we give the conclusion of this paper.

2. RELATED WORK

The location privacy is classified into source location privacy and base station privacy. Phantom routing (PhR)[2] is one of the major technique designed to hide the panda (source) in WSNs. In Phantom routing, the delivery of a packet is done in two steps. Firstly each packet takes a fixed-hop and directed random walk from source node to a random node. The packet is send through routing or flooding. DEFP[3] is a parent-child routing which support fake packet injection mechanism to protect the sink. The real direction of packet flows may be hidden from the adversary by injecting fake packets to the nodes and making the direction of ingoing and outgoing packets uniformly distributed.LPR(Location Privacy Routing)[4] is another routing technique that is based on fake packet injection. GROW(Greedy random Walk)[5] is another source location protection technique based on the method of random routing. Source node generates agents and randomly routes them in the network. To provide global network-wide source location privacy, they propose a Network Mixing Ring (NMR). NMR extends the routing through a random intermediate node. Large ring of nodes is created around the base station to mix messages globally.

The base station privacy is hampered basically by three main types of attacks such as rate monitoring attack, time correlation attack and content analysis attack. Deng at.al[6] found multi parent routing as one of the technique to route the messages by spreading the traffic along multiple paths. Differential fractal propagation (DFP) technique helps in avoiding the problem of large amount of traffic near the base station. A completely randomized scheme was recently proposed by Ngai [7]. In this scheme, a message randomly travels through a network for a predefined number of hops no matter whether it reaches the base station or not. To increase the probability of delivery, multiple copies of the same message can be sent out by the source or a history of already visited nodes can be appended to the message to prevent loops in the routing path. These are some of the basic schemes of location privacy against traffic analysis attacks.

2.1 Traffic analysis attack models:

The concept of location privacy is evolved from context privacy. Typical context-oriented information is information on source location, sink location and timing of event. The adversary effect can be either global or local. The local adversary is limited to radio range and is able to monitor traffic only in a small part of the network at a time while the global adversary is capable of monitoring the whole network at a time and is able to immediately localize all transmitting nodes. The location privacy can be further classified as source location privacy and base station privacy. Here we are mainly providing better methods for base station privacy. Base station collects data from the whole network and therefore the transparency of the data stored in the node is essential for a secure network.Traffic analysis attacks are only based on the monitoring of packets at MAC level or above[8]. Deng et.al [9] [10] identifies three main attacks when considering base station privacy such as:

2.1.1 Rate-monitoring attack:

Rate monitoring attack is based on deducing the packet sending rate between the nodes in a network. The malicious nodes monitors the nodes with larger data transfer rate and thereby identifies the location of the base station. Thus rate monitoring attack is classified as a traffic analysis attack against location privacy.

2.1.2 Time correlation attack:

Time correlation attacks is based on correlation of time between the packets send by a node and its neighbor. The adversary sense the time taken by the node and its neighbor and thereby trace the base station. One of the solution to this attack is delaying the data transfer by buffering the packet for a while before receiving.

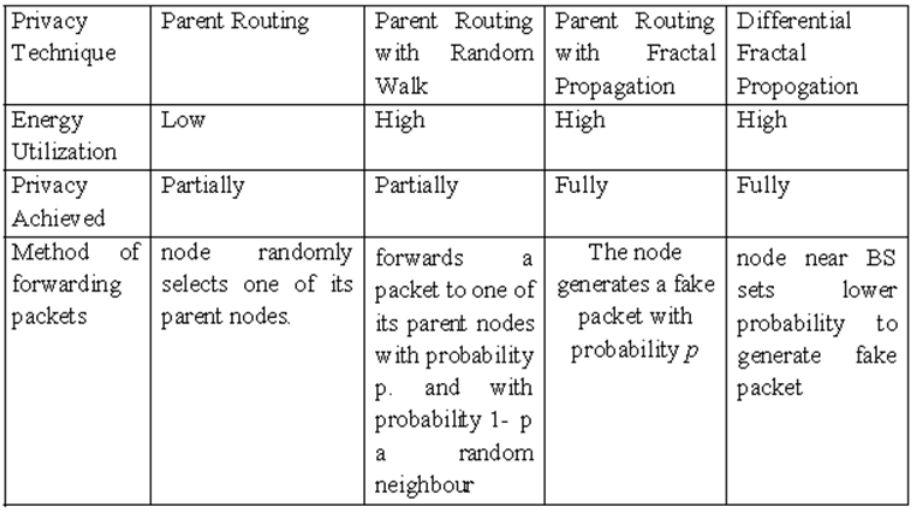
2.1.3 ID analysis attack:

ID analysis attacks is based on deducing the communication relationship between nodes .It is prevented through protecting the IP address.

2.2 Base station privacy:

The base station privacy have been provided by some of the major routing schemes. Which are compared in the below table:

Table 1 : **Comparison of the existing base location privacy techniques**



Privacy Technique	Parent Routing	Parent Routing with Random Walk	Parent Routing with Fractal Propagation	Differential Fractal Propogation
Energy Utilization	Low	High	High	High
Privacy Achieved	Partially	Partially	Fully	Fully
Method of forwarding packets	node randomly selects one of its parent nodes.	forwards a packet to one of its parent nodes with probability p. and with probabilty 1- p a random neighbour	The node generates a fake packet with probability *p*	node near BS sets lower probability to generate fake packet

3. THE PROPOSED SCHEME

The proposed solution is based on network mix ring[11] and trust value computation[12] with mobility of sink[13]. This technique aims at providing the base station privacy with minimum energy utilization. The model works against sybil attack in which a node presents multiple identities to other nodes. Sink hole attacks are another type of internal attack were attackers attracts all the nearby traffic and acts as the base node. A wireless sensor network consisting of a number of sensors deployed in an area, together with one or multiple mobile sink(s). Each sensor has a limited transmission range for wireless communication which allows it to exchange messages directly with its neighboring nodes. Sensors collect data and store them temporarily in the network. The sinks will walk randomly in the field and broadcast occasionally to some local sensors to collect data. Different from moving along periodic paths, the sinks move randomly in the network to collect data. random routing approach can protect the network from local adversaries who overhear and analyze the traffic passively, it cannot defend against active attackers who are able to capture the packets and read the receiver location in the destination field While the sink nodes move and collect data, it protects the data by building up a network mix ring which is a set of continuous-time mixes, each with a public key. The mix decrypts the message send to the mix which contains the next hop information. Initially a random number of nodes are arranged as a ring with session keys set for each node. When a source node sends the data to the sink the data message is divided into two sections. One message send to the base station and the cover message which acts as a protector by passing around the ring. Thus the data is protected against the timing analysis .While the network mix ring is created it is necessary for the sink node to ensure the 'trust value' of the neighbor nodes. Trust value helps in ensuring that the neighbor nodes of the sink from which the data is collected are not corrupted. The trust value is computed by:

$$T_{x,y} = \left[100\left(\frac{S_{x,y}}{S_{x,y} + U_{x.y}}\right) + \left(1 - \frac{1}{S_{x,y} + 1}\right)\right]$$

[.] is the nearest integer function

$S_{x,y}$:total number of successful interactions of node x with y during time δt

$U_{x.y}$:total number of unsuccessful interactions of node x with y during

time δt.

Later the trust is quantized as:

$$M_p(T_{x,y}) = \begin{Bmatrix} trustworthy \; 100 - f \le T_{x.y} < 100 \\ uncertain \quad 50 - g \le T_{x,y} < 100 - f \\ untrustworthy \quad 0 \le T_{x,y} \le 50 - g \end{Bmatrix}$$

f : half of the average values of all trustworthy nodes

g : represents one-third of the average values of all untrustworthy nodes above 100 − f will be declared as trustworthy lower than 50 − g consider as untrustworthy After time, Δt, nodes will recalculate the values of f and g

4. PERFORMANCE ANALYSIS

The experimental setup is done using the popular network simulator such as NS2.The wireless network in our experiments consists 50 randomly deployed nodes with node density 6, i.e., each node has 5 neighbors on average . We assume that all links have the same capacity, and nodes within the interference range share the capacity. In our experiments, we change the following parameters in our experiments:.

Simulaton Parameters	**Values**
Number of nodes	25 to 50
Geographcal area	300 X 300
Packet size(bytes)	64
Traffic type	CBR
Number of malicious nodes	3
Number of mobile sinks	1
Mobility model	Random Way Point
Simulation time	600

We evaluate the performance of our simulation in terms of energy consumption in fig. 4.1 and energy cost in fig. 4.2. We compare our scheme with the DFP (differential fractal propagation) scheme . In DFP,the amount of fake packet generation depends on the fake packet generation[14], whenever a sensor node forwards a real packet, it also transmits a fake packet to a neighbor which is randomly chosen from its further list. This scheme reduces the amount of energy wasted by the sensors when compared to the Fractal propagation. In energy consumption when the number of nodes is fewer, the DFP have been plotted lower than the proposed scheme. But at a denser environment the proposed scheme performs better than the later. Also the end to end delay of DFP increases with the number of nodes. Compared to the proposed scheme the end to end delay is lesser when we use DFP scheme.

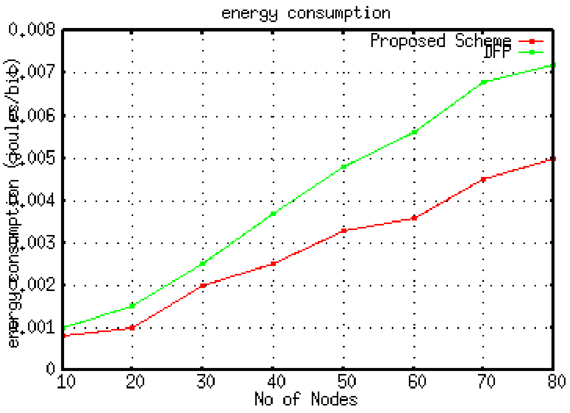


Fig 4.1:Energy consumption vs no of nodes

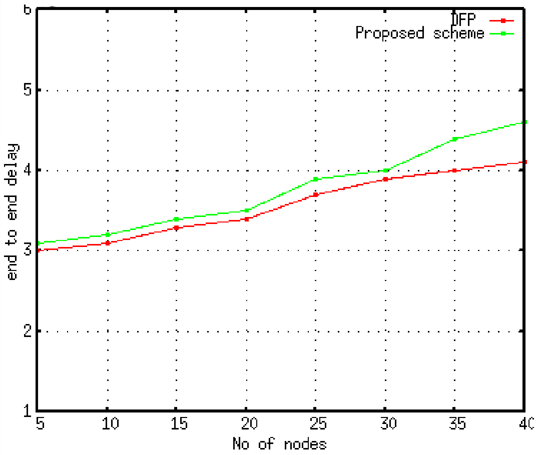


Fig 4.2: end to end delay vs no of nodes

5. CONCLUSION

The proposed scheme provides base station location privacy effectively through the mobile sink managed through trust value provided with a network mix ring. The scheme projects the base station location privacy as it seems to hold more importance than the source location. We have introduced the basic three concepts of the scheme in detail as well as the methodology used to combine then to form a countermeasure.

6. REFERENCES

[1] Raymond, J.F.,"Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems" International Workshop on Designing Privacy-enhancing Technologies pp: 159-186, April 2006.

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing," Proc. of 25th (ICDCS), 2005.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing," Proc. of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)

[4] Y.Jian, Shigang Chen, "Protecting Receiver-Location privacy in Wireless Sensor networks", IEEE INFOCOM 2007

[5] Yong Xi, L. Schwiebert, and Weisong Shi. "Preserving source location privacy in monitoring-based wireless sensor networks". In IEEE International Parallel and Distributed Processing Symposium, Los Alamitos,CA, USA, 2006. IEEE Computer Society

[6] Jing Deng Richard Han Shivakant Mishra, "Decorrelating Wireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks" Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems, vol 2, issue 2, pp: 159-186, April 2006.

[7] Edith C.-H. Ngai. On providing sink anonymity for sensor networks.In IWCMC '09: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing, pages 269-273, New York, NY, USA, 2009. ACM.

[8] R. Bettati, ``Modern Traffic Analysis and its Capabilities'', The NEXUS, Directorate of the Combined Arms Center (CAC) at Fort Leavenworth, Kansas, March 2009 Edition.

[9] J. Deng, R. Han, and S. Mishra. "'Intrusion tolerance and anti-traffic analysis strategies in wireless sensor networks" IEEE 2004 International Conference on Dependable Systems and Networks (DSN'04), Florence, Italy, June 2004.

[10] Jing Deng, Richard Han, and Shivakant Mishra." Countermeasures against track analysis attacks in wireless sensor networks" SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp:113-126, Washington, DC, USA, 2005

[11] Matthew Burnside and Angelos D. Keromytis. "Low latency anonymity with mix rings" Proceedings of the 9th International Information Security Conference (ISC), pp 32–45, June 2006.

[12] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Sungyoung Lee, Young-Jae Song, Heejo Lee, "Network Level Privacy for Wireless Sensor Networks", The Fourth International Conference on Information Assurance and Security, pp.261-266, 2008

[13] Edith C.-H. Ngai , Ioana Rodhe, "On Providing Location Privacy for Mobile Sinks in Wireless Sensor Networks " Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems(MSWiM '09) ,pp: 1 - 6 , 2009

[14] R. Rios, and J. Lopez, "Analysis of Location Privacy Solutions in Wireless Sensor Networks", In IET Communications, vol. 5, issue 17, pp. 2518 – 2532, 2011