Maintaining Trajectory Privacy in Mobile Wireless Sensor Networks

Osman Kiraz
Sabanci University
Istanbul, Turkey
osmankiraz@sabanciuniv.edu

Albert Levi
Sabanci University
Istanbul, Turkey
levi@sabanciuniv.edu

***Abstract*—Mobile wireless sensor networks (MWSN) is a subdomain of wireless sensor networks in which sensors and/or sinks are mobile. In this study, we propose a scheme for providing *trajectory privacy* of mobile sink nodes. The proposed scheme is based on random distribution of data packets. Moreover, sensor nodes do not use location information of the mobile sink or its trajectory. We performed simulation based and analytical performance evaluations for the proposed scheme. The results show that a network with up to 99% data delivery rate can be obtained by appropriate configuration while maintaining a fair level of trajectory privacy of the mobile sink node.**

Keywords—mobility; trajectory privacy; sensor networks

I. INTRODUCTION

The advances in robotics and wireless communication technologies have enabled the development of new architectures for MWSNs which have drawn considerable attention from the research community in the last decade. MWSNs have their own unique properties such as having dynamic mobile network topology. Since sensor and sink nodes are not always in direct communication, sensor nodes should have the data storage capability. These unique properties have brought many new security challenges. As having mobile sink is part of some network architectures of MWSNs, it is also a key player for the applications that are built on these architectures. For some applications, the owner and the user of the network are different. For instance, a set of sensors can be deployed on oceanic area in order to collect data about the geographical properties. The users of this network are oil companies with their own mobile collectors. Since these companies are competitors, they are interested in each other's data collection region. Therefore, the location privacy of the collectors of mobile companies is a security concern. Drastically, the network could be a military one and the mobile collector could be a soldier. The interest of the attacker would be not only the current location of mobile sink, but also the patrolling trajectory. Thus, the keeping the trajectory of the mobile sink secret is a new security and privacy challenge emerged with MWSNs.

In this study, we propose a scheme to maintain trajectory privacy of mobile sink for MWSNs. Although there are some works in the literature addressing the location privacy problem in MWSNs [1 2], to the best of our knowledge our proposed work is the first one in the literature addressing the concern of *trajectory* privacy of mobile sinks. Our scheme relies on homogeneously distributing the sensed data through the network. Our performance evaluation shows that our scheme supplies high data delivery rate (up to 99% for certain configurations).

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under grant 110E180.

II. THE PROPOSED SCHEME

The proposed scheme for preserving the trajectory privacy of sink nodes relies on the random forwarding of the packets and storing the packets in intermediate nodes with a predefined probability. Our scheme does not release any address information of the mobile sink.

A. Threat Model

The threat is basically mote-level such that the attacker cannot hear the direct communication between the mobile sink and the benign nodes, but can deploy it sown malicious sensor nodes into the network. Hence, it may at least be aware of the time and location of the direct communication of the mobile sink with its own malicious sensor nodes. Moreover, a node deployed by the attacker can capture packets and read the contexts of them. The mote-level assumption is fair enough since otherwise analytically no defense system can maintain the privacy of mobile sink node. With this assumption, attacks containing trace routing technique will not be sufficient since the route of a packet does not change with the existence of a mobile sink.

B. Overview of the Scheme

For each data collection phase, the mobile sink randomly selects a trajectory and travels on the selected trajectory with a preset constant speed. It broadcasts a beacon for every T_B, predetermined time for broadcasting beacon, to let the sensor nodes be aware of its existence. Also each sensor broadcasts fake beacons for every T_F, predetermined time for broadcasting fake beacon, with the probability of P_F, probability of sending fake beacon. When a node wants to store a new data packet (either because of generation of the data packet or receiving a forwarded data packet) into its buffer, it checks the volume of the already occupied storage; if it is equal to the buffer size of a sensor node, B, it drops the oldest packet.

When a sensor node generates data D_G, it inserts D_G into its buffer. If L , the maximum number of distinct sensor nodes

that keep D_G in its storage, is higher than 0, then the number of remaining nodes to a keep copy of data, L_R, is set to the L. The information of L_R is part of header of data packet D_G. Then, D_G is forwarded to S_S, the selected mobile sensor node among the neighbor nodes. If L is zero, the mobile sensor node stores the generated data packet but does not forward it.

When an intermediate node receives D_G from a mobile sensor node S_F, it stores D_G with a predetermined probability value of P_s in its buffer and decrements L_R. L_R is not decremented if the data packet is not stored with probability $1 - P_S$. If D_G is stored and L_R is higher than 0, then the mobile sensor node selects one neighbor node S_s among its neighbors except S_F and forwards D_G with (possibly decremented) L_R attached to the header of D_G.

The reason behind not decrementing L_R when D_G is not stored is to maintain a homogenous distribution of D_G in the entire network. By doing so, the delivery probability of D_G increases because if a mobile sensor node does not have chance to interact with the mobile sink node, the closer neighbor nodes may also have no chance to interact. The probability of having an interaction with the mobile sink node and at least one of the sensor nodes at far and different locations is higher. This situation is illustrated in Fig. 1.

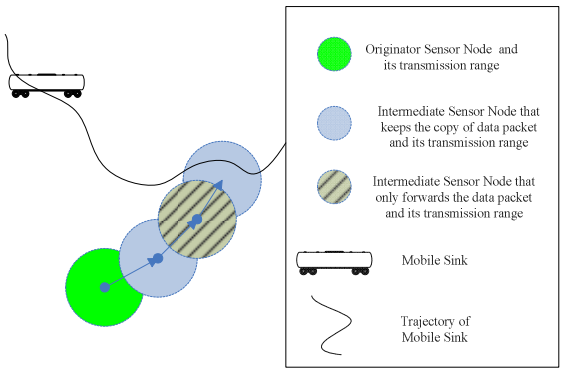

Fig. 1. A local view of data distribution with $L = 2$ and $P_s = 0.5$

III. Performance Evaluation (Some Highlights)

We performed detailed performance evaluation of our scheme using both simulation (Omnet++) and analytical techniques. Due to space limitations in this abstract, we provide some highlights in this section. The meanings of the symbols referred in this section can be seen at Section II.

- Data delivery rate reaches optional value (around 99%) when L values is 10, and remains there up to $L = 20$. Larger L values reduce the data delivery rate ($B = 10$, $P_s = 0.5$).
- P_S values up to 0.5 keep data delivery rate above 98% ($B = 10, L = 10$).
- Communication overhead, in terms of number of forwarded packets, increases linearly w.r.t. L and other parameters. Thus our system is scalable.
- With the value of $P_F = 0.015$, it is possible to fully confuse the attacker with fake beacons. Thus $P_F = 0.015$ is optimal value. This value causes to increase the number of broadcasts in the network 1.5 times.
- In our *Passive Attack* model, an attacker deploys its own static sensor nodes into the network area with its own generated data packets, but do not distribute these packets through the network. In case of receiving a data packet from other nodes, it is processed via proposed scheme principles. Here, interaction with the mobile sink gives exact information about the location of the mobile sink since the attacker's data is not distributed (thus the assumption not forwarding attacker's data assumption is to favor the attacker). We analytically show that in order to learn all the points in the trajectory, the expected value for the total number of malicious nodes that the attacker should deploy is equal to the number of benign nodes in the network. We also show that in a case where partial learning the trajectory, say with rate β where $0 < \beta < 1$, would suffice for the attacker, the amount of the malicious nodes needed to be deployed is shown to be β times the number of benign nodes. Thus, we conclude that our system is fairly resilient against trajectory disclosure attacks.

IV. Conclusions and Future Works

In this study, we motivate a new type of privacy challenge for mobile wireless sensor networks: trajectory privacy of mobile collector nodes. We have proposed an abstract network scheme with no cryptography for this problem. Our scheme is based on introducing randomness in data forwarding and storage in mobile sensor nodes with the aim of achieving homogeneity for data packet duplication.

We have done a set of simulative and analytical evaluation against different metrics to understand the performance of the proposed scheme. The results show that with fine tuning of parameters, data delivery rate reaches up to 99%. The network yields a deterministic and linear communication overhead that can be maintained at desirable ratios. Moreover, we also showed that the proposed scheme fairly resists against the trajectory disclosure attacks.

As future work, we plan to analyze the resiliency of our scheme against traffic analysis and we will also study the resiliency performance of our proposal against an active attack where the attacker uses the disclosed data transferred within MWSN. In this new attack model, to strengthen the attacker, it will be assumed that the attacker would know about the packets with their context that are collected by the mobile sink. With this assumption, attacker would also trace route of its own packets and would learn about if they are collected and know about which sensor nodes have received its packets.

References

[1] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing,", Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), pp. 599–608, 2005.

[2] E. C. H. Ngai, and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks", In MSWiM'09: Proceedings of the 12th ACM international conference on modeling, analysis and simulation of wireless and mobile systems, pp. 116–123, 2009.