This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Reuse-Attack Mitigation in Wireless Sensor Networks

H. Shafiei*†, Ahmad Khonsari*†, B. Mirzasoleiman‡, and Mohamed Ould-Khaoua§
Emails: {shafiei, ak}@ipm.ir, baharan@mehr.sharif.edu, mohamed@dcs.gla.ac.uk
*Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
†School of Computer Science, IPM, Tehran, Iran
‡Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
§Department of ECE, University of Soltan Qaboos, Oman

***Abstract*—Privacy preservation in wireless sensor networks has drawn considerable attention from research community during last few years. Emergence of single-owner, multi-user commercial sensor networks along with hostile and uncontrollable environment of such networks, makes the security issue in such networks of a great importance. This paper concentrates on token-based privacy preservation schemes. A possible attack on such schemes is introduced and two different approaches are utilized to mitigate the attack. Mathematical models for considering the attack effect and overhead are presented and the results are verified using extensive simulations.**

I. Introduction

Wireless sensor networks (WSN) has been recognized as an effective and affordable solution for wide area of today's applications ranging from habitat monitoring to surveillance and target tracking [1]. Various aspects of WSNs have been studied during last decade, however, privacy preservation in such networks has drawn considerable attention from research community only in the course of last few years [2]–[5]. Resource constraints (notably power and computation constraints) along with uncontrollable deployment area of such networks impose unique challenges to the field.

Rapid growth in usage of WSNs makes the idea of constructing large-scale commercial networked sensor system, conceivable. As a result, various environmental projects such as NOPP [6] and IOOS [7] has been emerged. These networks are comprised of sensor nodes deployed in the nature with sensing and observation missions. As the owners of these networks are willing to compensate their costs and also expect return on their investment, they necessitate interested users to pay for every access to each sensor node in order to obtain gathered data. Users may want to keep their access information confidential as the revelation of such information may put their aims and targets in jeopardy. As an example, for oil companies which seek data of interest in a specific region of an ocean, the access privacy is a priority since its disclosure might be very useful to their competitors [8].

So, there exist orthogonal requirements in such systems, on one hand, owners want to enforce access control to the users and on the other hand, users want to protect their data access privacy. While there exists a fairly rich literature on securing WSNs [9]–[11], few research studies have addressed privacy concerns in such networks. The proposed approaches can be categorized into two categories, namely data-oriented and context-oriented privacy protection. In data-oriented privacy protection, the main focus is on preserving the privacy of data i.e., sensed data and queries posed by user. The latter deals with the location and temporal privacy of such networks. Interested readers can be referred to [2] for a brief survey.

A particularly interesting approach for query privacy protection has been introduced in [5]. They introduced a distributed privacy preserving access control scheme for single-owner multi-user sensor networks, called DP^{2}AC. In their proposed scheme, a user can access the data of a sensor node only after spending some previously purchased *tokens* from the owner of the network. Their approach utilized a blind signature technique to hide user's identity from purchased tokens, thus ensuring query privacy. The main issue of concern in such approach is to detect and prevent users from reclaiming their used tokens. They proposed various distributed token reuse detection schemes by using each node as a *witness* for others. They also rigorously analysed each of the schemes and extensively compared them. DP^{2}AC does not concerned with security attacks as it assumes rational behaviour of users.

In this paper, a possible attack on token-based privacy protection schemes is introduced. It has been shown that a malicious user can infinitely reuse its tokens by intercepting the target node. The attack is tended to mitigated by two possible approaches. In the first approach a pairwise security infrastructure between sensor nodes is considered in order to reduce the risk of eavesdrop and thus interception. Then, the effects and overheads of such strategy is studied. In the second approach, a distributed voting system for witnesses is utilized and finally, an extensive simulations are provided to verify the obtained results.

The rest of the paper is organized as follows. First related works are described in Section II. Section III provides some assumptions, describes the model that is used throughout the paper. Two mitigation approaches are introduced and analysed in Section IV. Section V presents extensive simulation results and finally, Section VI provides some concluding remarks and outlines directions of future research.

978-1-61284-233-2/11/$26.00 ©2011 IEEE

II. Related work

Query privacy protection in WSNs has received research interest during past few years. [8] protects clients from untrusted servers using a predefined transformation to fuzzy the target region in order to preserve the privacy of query. In [12] a privacy schema for data and range queries under in-network storage has been proposed. Anonymization-based approaches have been introduced in [13]. Privacy protection of data and query in the presence of compromised sensor nodes has been studied in [2]. However, the concentration of this paper is on possible attacks against token-based privacy schemes, particularly DP^{2}AC.

Privacy protection schema in DP^{2}AC is comprised of three phases [5]. In the initialization phase, network owner creates a pair of RSA keys and publishes the public-key. In the next phase, called withdrawal phase, users purchase tokens protected by a blind signature technique in the sense that network owner cannot associate tokens to the users. In the last phase i.e., token spending phase, each user may acquire data from a sensor node using a purchased token. After being verified using RSA signatures, legitimacy of tokens is checked by a token-reuse detection (TRD) scheme. Various TRD mechanisms are proposed as follows:

- Flooding i.e., each node floods used tokens to others (called update messages), so that they can raise token-reuse (TR) alarm, upon request.
- Randomized, that is, each node chooses some nodes as witnesses and frequently update their lists. Either they raise a TR alarm or (in an enhanced version) some of their neighbours raise it.
- Double-ruling, based on techniques proposed in [14].

III. models and Assumptions

A. System Model

We assume a single-owner, multi-user network of n sensor nodes without any coordination node or base-station. Each sensor node is resource-constrained with maximum radio range $r_{\max}$. We also assume that nodes are deployed according to a stationary point process in a 2-dimensional unit area of size 1 where the average distance between each neighbouring node is $r(n) \leq \bar{r} \leq r_{\max}$ [1]. For the sake of simplicity, we further divide our unit area into $R(n)$ disjoint regions, each of which has radius $\bar{r}$. It is not hard to prove that there are $R(n) = 4\bar{r}^2$ regions, each has at most $n\pi\bar{r}^2$ nodes. Moreover, we assume that there exist a pairwise security infrastructure between nodes using the one proposed in [10]. Each node has at least $\bar{k}$ secured neighbours where $\bar{k} = \alpha n^{\beta}$ and α and β are parameters obtained in [16]. Figure 1 depicts an example of such network.

Attacker is resourceful i.e., it can launch attack without any energy (battery) concern. It also may constitute out-of-band high-bandwidth channel between other malicious nodes in order to collude with those nodes and conduct a system-wide attack to the network.

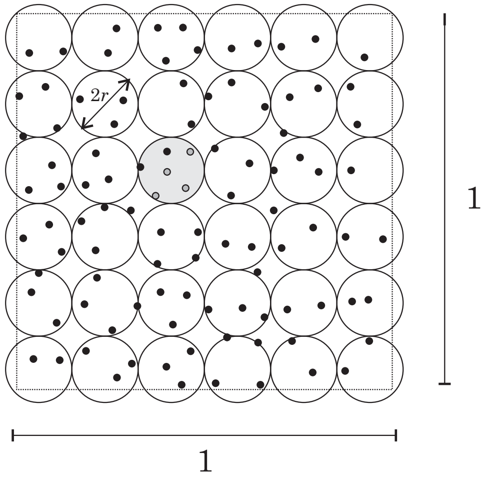

Fig. 1: An example of a two dimensional Secured Random Geometric Graph with radio range $\bar{r}^2$. At most $\bar{k}$ (in this case $\bar{k} = 4$) nodes in their radio range possess a common key

We assume that the amount of energy expanded to transmit a message of unit length to a distance of size $\bar{r}$ far from the sender can be obtained using the following estimation:

$$E_{\bar{r}} = \bar{r}^{\bar{\alpha}} + c \tag{1}$$

where $2 \leq \bar{\alpha} \leq 6$ and c is technology-dependant positive constant. While exact evaluation of c is challenging, a reasonable approximation of c is about 4500 [17].

B. Attack Model

Assuming unattended nature of WSNs, various security attacks can be launched at every layer of each sensor's protocol stack [18]. As there is no general solution for combating various attacks in such networks, we only focus on a specific attack on token-based privacy protection schemes. We assume that the attacker has no intention to capture and read-out the sensors, due to the cost/benefit trade-off. The goal of attacker is to reuse its token as many times as it is possible. To achieve this goal, an attacker may launch *reuse attack*, that is, an attacker may passively eavesdrop on the target node and store its traffic. Upon receiving TRD request, attacker returns a TR alarm. Target node thus considers the token as a reused one. Attacker can simply use the intercepted token without any payment.

C. Performance Metrics

In order to compare each of the proposed approaches with the standard case, we define the following performance metrics[2]:

- **Update overhead** (O_u): O_u is defined as the amount of energy expenditure due to the TRD update phase in

[1] $r(n)$ is equal to the minimum radio range which has been obtained in [15].

[2] We assume that update and request messages are short messages with same energy consumption model.

the proposed approach to the standard case. For example, assume that $E^s_{\bar{r}}$ is energy expenditure in secure TRD update and $E_{\bar{r}}$ is for unsecured case. Then the energy overhead of update is defined as $O_u = E^s_{\bar{r}}/E_{\bar{r}}$.

- **Request overhead** (O_r): This is defined as the total amount of energy expenditure due to the TRD request triggered by a node to the standard case.
- **Detection probability** (p): p is equal to the probability of reuse detection according to the adopted strategy.

IV. Reuse-Attack Mitigation

In this paper we propose two possible approaches to mitigate reuse attacks. These approaches are described as follows. Each approach is followed by analysis of overhead burdened by conducting that approach.

A. Using Pairwise Security

Many research studies have been conducted in order to establish a security infrastructure for WSNs, among which, pairwise security approaches have drawn more attention due to resource constraints of such network [9]. Using pairwise security can effectively reduce risk of interception; however, it can affect some of the important performance metrics in such networks. In what follows we elaborate on the impacts of pairwise security on each of the TRD methods.

1) Secure flooding: We assume that there exist a pairwise security scheme between nodes using random key predistribution method proposed in [10], [11]. A lower bound for the update overhead of using such a security scheme in flooding-based TRD, can be obtained according to the following theorem:

Theorem 1: Assume that $E^s_{\bar{r}}$ is equal to the amount of energy expenditure in secure flooding-base TRD update and $E_{\bar{r}}$ is for unsecured case. Then the energy overhead of update can be approximated by the following bound:

$$O_u \leq \frac{1}{\bar{k}-2}\frac{\alpha}{\pi\bar{r}^2}n^{\beta-1} \tag{2}$$

Proof: See Appendix I. ■

Since TRD requests will be replied locally in flooding scheme i.e., in $O(1)$ hops, the energy expenditure in both cases are equal in average thus, $O_r = 1$. TRD updates are stored in the entire network therefore each request can be replied with probability equal to one if the network remains connected.

2) Random witnesses: In this approach each node selects x witnesses in the network and updates their list. Each node selects its witnesses at the distance greater than half of the network diameter. The energy overhead of update in this case can be obtained as follows:

Theorem 2: Assume that pairwise keys are distributed using expander graphs with second largest eigenvalue λ. The overhead of energy in randomized TRD obeys the following lower bound:

$$O_u \geq \frac{\sqrt{2}}{2}\frac{\log(n-1)}{\beta\log(\alpha n/\lambda)} \tag{3}$$

Proof: See Appendix II. ■

It can be shown that O_r follows the same lower bound. The following theorem provides a lower bound for the detection probability (p) using such scheme in pairwise secured WSNs.

Theorem 3: Assume that each node selects x random nodes as its witnesses and p_f is retrieval failure in each node, the detection probability can be determined by the following bound:

$$p \leq \exp(-\frac{(xp_f-1)^2}{2xp_f}) \tag{4}$$

Proof: Using Chernoff's inequality, the lower bound can be obtained. ■

In the above theorem, p_f is related to the storage size of each node i.e., amount of tokens it can store for TRD detection. One possible solution to improve p_f is to adopt a token replacement strategy, for example, replacement of old tokens with new ones or keeping tokens according to most-recently-used strategy.

3) Double Ruling: Using GPSR [19] routing in pairwise secured WSNs is quite inefficient. In fact, nodes may not possess common keys along a geographic path, which makes geographic information useless and in turn leads to failure in message delivery. Since double ruling directly utilizes GPSR routing, adopting such method in pairwise secured WSNs is beyond the scope of this paper, so we leave it to future works.

B. Using Distributed Voting System

Although using a pairwise security infrastructure reduces the risk of interception however, it is still possible for attacker to establish sophisticated cryptographic analysis due to the symmetric nature of such infrastructure. A possible solution for such shortcoming is using a distributed voting system. Witnesses reply each TRD request; however, the request initiator adopts the result if a certain number of witnesses return a same result.

In a distributed voting system of size n, the obtained result is accepted only if $k \leq n$ participants return the same result where k is a previously known threshold. These systems often called k-out-of-n systems. Such systems have been utilized in WSNs to combat some of the security attacks, such as wormhole and sink-hole attacks [20].

In the aforementioned TRD detection scheme the initiator considers the token as a reused one upon receiving a TR alarm. Attacker can interfere in this system on the following procedure: If attacker extract the key-chain of a target node it can intercept its TRD requests and send back TR alarm to the initiator. The main idea is to adopt a threshold for the number of TR alarms received from different paths beyond which, the target node considers the token as a reused token. In this scheme attackers could still collude and send back TR alarms beyond the threshold, however, it calls for key-chain revelation of numerous sensor nodes, which is quite impractical in real world WSNs. Moreover, the threshold is a user-adjustable parameter i.e., the network administrator can change the threshold according to criticality of the network's mission and environment.