Sensors **2010**, *10*, 2770-2792; doi:10.3390/s100402770

OPEN ACCESS

sensors

ISSN 1424-8220

www.mdpi.com/journal/sensors

Article

Acquiring Authentic Data in Unattended Wireless Sensor Networks

Chia-Mu Yu [1,2], Chi-Yuan Chen [3], Chun-Shien Lu [1,⋆], Sy-Yen Kuo [2] and Han-Chieh Chao [3,4]

[1] Institute of Information Science, Academia Sinica, Taipei, Taiwan;
E-Mail: r91045@csie.ntu.edu.tw (C.-M.Y.); lcs@iis.sinica.edu.tw (C.-S.L.)

[2] Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan;
E-Mail: sykuo@cc.ee.ntu.edu.tw

[3] Department of Electrical Engineering, National Dong Hwa University, Hualian, Taiwan;
E-Mail: chiyuan.chen@gmail.com (C.-Y.C.)

[4] Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, I-Lan, Taiwan; E-Mail: hcc@niu.edu.tw (H.-C.C.)

⋆ Author to whom correspondence should be addressed; E-Mail: lcs@iis.sinica.edu.tw;
Tel.: +886-2-2788-3799#1513; Fax: +886-2-2782-4814.

Received: 10 February 2010; in revised form: 25 February 2010 / Accepted: 16 March 2010 / Published: 26 March 2010

Abstract: An Unattended Wireless Sensor Network (UWSN) can be used in many applications to collect valuable data. Nevertheless, due to the unattended nature, the sensors could be compromised and the sensor readings would be maliciously altered so that the sink accepts the falsified sensor readings. Unfortunately, few attentions have been given to this authentication problem. Moreover, existing methods suffer from different kinds of DoS attacks such as Path-Based DoS (PDoS) and False Endorsement-based DoS (FEDoS) attacks. In this paper, a scheme, called AAD, is proposed to Acquire Authentic Data in UWSNs. We exploit the collaboration among sensors to address the authentication problem. With the proper design of the collaboration mechanism, AAD has superior resilience against sensor compromises, PDoS attack, and FEDoS attack. In addition, compared with prior works, AAD also has relatively low energy consumption. In particular, according to our simulation, in a network with $1,000$ sensors, the energy consumed by AAD is lower than 30% of that consumed by the existing method, ExCo. The analysis and simulation are also conducted to demonstrate the superiority of the proposed AAD scheme over the existing methods.

Keywords: unattended wireless sensor network; UWSN; authentication

---

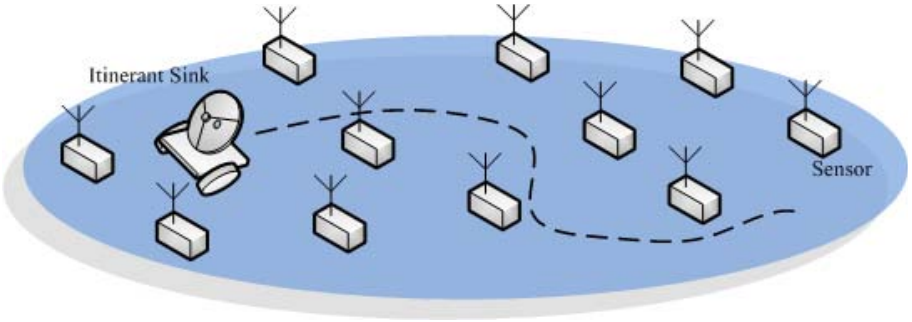
1. Introduction

The use of wireless sensor networks (WSNs) on data gathering applications has been popularized in recent years. Since WSNs could be deployed in the hostile environments, one of the fundamental issues is how to secure the collected data. Unfortunately, with the consideration of the sensors' scarce resources, the security issue becomes very challenging because conventional computationally-intensive cryptographic primitives cannot be utilized.

WSNs considered in the literature are usually assumed to have a constant connection between sensors and a trusted data collection unit, e.g., the sink. From the security point of view, in such a scenario, sensors can collect and then report the sensitive data to the sink at will. With the cryptographic primitives such as encryption and authentication, the confidentiality and authenticity of the transmitted sensed data can be guaranteed. More importantly, this avoid storing a large amount of data in sensors that are easily to be compromised. Even more, with the aid of the always-present sink, the network can defend against the attacks such as sensor compromises more efficiently and effectively. Nevertheless, due to the application restrictions, the above scenario is not always the case. In real world applications, there could be the cases where after the sensor deployment, the sensed data should be temporarily stored in the sensors because the sink is away from the network in most of the sensor network lifetime. Only at the end of each *collection interval*, will the itinerant sink roams around the sensing region and collects the data sensed by sensors. In contrast to the usual sensor networks, to emphasize the unattended WSN feature, this type of WSN consisting of sensors and an itinerant sink that periodically collects sensed data is termed as *unattended wireless sensor networks* (UWSNs). In fact, UWSNs have been used in practical WSN applications [1,2]. In particular, the unattended sensor networks in [1] operate in an unmanned manner. For example, the nuclear emission sensor network could be deployed to monitor potential nuclear activity. In addition, another example is to deploy unattended sensors to detect underground sound and vibration, in order to be aware of troop movements, border crossings, and enemy's aircrafts as soon as possible. Trident systems [2] deploy the unattended ground sensors for providing reliable communication links. It is often used for transmitting timely message back to command and control centers. These sensors can be used in battlefield applications including perimeter defense, border patrol and surveillance, target acquisition, and situation awareness. The conceptional illustration is shown in Figure 1.

Due to its inability to offload the sensed data in a real-time manner, sensors should keep the data sensed in the local memory within the collection interval between successive sink visits, incentivizing various attacks. The adversary may have different goals; it may be interested in learning the data sensed by a specific set of sensors, or want to prevent certain data from reaching the data sink. In this paper, we consider the adversary whose goal is to alter the sensors' data so that the falsified data can mislead the sink. In spite of the paramount importance of this authentication problem, only few solutions [3,4] are proposed. Specifically, in [3], a novel authentication function was proposed to deal with the authentication problem in a storage-efficient manner. Nevertheless, it is effective only against the *reactive adversary* (described in Section 3.2) that is relatively weak and is easily to be overcame. In [4], two collaborative authentication schemes, CoMAC and ExCo, were proposed to defend against the stronger adversary, *proactive adversary* (described in Section 3.2).

Figure 1. In a UWSN, the itinerant sink roams around the sensing region and collects the data sensed by sensors.



Unfortunately, the simple collaboration among the sensors in CoMAC and ExCo incurs more attacks such as Path-Based DoS (PDoS) [5] and False-Endorsement DoS (FEDoS) [6] attacks (described in Section 4.1). In addition, the resilience of ExCo against sensor compromises is not as strong as [4] claims (described in Section 4.1). Furthermore, due to the lack of the proper use of sensors' position information, CoMAC and ExCo have relatively high energy consumption especially in a large scale network. The above reasons motivate us to develop a secure and efficient collaborative authentication scheme in UWSNs.

1.1. Contribution

We identify the security flaws of the schemes in [4]. Aiming at solving the identified problems, a scheme, called AAD, is proposed to Acquire Authentic Data in UWSNs. AAD possesses three characteristics. (1) Due to the proper use of sensors' position information, it is communication-efficient. (2) In addition to acquiring authentic data, AAD is also resilient against both Path-Based DoS (PDoS) [5] and False-Endorsement DoS (FEDoS) [6] attacks. (3) The resilience of AAD against sensor compromises is superior to that in prior works [4]. From analytical and simulation results, the robustness of AAD is demonstrated to be superior to those of CoMAC and ExCo.

2. Related Work

Due to the use of Bloom filter in our proposed AAD scheme, its brief introduction is given in Section 2.1 Then, some related works performed on UWSNs are briefly described in Section 2.2

2.1. Bloom Filter

As a kind of probabilistic data structure, a Bloom filter consists of an array of n bits. Together with k independently and randomly selected hash functions, $h_1, \cdots, h_k$, with range $[0, n-1]$, it is used to represent a set of elements with the support of membership query. Assume that a Bloom filter B is used to represent a set $S = \{s_1, \ldots, s_m\}$ of m elements. To insert an element s_i, the bits $B[h_j(s_i)]$ for $1 \leq j \leq k$ are set to 1. Note that the bit remains unchanged when being already set to 1. To check whether an element x is in the set S, we can check whether the bits $B[h_j(x)]$ for $1 \leq j \leq k$ are all 1's. If and only if they are all equal to 1, x is deemed to be an element of S. The size n of Bloom filter is