Ad Hoc Networks 7 (2009) 1463–1475

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks

Roberto Di Pietro [a], Luigi V. Mancini [b], Claudio Soriente [c], Angelo Spognardi [d,*], Gene Tsudik [c]

[a] Dipartimento di Matematica, Universitá Degli Studi di Roma Tre, Italy
[b] Dipartimento di Informatica, Universitá "La Sapienza" Roma, Italy
[c] Computer Science Department, University of California, Irvine, United States
[d] Equipe Planéte, INRIA Rhône-Alpes, Montbonnot, 38334 Saint Ismier, France

ARTICLE INFO

Article history:
Available online 12 April 2009

Keywords:
Unattended WSN
Data survival
Security
Mobile adversary
Probabilistic analysis

ABSTRACT

Some sensor network settings involve disconnected or unattended operation with periodic visits by a mobile sink. An unattended sensor network operating in a hostile environment can collect data that represents a high-value target for the adversary. Since an unattended sensor can not immediately off-load sensed data to a safe external entity (such as a sink), the adversary can easily mount a focused attack aiming to erase or modify target data. To maximize chances of data survival, sensors must collaboratively attempt to mislead the adversary and hide the location, the origin, and the contents of collected data.

In this paper, we focus on applications of well-known security techniques to maximize chances of data survival in unattended sensor networks, where sensed data can not be off-loaded to a sink in real time. Our investigation yields some interesting insights and surprising results. The highlights of our work are: (1) thorough exploration of the data survival challenge, (2) exploration of the design space for possible solutions, (3) construction of several practical and effective techniques, and (4) their evaluation.

1. Introduction

In recent years, sensors and sensor networks have been extremely popular in the research community. Much of prior research explored various aspects of *Wireless Sensor Networks* (WSNs), including: system architecture, routing, security, power-awareness and data abstraction. In particular, security issues in WSNs have received a lot of attention. One common assumption in prior WSN security research is that data collection is performed in, or near, real time. In other words, a trusted entity (such as a sink) is assumed to be always present. Individual sensors submit their data to the sink either periodically or based on some external trigger, e.g., a change in the sensed environment or an explicit request by the sink.

Another emerging sensor network type involves sensor mobility and opportunistic connectivity among sensors as well as between sensors and the sink [1–3]. This concept is similar to Delay Tolerant Networks (DTNs). It is characterized by sensors' inability to communicate with other sensors, for reasons such as: limited transmission ranges, power constraints or signal propagation problems (e.g., line-of-sight limitations or physical obstacles).

In this paper, we focus on WSN scenarios and applications that do not fit into either the real-time data collection model or the opportunistic DTN-like model. We are interested in *sensor networks* where sensors are connected but there is no real-time communication with the sink. We refer to such networks as *Unattended WSNs* or UWSNs. We narrow our scope even further to UWSNs operating in a hostile – or at least untrusted – environment where the adversary has free reign. Specifically, the adversary has one central goal: to prevent certain data collected by sensors from ever reaching the sink. We elaborate on this below.

* Corresponding author. Tel.: +39 3475802987.
E-mail addresses: dipietro@mat.uniroma3.it (R. Di Pietro), mancini@di.uniroma1.it (L.V. Mancini), csorient@ics.uci.edu (C. Soriente), spognard@inrialpes.fr (A. Spognardi), gts@ics.uci.edu (G. Tsudik).

1570-8705/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2009.04.002

One example of hostile unattended environment could be a network of nuclear emission sensors deployed in a recalcitrant country (under, say, an international treaty) in order to monitor any potential nuclear activity. Another example is an underground sensor network aimed at monitoring sound and vibration produced by troop movements (or border crossings). One can also imagine an airborne sensor network tracking fluctuations in air turbulence and pressure to detect enemy aircrafts. Among the features that unify these examples is the likely presence of a powerful – yet careful – adversary. Informally speaking, we say that the adversary is *powerful* if it can subvert a number of sensors at will, while it is considered *careful* if it wishes to remain undetected in the process. Quite recently, the US Defense Advanced Research Projects Agency (DARPA) initiated a new research program to develop so-called LANdroids [4]: smart robotic radio relay nodes for battlefield deployment. LANdroid nodes are supposed to be deployed in hostile environment, establish an ad-hoc network, and provide connectivity as well as valuable information for soldiers that would later approach the deployment area. LANdroids might retain valuable information for a long time, until soldiers move close to the network. In the interim, the adversary might attempt to delete or modify that information, without disrupting network operations, so as to remain undetected.

In such settings, the greatest challenge is to ensure data survival for long enough that it can be collected by the itinerant sink. Clearly, if the adversary is unable to break into (i.e., compromise) a single sensor or inhibit communication between a sensor and an eventual collector or sink, it has no hope of destroying the data. However, we envisage a more realistic adversary who is aware of the origin(s) of targeted data and is also assumed capable of compromising any sensor it chooses, up to a specific threshold (fraction or absolute number) of sensors, within a certain time interval. This type of adversary has been studied in the cryptographic literature where it is usually referred to as a *mobile adversary* [5]. An entire branch of cryptography, called *proactive cryptography* has been dedicated to developing cryptographic techniques (e.g., decryption and digital signatures [6,7]) that remain secure in the presence of a mobile adversary. Although our adversary models are similar, the UWSN application domain is very different from that in proactive cryptography (as described below), thus motivating radically different solutions.

Scope. This paper represents the very first attempt to develop cryptographic defenses for coping with a focused mobile adversary in UWSNs. However, as becomes clear throughout, this paper **does not** address a number of important problems. This is partly because of space limitations and partly due to the novel nature of the topic and problem at hand. We expect that this paper will result in follow-on investigations on our part as well on the part of the research community.

We also stress that our work is oriented towards sensor networks and is not particularly novel in terms of cryptography. Its novelty stems from applying well-known and accepted cryptographic tools to solving a novel networking problem.

Our Contributions. This paper provides the following contributions:

1. *Problem exposure:* although some recent work [8] first brought the problem to light, it focused on trivial and intuitive data survival strategies. In contrast, the present work delves much deeper into the problem and constructs effective and efficient countermeasures that achieve our main goal of maximizing data survival in UWSNs in the presence of a powerful mobile adversary.
2. *Novel techniques and analysis:* we thoroughly explore the design space of cryptographic solutions and – without resorting to expensive and/or exotic techniques – develop several practical and optimal (or near-optimal) data survival strategies. Our investigation yields some interesting results; for instance, when using public key cryptography, continuously moving data around the network provides the same security of combining the following techniques: moving data just once, plus re-encryption. Further, our evaluations of proposed techniques demonstrate a surprising degree of data survival even when the adversary is very agile and powerful, while the sensor network remains unattended for a relatively long time.

Organization. Section 2 introduces our environment assumptions. Then, Section 3 explores potential data survival strategies for the UWSN, adversarial counter-strategies and a number of design parameters. Section 4 investigates encryption–related issues and parameters. Section 5 presents our analysis. Next, Section 6 overviews relevant prior work. Finally, Section 7 provides a summary and some directions for future work.

2. System assumptions

In this section we present our assumptions about the sensor network environment and the adversary.

2.1. Network environment

We envisage a UWSN which operates as follows:

- Sensors are programmed to sense and collect data periodically. There is a fixed global periodicity parameter p denoting the time interval between successive sensing operations.
- Each sensor collects a single unit of data for each interval. In an UWSN composed of n sensors, we say, sensor s_j collects data d_j^r for interval r.
- The network is unattended. There exists a parameter q ($q = v * p$ for some integer v) which denotes the maximum time between successive visits of the sink or collector—we use the term sink from here on to mean both.
- As soon as each sensor off-loads its accumulated data to the sink, it erases its entire storage. Moreover, the sink re-initializes all sensors' secret material upon each visit. In other words, any secret values held by a sensor right before the sink visit are completely independent from those held after the visit.