Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 6 (2008) 1031–1050
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Secure localization with phantom node detection ☆

Joengmin Hwang *, Tian He, Yongdae Kim

Department of Computer Science and Engineering, University of Minnesota, 4-192 EE/CS Building, 200 Union Street SE, Minneapolis, Minnesota 55455, United States

Received 15 March 2007; received in revised form 5 October 2007; accepted 22 October 2007
Available online 9 November 2007

Abstract

In an adversarial environment, various kinds of attacks become possible if malicious nodes could claim fake locations that are different from their physical locations. In this paper, we propose a secure localization mechanism that detects existence of these nodes, termed as phantom nodes, without relying on any trusted entities, an approach significantly different from the existing ones. The proposed mechanism enjoys a set of nice features. First, it does not have any central point of attack. All nodes play the role of verifier, by generating *local map*, i.e. a view constructed based on ranging information from its neighbors. Second, this distributed and localized construction results in strong robustness against adversaries: even when the number of phantom nodes is greater than that of honest nodes, we can filter out most of the phantom nodes. Our analytical results as well as simulations under realistic noisy settings demonstrate that the proposed mechanism is effective in the presence of a large number of phantom nodes.

Keywords: Sensor networks; Localization; Secure localization; Location verification; Speculative algorithm; Decentralized algorithm

1. Introduction

With thousands of tiny devices, Wireless Sensor Networks (WSNs) can support ubiquitous surveillance with a very low profile, which can be quickly deployed without infrastructure. These features make them attractive for a wide variety of applications such as environmental and habitat monitoring [36], surveillance and tracking for military [13], emergency response and structural monitoring [40]. Networked sensors can monitor the behavior of animals in wildlife. It may be used to detect smoke in forest to indicate a fire. The passage of soldiers or tanks of enemy can be monitored. In such mission, common queries accompanying the detection of the events are, for example, ''where are the detected animals?'', ''where is the fire?'', and ''where is the enemy?'' To answer these questions, a sensor node needs to know its location in deployment area. When we are interested in only a certain area, we can query only nodes in a certain geographical area. In addition, knowledge of node location can be used to

☆ The abbreviated version of this paper is presented in [16]. This paper provides a set of extensions and improvements. We added the state of the art about the related works, and describe the limitation of conventional approach in detail. Importantly, a new atomic commit protocol is proposed to deal with collusion attack. We also reveal the detrimental effect of the collinear pivots. The analysis and extended evaluation is added.

* Corresponding author. Tel.: +1 612 532 0845.
E-mail addresses: jhwang@cs.umn.edu (J. Hwang), tianhe@cs.umn.edu (T. He), kyd@cs.umn.edu (Y. Kim).

1570-8705/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2007.10.005

support various location aware application. For example, it can be used for location-based routing [19,2] or geographic hash table [30]. The wakeup scheduling of sensor nodes can be coordinated more efficiently based on location of sensor nodes while providing enough sensing coverage [1,9]. The location of sensor node can be used to track the movement or behavior of targets [35,28,11]. For example, in hospital we can track the movement and interaction of patients, doctors, and nurses.

These applications run correctly when the localization error is limited to a certain range [12]. However, if malicious nodes (attackers) distort the coordinate system severely by claiming fake locations, the performance of these applications could degrade significantly. To address these issues, various methods [8,17,18,20,22,31,37,38] are proposed. They provide a set of nice mechanisms to detect and filter out compromised nodes and anchors. Most approaches depend on a few trusted entities (nodes or anchors), requiring at least the majority of these entities are not compromised. We argue that since the number of trusted entities in these approaches is relatively small, it would be relatively easy to break. Naturally, we raise the following question: "Is it possible to design a pure decentralized secure localization scheme that can detect phantom nodes, without requiring any trust entities?". The objective and intellectual contribution of this work lie in our answer to this challenging question.

1.1. Protecting fake ranging and location

To obtain correct location information in the presence of adversaries, several approaches have been proposed. These approaches share some common features: adversaries try to fake location information and honest nodes (called verifiers) try to verify if each piece of location information is correct. Depending on which information the approach verifies and who plays the role of the verifier, there can be three different approaches.

In the first category, a few trusted, but centralized nodes (called verifiers) validate the position or ranging claims of individual nodes [18,31,37]. (We call this Centralized Phantom node Detection, CPD in short.) In CPD, a set of verifiers are used to detect Sybil and Wormhole attacks independent from the number of attackers. However, it is not clear how to protect such verifiers from adversaries in WSNs. We argue that the CPD approach is relatively easy to break, because the number of verifiers is normally much less than that of regular nodes, and they could be traced and located more easily based on the traffic analysis, since they are involved with more communication than regular nodes.

In the second category, (set of) regular nodes verify the location information of anchors, who know their location. Through this verification, regular nodes can filter out compromised anchors or beacon information (possibly) generated by adversaries [20–22]. (We call this Compromised Anchor Detection, CAD in short.) When a regular node receives a set of beacons from anchors in its range, it finds the majority of consistent beacons. These approaches rely on the assumption that the majority of anchors or their beacons are not compromised. However, for a given area, if a majority of anchors are compromised all regular nodes in the area will be deceived. The number of anchors are relatively few in deployment area, and they are easy to be found and compromised by attacker because they periodically announce their locations in the beacons.

A common weakness of the above two approaches comes from the centralization. A natural approach that overcomes this weakness is to remove the centralized nodes. In other words, it is desirable to design a localization mechanism where each node plays the role of both verifier and regular node, so that they can filter out phantom nodes. We call this new approach as Decentralized Phantom node Detection, DPD in short. DPD can inherently overcome some of the weaknesses of both CPD and CAD. Since DPD does not have trusted verifiers, attackers need to compromise much more nodes to make the attack successful. Furthermore, since there is no globally shared information, the damage, if any, is confined locally. We argue that a successful implementation of DPD would make localization much more robust against various attacks.

1.2. The contributions of this work

In this paper, we are targeting to the scenarios where attackers announce phantom nodes, who fake their locations, in proximity of legitimate nodes. To design a mechanism to support DPD, we focus on the development of the local map for individual nodes. A local map is a visual representation of the locations of neighbors of a node, which can be constructed correctly by verifying all location claims of its legitimate neighbors and filtering out phantom nodes generated by attacks.