TDOA-based Sybil attack detection scheme for wireless sensor networks

WEN Mi (温蜜), LI Hui (李辉), ZHENG Yan-fei (郑燕飞), CHEN Ke-fei (陈克非)
Lab of Cryptography and Information Security, Shanghai Jiaotong University, Shanghai 200240, P. R. China

Abstract As wireless sensor networks (WSN) are deployed in fire monitoring, object tracking applications, security emerges as a central requirement. A case that Sybil node illegitimately reports messages to the master node with multiple non-existent identities (ID) will cause harmful effects on decision-making or resource allocation in these applications. In this paper, we present an efficient and lightweight solution for Sybil attack detection based on the time difference of arrival (TDOA) between the source node and beacon nodes. This solution can detect the existence of Sybil attacks, and locate the Sybil nodes. We demonstrate efficiency of the solution through experiments. The experiments show that this solution can detect all Sybil attack cases without missing.

Keywords attack detection, Sybil attack, time difference of arrival (TDOA), wireless sensor networks (WSN).

1 Introduction

Wireless sensor networks (WSN) have recently emerged as an important application resulting from the fusion of wireless communications and embedded computing technologies. It has been wildly applied in many fields including monitoring, location, tracking and forestry. However, the nature of wireless sensor network makes them vulnerable to security attacks. Especially, without a trusted centralized authority, the Sybil attack is always possible. The Sybil attack introduced in [1] denotes an attack that the Sybil node tries to forge multiple identifications to broadcast messages in a certain region. Broadcasting messages with multiple identifications can be extremely harmful to many important functions of the sensor network such as voting, fair resource allocation, group based decisions, routing, data aggregation, and misbehavior detection.

A number of protocols for Sybil attack prevention have been proposed in recent years. But most of them are too costly for the resource-poor sensors. Douceur [1] proposes a resource testing method. It assumes that each physical entity is limited in some resource. The verifier tests whether identities correspond to different physical entities by verifying that each identity has as much of the tested resource as a physical device. It is unsuitable for wireless sensor networks because the attacker may use a physical device with several orders of magnitude more resources than a resource-starving sensor node. Karlof, et al. [2] used a Needham-Schroeder like protocol to verify each other’s identity and establish a shared key. Consequently, it can limit the number of neighbors a node allowed to have and send an error message when a node exceeds it. But this method just limits the capability of the Sybil attack and cannot locate the Sybil node and remove it. Newsome, et al. [3] adopts key validation for random key pre-distribution and registration. However, they consume precious memory space as every node is required to store pair-wise keys with neighbors. Bazzi [4] prevents Sybil attacks via geometric distinctness certification, which tests that amongst a group of identities a large enough subset resides on a set of distinct entities. It is too complex and energy consumptive. Demirbas, et al. [5] presents a scheme based on the received signal strength indicator (RSSI) readings of messages to detect the Sybil attack. This is the one most close to ours. Zhang, et al. [6] proposes a suite of location-based compromise-tolerant security mechanisms based on a new cryptographic concept called pairing. To our knowledge, pairing is energy-consuming and it is not suitable for the sensor networks.

The major contribution of this paper is that, it proposes a time difference of arrival (TDOA) based solution to Sybil attack detection and demonstrates its efficiency by experiments. This solution can not only detect the existence of Sybil attacks but also locate the Sybil nodes. It requires minimal storage and communication overhead for sensors, as they are listened by three beacon...
nodes in each cluster, which are assumed to know their own locations (e.g., through GPS receivers or manual configuration). It also does not burden the WSN with shared keys or piggy backing of keys to messages. The essential point of the TDOA-based solution is to associate the TDOA ratio with the sender’s identity (ID). Once the same TDOA ratio with different ID is received, the receiver knows there is a Sybil attack. To use TDOA ratio instead of TDOA to associate the ID is to avoid the sensors at the circle centered at one of the beacon nodes being misdiagnosed.

This paper is organized as follows. In Section 2 we discuss the network model and methodology. In Section 3 we present our Sybil attack detection schemes. In Section 4 we discuss the experiments of our solution. In Section 5 we analyze the performance of our solution. Finally, in Section 6 we give our conclusion and propose the future work.

2 Network model and methodology

2.1 Network model

We assume a static network, where all nodes are deployed randomly over a 2-dimensional monitored area (it can be easily expand to 3 dimensions). If the nodes are deployed too dense, on one hand, the position of more than one node may be located at the same place. This location error may influence the detection of the Sybil attack. On the other hand, in a large scale network deployed randomly over a 2-dimensional monitored area, which will be determined by time-based positioning schemes [7,8]. Each node can reach all beacon nodes in the cluster. Note that Sybil node can forge non-existent multiple identities.

2.2 Time difference of arrival principle

The TDOA of a message can be estimated by the hyperbolic position location solution (HPL) [9]. Assume that $S_1$ is the master beacon node. The distance between the source and the $i$th beacon node is

$$R_i = \sqrt{(X_i - x)^2 + (Y_i - y)^2}.$$  

Now, the distance difference between beacon nodes with respect to $S_1$ is given as

$$R_{i,1} = cd_{i,1} = R_i - R_1,$$  

where $c$ is the signal propagation speed, $R_{i,1}$ is the range difference between $S_1$ and $S_{(i>1)}$, and $d_{i,1}$ is the estimated TDOA between $S_1$ and $S_{(i>1)}$. This defines the set of nonlinear hyperbolic equations whose solution gives the 2-D coordinates of the source. From (2) we know that

$$R_i = R_{i,1} + R_1.$$  

Subtracting (1) at $i = 1$ from (3) results in

$$R_{i,1}^2 + 2R_1R_i = X_i^2 + Y_i^2 - 2X_{i,1}x - 2Y_{i,1}y - X_1^2 - Y_1^2,$$  

where $X_{i,1}$ and $Y_{i,1}$ are equal to $X_i - X_1$ and $Y_i - Y_1$ respectively. Without loss of generality, we assume that the beacon node $S_1$ is located at $(0, 0)$. From (2) we obtain

$$R_1^2 = x^2 + y^2.$$  

For a three base station system, Chan’s method [9] producing two TDOA to render solution for $x$ and $y$ in terms of $R_1$ is in the following form:

$$\begin{bmatrix} x \\ y \end{bmatrix} = -\begin{bmatrix} X_{2,1} & Y_{1,2} \\ X_{3,1} & Y_{1,3} \end{bmatrix}^{-1} \begin{bmatrix} R_{2,1} \\ R_{3,1} \end{bmatrix} R_1 + \frac{1}{2} \frac{R_{2,1}^2 - K_2 + K_1}{R_{3,1}^2 - K_3 + K_1},$$  

where

$$K_1 = X_1^2 + Y_1^2, \quad K_2 = X_2^2 + Y_2^2, \quad K_3 = X_3^2 + Y_3^2,$$

$$R_{2,1} = cd_{2,1}, \quad R_{3,1} = cd_{3,1}.$$  

On the right side of the above equation, all quantities are known except $R_1$. Therefore solution of $x$ and $y$ will be determined by $R_1$. When these values of $x$ and $y$ are substituted into (5), a quadratic equation in terms of $R_1$ is produced. Once the roots of $R_1$ are known, values of $x$ and $y$ can be determined.

![Fig.1 Hyperbolic position location (redrawn from [8])](image.png)