Proactive Defense-Based Secure Localization Scheme in Wireless Sensor Networks

Nabila Labraoui[1], Mourad Gueroui[2], and Makhlouf Aliouat[3]

[1] STIC, University of Tlemcen, Algeria
[2] PRISM, University of Versailles, France
[3] University of Setif, Algeria
labraouinabila@yahoo.fr

Abstract. Sensors' localizations play a critical role in many sensor network applications. A number of techniques have been proposed recently to discover the locations of regular sensors. However, almost all previously proposed techniques can be trivially abused by a malicious adversary involving false position. The wormhole attack is a particularly challenging one since the external adversary which acts in passive mode, does not need to compromise any nodes or have access to any cryptographic keys. In this paper, wormhole attack in DV-hop is discussed, and a Wormhole-free DV-hop Localization scheme (WFDV) is proposed to defend wormhole attack in proactive countermeasure. Using analysis and simulation, we show that our solution is effective in detecting and defending against wormhole attacks with a high detection rate.

Keywords: Range-free localization, secure localization, WSN.

1 Introduction

Recently, the wireless sensor networks (WSNs) has emerged an exciting new development in the field of signal processing and wireless communications for many innovative applications [1]. When a sensor detects an emergency event-driven, its location information should be quickly and accurately determined; sensing data without knowing the sensor's location is meaningless [2]. A straightforward solution is to equip each sensor with a GPS receiver that can accurately provide the sensors with their exact location. Unfortunately, the high costs of GPS technology are at odds with the desire to minimize the cost of individual nodes. Thus it is only feasible to fit a small portion of all sensor nodes with GPS receivers. These GPS-enabled nodes called *anchor* or *beacon nodes* provide position information, in the form of beacon message, for the benefit of *non-beacon* or *blind nodes* (i.e nodes without GPS capabilities). Blind nodes can utilize the location information finished from multiple nearby beacon nodes to estimate their own positions, thus amortizing the high cost of GPS technology across many nodes [3].

Localization in WSNs has drawn growing attention from the researchers and many range-based and range-free approaches [4, 5] have been proposed. However, almost all previously proposed localization can be trivially abused by a malicious adversary. Since location information is an integral part of most wireless sensor networks

H. Cherifi, J.M. Zain, and E. El-Qawasmeh (Eds.): DICTAP 2011, Part I, CCIS 166, pp. 603–618, 2011.