Information Sciences 254 (2014) 39–53

Contents lists available at ScienceDirect

Information Sciences

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

Defending collaborative false data injection attacks in wireless sensor networks

Jianxin Wang [a,*], Zhixiong Liu [a,b], Shigeng Zhang [a], Xi Zhang [c]

[a] School of Information Science and Engineering, Central South University, Changsha, Hunan, China
[b] Department of Computer Science and Technology, Changsha University, Changsha, Hunan, China
[c] Department of Electrical and Computer Engineering, Texas A&M University, TX, USA

ARTICLE INFO

Article history:
Received 7 March 2012
Received in revised form 11 July 2013
Accepted 5 August 2013
Available online 20 August 2013

Keywords:
Wireless sensor network
Compromised node
False data injection
Location information
Relative position

ABSTRACT

False data filtering is an important issue in wireless sensor networks. In this paper, we consider a new type of false data injection attacks called collaborative false data injection, and propose two schemes to defend such attacks. In collaborative false data injection attacks, multiple compromised nodes collaboratively forge a fake report and inject the report into the network. This type of attacks is hard to defend with existing approaches, because they only verify a fixed number of message authentication codes (MACs) carried in the data report but the adversary can easily obtain enough compromised nodes from different geographical areas of the network to break their security. Our novel solution is to bind the keys of sensor nodes to their geographical locations, and verify the legitimacy of a data report by checking whether the locations of the sensors endorsing the report are logical (e.g., the sensors should be close enough to each other to sense the same event). We propose two filtering schemes: The geographical information based false data filtering scheme (GFFS) which utilizes the absolute positions of sensors in the verification, and the neighbor information based false data filtering scheme (NFFS) which utilizes relative positions of sensors when absolute positions cannot be obtained. We theoretically analyze the filtering probability of the two proposed schemes, and evaluate their performance through extensive simulations. Simulation results show that, when there are totally ten nodes compromised in a 400 nodes network, the detection probability of collaborative false data injection attacks is higher than 97% in GFFS and NFFS, but is less than 7% in traditional false data filtering approaches such as SEF.

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

Wireless sensor networks (WSNs) are widely used in many applications including military surveillance, habitat monitoring, and health care [14]. WSNs are usually composed of a large amount of sensor nodes with limited resources, and are usually deployed in unattended environments. In such environments, the security of sensor nodes is very important [7,8,10,13,17,24,25]. Once a node is compromised, the adversary will disclose all the secret information stored in that node. The adversary can then use the compromised nodes to launch false data injection attacks [16], i.e. to inject bogus reports into sensor networks. Defending false data injection attacks is an important research issue in WSNs, because this type of attacks not only causes false alarms that waste real-world response efforts (e.g. sending response teams to the event location), but also may drain out the constrained resources of the forwarding sensors.

* Corresponding author. Tel./fax: +86 0731 88830212.
E-mail addresses: jxwang@mail.csu.edu.cn (J. Wang), lzxterry@163.com (Z. Liu), sgzhang@mail.csu.edu.cn (S. Zhang), xizhang@ece.tamu.edu (X. Zhang).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.08.019

To prevent such false data injection attacks, a general en-route filtering framework has been proposed to detect and filter out false reports in [23]. In this framework, every node is preloaded with some symmetric keys. When an event happens, multiple surrounding nodes collaboratively generate a report that carries $t(t > 1)$ distinct message authentication codes (MACs). Here t is a security threshold. A MAC represents a node's agreement on the report, which is generated by using one of the symmetric keys stored in that node. During the forwarding of the report towards the sink, each forwarding node verifies the correctness of the MACs carried in the report in a probabilistic manner. A report that carries less than t MACs or contains wrong MACs is detected as an invalid report, and hence will be dropped by intermediate nodes or the sink. The framework proposed in [23] inspired some following researches on false reports filtering in recent years [1,15,18–21,27–30]. Most of them focus on improving the filtering probability and reducing the energy consumption of sensor nodes.

However, existing data filtering schemes only consider whether there is *enough number* of sensors endorsing the data report or not. They do not consider whether the endorsement of these sensors is *logical* or not. This makes them fail in filtering out false data report forged collaboratively by more than t compromised nodes from different geographical areas. An example of collaborative false data injection attack is illustrated in Fig. 1. In this example, the adversary has compromised five nodes $S_1, \ldots, S_5$. Assume that the security threshold is five and the compromised nodes have distinct key partitions. By coordinating the five compromised nodes, the adversary can successfully claim a fabricated event at an arbitrary location and forge a data report. Existing data filtering schemes, e.g. SEF, will fail to correctly filter out this data report because there is enough number of correct MACs in the data report. On the other hand, if we take the locations of the endorsing sensors of the data report into account, we can correctly find that the data report is fake because it is not logical: The five sensors endorsing the event are far from each other, so they cannot observe the event simultaneously.

In this paper, we study collaborative false data injection attack and propose two schemes to defend this type of attacks. The novelty of our schemes is that we bind the keys of sensor nodes to their geographical locations. In the geographical information based false data filtering scheme (GFFS), we assume that sensor nodes know their absolute geographical locations and utilize this information to filter out fake reports forged by compromised sensors from different geographical areas. Considering that GFFS requires expensive positioning devices (e.g., GPS), we then propose a neighbor-information based false data filtering scheme (NFFS). NFFS utilizes relative positions of sensor nodes to defend collaborative false data injection attacks. Theoretical analysis and simulation results show that GFFS and NFFS can effectively resist the collaborative false data injection attacks, and tolerate much more compromised nodes than existing schemes.

The main contributions of this paper are summarized as follows:

First, we propose a new false data injection model called collaborative false data injection, and point out that existing data filtering approaches cannot defend such attacks. To our knowledge, we are the first to investigate collaborative false data injection attacks in wireless sensor networks.

Second, we propose the GFFS scheme. In GFFS, each node distributes its location information to some forwarding nodes after deployment. Each data report must carry the MACs and locations of t detecting nodes that sense the event simultaneously. All the forwarding nodes verify the correctness of both MACs and locations. Besides, they also verify the legitimacy of the t locations. Because the keys of sensor nodes are bound to their geographical locations, false reports injected collaboratively by compromised nodes from different geographical areas can be detected and filtered out. Moreover, the ability of compromise tolerance can also be enhanced. Simulation results show that when ten nodes are compromised in a network containing 400 nodes, the probability that the adversary breaks down GFFS is only 3%, while it can break down the security of SEF with a probability of 93.2%.

Third, considering that GFFS requires expensive positioning devices, we further propose the NFFS scheme. In NFFS, each node distributes its neighbor information to some other nodes after deployment. When a report is generated for an observed event, it must carry the IDs and MACs from t detecting nodes. Each forwarding node checks the correctness of the MACs carried in the report and the legitimacy of relative positions of detecting nodes. As a result, false data reports can be detected by

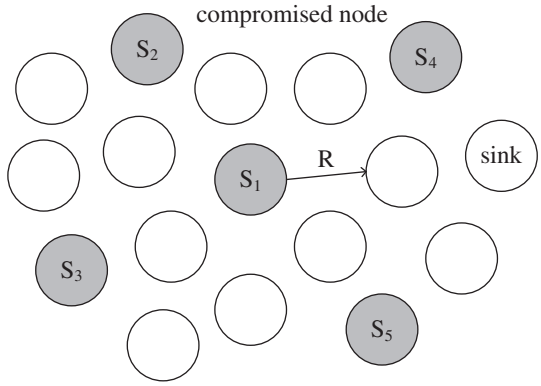

Fig. 1. An example of collaborative false data injection attack.

Download English Version:

https://daneshyari.com/en/article/392924

Download Persian Version:

https://daneshyari.com/article/392924

Daneshyari.com