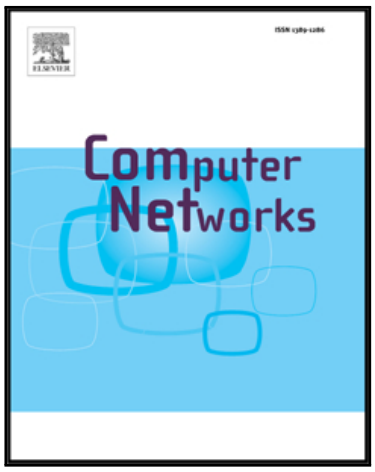

Robust Detection of False Data Injection Attacks for the Data Aggregation in Internet of Things based Environmental Surveillance

Lijun Yang , Chao Ding , Meng Wu , Kun Wang

PII: S1389-1286(17)30237-2
DOI: 10.1016/j.comnet.2017.05.027
Reference: COMPNW 6221

To appear in: *Computer Networks*

Received date: 13 December 2016
Revised date: 30 March 2017
Accepted date: 26 May 2017

Please cite this article as: Lijun Yang , Chao Ding , Meng Wu , Kun Wang , Robust Detection of False Data Injection Attacks for the Data Aggregation in Internet of Things based Environmental Surveillance, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.05.027

Robust Detection of False Data Injection Attacks for the Data Aggregation in Internet of Things based Environmental Surveillance

Lijun Yang [1,2,3,*] , Chao Ding [2], Meng Wu [3], and Kun Wang[1,*]

[1] College of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210046, China;
[2] College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210046, China;
[3] Key Lab of "Broadband Wireless Communication and Sensor Network Technology" of Ministry of Education, Nanjing 210046, China;

***** Corresponding Authors: Lijun Yang, Kung Wang.

E-Mail: yanglijun@njupt.edu.cn, kwang@njupt.edu.cn.
Tel.: +86-136-7513-9056.

Received: / Accepted: / Published:

Abstract: Data aggregation is a significant technology for Internet of Things (IoT) based environmental surveillance to compress the redundant data collected from the small devices which is wide-area distributed over the network. However, since most IoT devices work in an unattended manner with limited security guarantee, they are extremely vulnerable to node compromise. Once the adversaries take charge of the compromised nodes, they can launch false data injection (FDI) attack, which is known to be destructive for data aggregation. To minimize the damage caused by the FDI attack, we adopt Hierarchical Bayesian Spatial-Temporal (HBST) model to describe the statistical characteristics of sensory data in the aggregation-based communication mode, and propose an anomaly detection based scheme to detect compromised nodes in an early stage. The basic idea behind our scheme is to use the divided difference filtering (DDF) based state estimation techniques to detect false aggregated data, and further determine the nodes which are suspected to inject false data using sequential hypothesis testing (SHT). Additionally, we model problem of FDI attack detection using a quantitative two-player game theoretic analysis, derive the optimal strategies for both the adversaries and defenders, and demonstrate that the adversaries' gain from the attack is greatly limited by the defenders even in the worst case when both players follow their respective optimal strategies. Moreover, we present the theoretic and simulation analysis to evaluate the performance of the proposed scheme in terms of the effectiveness, efficiency and overhead. The analysis results show that the proposed scheme achieves high detection rate and low false positive rate with a small amount of detection samples.

Keywords: Internet of Things (IoT); security; in-network aggregation; false injection attack detection; divided difference filter (DDF); sequential analysis