# Energy Efficient Detection of Compromised Nodes in Wireless Sensor Networks

Haengrae Cho

Department of Computer Engineering, Yeungnam University
Gyungbuk 712-749, Republic of Korea
hrcho@yu.ac.kr

**Abstract.** A wireless sensor network (WSN) is often partitioned into a set of spatial clusters to save energy for data collection. Each cluster includes sensor nodes with similar sensing data, and only a few sensor nodes (samplers) report their sensing data to a base node. Then the base node may predict the missed data of non-samplers using the spatial correlation between sensor nodes. The problem is that the WSN is vulnerable to internal security threat such as node compromise. If the samplers are compromised and report incorrect data intentionally, then the WSN should be contaminated rapidly due to the process of missed data prediction at the base node. In this paper, we propose three algorithms to detect compromised nodes for secure data collection in the WSN. The proposed algorithms are novel in the sense that they are completely integrated into the underlying data collection algorithms. Experiment results indicate that the proposed algorithms can detect compromised nodes with a high accuracy and an energy-efficient manner.

**Key words:** Wireless sensor network, Security, Data collection, Node compromise, Performance evaluation

## 1 Introduction

The primary function of a wireless sensor network (WSN) is to collect data for observation and analysis of physical phenomena [4, 7]. In periodic data collection, every node reports periodically its sensing data to the base node. Many researches prefer the periodic approach because it enables arbitrary data analysis at the base node [1, 3, 9]. A *spatial clustering* is a representative way of saving energy in periodic data collection [1, 5]. It partitions the network into a set of clusters where a cluster includes sensor nodes with similar sensing data. For each cluster, only a few sensor nodes (samplers) report their data to the base node. All the rest of sensor nodes can save their energy by keeping in sleep mode. The base node may predict the missed data using the spatial correlation between sensor nodes.

The WSN is vulnerable to security threats both external and internal due to unreliable wireless channels, unattended operation of sensor nodes, and resource constraint [2]. *Node compromise* is a major type of internal attacks. Compromised sensor nodes release all the security information to the adversary. Then, the adversary can easily launch internal attacks with data alteration, message negligence, selective forwarding, and jamming. Note that the node compromise is especially problematic for periodic

data collection, where only the samplers may report data to the base node. If the samplers are compromised and report incorrect data intentionally, then the WSN should be contaminated rapidly due to the process of missing data prediction at the base node. This means that detecting and defending against node compromise are inevitable tasks to guarantee the correctness of data collection at the WSN.

In this paper, we propose three algorithms to detect node compromise for secure data collection in a WSN. The proposed algorithms are based on the spatial clustering and tries to detect compromised nodes with an energy-efficient manner. Unlike previous security algorithms for the WSN [2, 6, 8], our algorithms consider the underlying data collection architectures. The security task is completely integrated into the underlying data collection algorithm. This enables our algorithms to optimize energy consumption for message transmission and sampling.

## 2 Algorithms for Node Compromise Detection

### 2.1 Monitoring by Neighbors (MBN)

At MBN, every neighbor node of a sampler has a role to a watchdog that monitors the message sent from the sampler. To detect compromised samplers, MBN requires that a cluster header (CH) has complete location information of every sensor node in its cluster to identify neighbor nodes of the sampler. Furthermore, each sensor node is assumed to have a correlation vector to its neighbor nodes in the cluster.

Suppose that a sensor node $s_s$ is selected as a sampler. $s_s$ notifies itself to the CH, and the CH wakes up the sensor nodes in $nbr(s_s)$. For each node $s_i \in nbr(s_s)$, it reads its sensing data and overhears the message from $s_s$. If the sensing data sent from $s_s$ is not strongly correlated to that of $s_i$, $s_i$ reports to the CH. If majority in $nbr(s_s)$ report to the CH, the CH decides that $s_s$ is compromised. The underlying assumption of MBN is that majority in $nbr(s_s)$ are not compromised. However, if the assumption is not hold, MBN would fail to detect compromised samplers.

### 2.2 Monitoring by Cluster Head (MBCH)

At MBCH, the CH has a role to detect the compromised node. MBCH modifies the data collection procedures such that (1) at least three samplers of a cluster are selected for each data-sampling period, and (2) samplers are required to send their sensing data to the CH.

The CH determines some samplers as compromised nodes if their sensing data are not strongly correlated from those of majority samplers. The CH forwards sensing data to the base node only for samplers it decides not to be compromised. Since MBCH is based on majority consensus between samplers, MBCH would be more accurate as the number of samplers increase. If there are only a few samplers, small number of compromised samplers would lead to a wrong decision at the CH. This shows an interesting tradeoff between energy consumption and security enforcement.

### 2.3 Monitoring by Hybrid (MBHB)

Both MBN and MBCH cause *false negative errors* in the sense that they could not detect compromised samplers. MBHB tries to prevent the false negative error by combining MBN and MBCH. It consists of two phases to detect the node comprise. At the first phase, the majority vote is performed by neighbor nodes of each sampler, which is similar to MBN. If the sampler gets a majority vote, the CH determines it as a compromised node. At the second phase, similar to MBCH, the CH performs another checking of majority consensus among samplers passing the first phase. Some sampler may also be decided as a compromised node in this phase. The CH forwards sensing data to the base node only for samplers passing both phases.

## 3 Concluding Remarks

The WSN is vulnerable to security threats both external and internal due to unreliable wireless channels, unattended operation of sensor nodes, and resource constraint. In this paper, we proposed three algorithms to detect compromised nodes in WSN. They are monitoring by neighbors (MBN), monitoring by cluster head (MBCH), and a hybrid algorithm of MBN and MBCH (MBHB). Every algorithm is based on spatial clustering and tries to detect compromised nodes with energy-efficient manner. The performance study indicates that MBHB can detect compromised nodes with the most energy-efficient manner. Furthermore, it can detect every compromised node even the case when half of entire sensor nodes are compromised.

## References


1. H. Cho, "Distributed Multidimensional Clustering based on Spatial Correlation in Wireless Sensor Networks," *Computer Systems Science and Engineering* 26 (2011).
2. X. Du, "Detection of Compromised Sensor Nodes in Heterogeneous Sensor Networks," *Proc. Int Conf Communications* (2008).
3. B. Gedik, L. Liu, and P. Yu, "ASAP: An Adaptive Sampling Approach to Data Collection in Sensor Networks" *IEEE Trans Parallel and Distributed Syst* 18 (2007).
4. K. Jang, J. Kang, and H. Kouh, "A Cluster Formation Scheme with Remaining Energy Level of Sensor Nodes in Wireless Sensor Networks," *The Journal of IWIT* 9 (2009).
5. T. Le, N. Pham, and H. Choo, "Towards a Distributed Clustering Scheme based on Spatial Correlation in WSNs," *Proc. Int. Wireless Communications and Mobile Computing Conf* (2008).
6. F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks" *Proc. IEEE Int Conf Computer Communications* (2007).
7. C. Nam, K. Jang, and D. Shin, "Energy-Efficient Data Aggregation and Dissemination based on Events in Wireless Sensor Networks," *The Journal of IWIT* 11 (2011).
8. A. Stetsko, L. Folkman, and V. Matya, "Neighbor-based Intrusion Detection for Wireless Sensor Networks," *Proc. Int Conf Wireless and Mobile Communications* (2010).
9. S. Yun and H. Cho, "An Energy-Efficient Periodic Data Collection using Dynamic Cluster Management Method in Wireless Sensor Network," *Journal of IEMEK* 5 (2010).