Abstract. Data aggregation techniques are useful means in order to reduce number of data transmissions and improve the bandwidth and energy utilization in wireless sensor networks (WSNs). The simplest way to achieve distributed data aggregation is to select data aggregator nodes. However, if captured by an intruder, aggregator node can be a subject to several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on. This paper discusses security issues of data aggregation in WSNs and describes existing solutions and their limitations.

Keywords: Wireless sensor networks, security and protection, intrusion detection system, authentication, cryptography.

1 Introduction

Wireless sensor networks (WSNs), consisting of a sink node (base station) and a group of sensor nodes, have been used in a wide range of applications. The sensor nodes are equipped with a sensing, data communicating, and processing units, which enable them to monitor the physical world, communicate and exchange the collected sensory data with other nodes. In typical wireless sensor networks (WSNs), sensor nodes have limited resources such as battery power, computing capability and memory. Data aggregation techniques are useful means in order to reduce number of data transmissions and improve the bandwidth and energy utilization in wireless sensor networks (WSNs).

The simplest way to achieve distributed data aggregation is to select data aggregator nodes. Aggregator nodes are regular nodes that receive data from neighboring nodes, perform some kind of processing, and then forward the filtered data to the next hop and finally to the base station [3]. However, if captured by an intruder, aggregator node can be a subject to several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on. This paper discusses security issues of data aggregation in WSNs and describes existing solutions and their limitations. The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 describes our proposed approach. Section 6 highlights conclusions.
2 Security in Data Aggregation

In this section, we discuss security issues of data aggregation in WSNS and describe existing solutions and their limitations.

In [3], the authors present the Tiny AGgregation (TAG) service for aggregation in low-power, distributed, wireless environments. TAG allows users to express simple, declarative queries and have them distributed and executed efficiently in networks of low-power, wireless sensors. This approach defines two attributes. First, it offers a simple, declarative interface for data collection and aggregation, inspired by selection and aggregation facilities in database query languages. Second, it intelligently distributes and executes aggregation queries in the sensor network in a time and power-efficient manner, and preserves the resource constraints and loss communication properties of wireless sensor networks. Several significant improvements have been proposed in [6, 7].

Roy et al. [4] discussed the issues of a robust aggregation framework called synopsis diffusion. Particularly, the authors describe the problem of false subaggregate values contributed by compromised nodes resulting in large errors in the aggregate computed at the base station. In contrast, the authors make synopsis diffusion approach secure against various attacks. They propose a lightweight verification algorithm which would enable the base station to verify whether the computed aggregate was valid.

Yang et al. [5] examined the security challenges in hop-by-hop aggregation and proposed SDAP, a Secure Hop-by-hop Data Aggregation Protocol for sensor networks. The main idea of SDAP is based on the principles of divide-and-conquer and commit-and-attest. The authors used divide-and-conquer approach in order to partition the aggregation tree into groups to reduce the importance of high-level nodes in the aggregation tree. They use commit-and-attest so that the BS has a way to verify the aggregates. Through extensive experiments, it is demonstrated that SDAP can have similar efficiency as an ordinary hop-by-hop aggregation protocol while providing security guarantees of the aggregation results.

Huang et al. [1] proposes a secure encrypted-data aggregation scheme for WSNs. The authors state that aggregation functions operate when readings are received in plaintext, and if readings are encrypted, aggregation requires decryption creating extra overhead and key management issues. Thus, they propose an approach to remove redundant sensor readings and maintain secrecy and privacy in transmission without using encryption. Proposed scheme is robust against known-plaintext attacks, chosen-plaintext attacks, ciphertext-only attacks and man-in-the-middle attack.

Li et al. [2] discuss the issue when intruder inject into the network bogus aggregation results. They propose secure and energy-efficient data aggregation scheme that can detect the malicious nodes with a constant per node communication overhead. The main idea of this approach is to ensure that not only the base station does not accept any forged aggregation results, but also the malicious aggregators tampering with the intermediate results can be identified. In this approach, all aggregation results are signed with the private keys of the aggregators in order to avoid the alteration by others. Nodes on each link additionally use their pairwise shared key for secure communications. Each node receives the aggregation results from its parent and its siblings, and verifies the aggregation result of the parent node.
3 Conclusions

The simplest way to achieve distributed data aggregation is to select data aggregator nodes. However, if captured by an intruder, aggregator node can be a subject to several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on. This paper discussed security issues of data aggregation in WSNs and describes existing solutions and their limitations.

4 Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012-003797)

References