Secure and Dependable Distributed Data Storage and Access Control in Mission-critical Wireless Sensor Networks

Wenjing Lou, Dept. of ECE, Worcester Polytechnic Institute

Abstract—Distributed data storage and access in wireless sensor networks (WSNs) recently has found increased popularity driven by many mission-critical applications. While WSN security has been extensively studied in recent years with focus on network communication security, little attention has been paid to the security and dependability of distributed data storage and access control. However, it is of paramount importance to ensure data security and dependability in the mission-critical applications, where data genuineness and availability can be about life or death. This paper sketches an outline of the motivation and the development of security mechanisms for data security and dependability.

1 Introduction

Wireless sensor network (WSN) has been an area of active research in recent years. A WSN usually consists of a large number of sensor nodes that can be easily deployed to various terrains of interest to sense the environment. WSN has found its wide applications in both civilian and military domains. To accomplish the targeted application and fulfill its functionalities, a WSN usually generates a large amount of data over its lifetime. One of the biggest challenge then is how to store and access these sensed data.

Data storage and access in WSNs mainly follow two approaches, namely, centralized and distributed approaches. In the centralized case, sensed data are collected from individual sensors and transmitted back to a central location, usually the sink, for storage and access. In the distributed approach, after a sensor node has generated some data, the node stores the data locally or at some designated nodes within the network, instead of immediately forwarding the data to a centralized location out of the network. The stored data later on can be accessed in distributed manner by the users of the WSN. For example, in "Unattended WSN", data collection is not performed in (or near) real time and data should survive for a long enough time to be collected. "In-Situ Data Storage WSNs" store the sensor readings at the generating sensor node (In-Situ); "Storage-Centric WSNs" store historical data for the applications that need to mine sensor logs to analyze historical trends; In "Asynchronous WSN", sensor nodes do not transmit the data to authorized devices in real-time, but store the data itself; In "Data Centric WSN", relevant data are stored by name at the network nodes, and all data with the same general name will be stored at the same nodes.

Distributed data storage and access recently has found increased popularity due to many reasons. First, new generation sensor nodes with significant performance enhancement are available. Such enhancement includes energy-efficient storage, greater processing capabilities, and data management abilities. Energy-efficient storage such as the new generation flash memory with several gigabytes and low-power consumption is now possible to equip sensor devices. Second, distributed data storage has more efficient energy consumption. In Mica Mote platform, flash memory has less energy efficiency, thereby reducing the energy benefits of local data storage. However, new generation flash memory has significantly altered the energy efficiency and *computation vs communication trade-off* as well, which makes local storage and processing more desirable. Last but not least, distributed data storage achieves more robust WSN. Centralized storage can lead to the single point of failure and easily attracts attacks. Centralized storage may also cause performance bottleneck as all data collection and access have to go through the base station or sink.

2 New Research Directions

WSN security has been extensively studied in recent years with focus on network communication security, such as key management, message authentication, secure time synchronization and localization, and intrusion detection. However, distributed data storage and access security as a fairly new area receives limited attention this far. This becomes a more severe issue given the trend that more and more distributed in-network data storage and access/retrieval schemes are being proposed. A few related works can be found in the literature but none of them satisfies the overall requirements of security and dependability. Therefore, an importnat new research direction therefore is secure and dependable distributed data storage and access in WSNs. The necessity of the research can be best illustrated by the following example. A WSN is deployed in a hospital environment for a variety of purposes centered on the overall goal of

providing better quality of and more efficient healthcare services. A large number of sensors of different functionalities are strategically deployed and self-organized into a large scale WSN possibly spanning several buildings. These sensor nodes are expected to continuously collect a large variety of information regarding the environment, patients, medical equipments, infrastructure, staff, etc. The network users of the WSN, e.g., doctors, nurses, supporting staff, medical equipment technicians, pharmacist, issuance company personnel, etc., may query the network on demand for the various information they need. A doctor may query the sensors resided in and/or on a patient (formed as a small body area network (BAN)) for certain health-related data; a nurse may query certain medical equipments for patient information in a particular time period; a supporting staff may query moisture, temperature, and photo sensors for moisture, temperature, and light information at certain areas; there are also possibilities for automatic data collection through mobile sinks/robots, so on and so forth. In such an application, distributed data storage and access approach is preferred. That is, sensor nodes sense and store various kinds of data locally and provide access to the stored data to the authorized network users in a distributed manner when queried. Because distributed data storage results in a much more robust network as compared to the centralized approach: 1) if centralized data storage and access approach is implemented, every query must go through the centralized entity, data access delay could be significantly increased; not to mention that the query or data response could be lost due to link failures, traffic congestion, or other reasons, whose result can be devastating. 2) centralized approach will lead to single point of failure and expose the central server as an obvious attack target. Obviously, in such a mission critical application, security and dependability of the stored data are of paramount importance. This is because 1) critical medical data items can be lost due to sensor nodes fail; 2) data items can be compromised by the possible attacker through compromising a selective subset of sensor nodes; 3) data items can be intentionally modified by the attacker without being detected through compromising a selective subset of sensor nodes; 4) data items, which are beyond the entitled access right of a group of network users, can be illegally accessed due to their collusion. In all above cases, it can all become life or death issues as the medical information are highly critical to the patients. In fact, there have been report about hacker intrusion of critical medical data. Hence, in order to fulfill the network mission a WSN has to ensure data availability and confidentiality despite of these faults and attacks. That is, a fault-tolerant and compromise-resilient distributed data storage and access mechanism has to be in position to guarantee the success of such mission critical applications.

3 New Approaches

Two important security issues need to be addressed in wireless sensor networks – distributed data storage and access control. To tackle the security and dependability problem of **distributed sensor data storage**, we need to study the problem of how to store the sensor network data in a distributed manner while satisfying the requirements of both fault-tolerance and compromise-resilience. Straightforward solutions, such as individual storage and simple replication approaches, are usually either insecure or inefficient and hence not adequate. We investigate solutions where secret sharing and erasure coding are integrated to achieve both security and efficiency. We also consider dynamic data security and dependability after the initial data storage as over time sensors may be compromised and/or behave Byzantine failures. In this case, it is critical to enable dynamic data consistency verification to ensure continuous data security. However, the challenge we are facing is how to perform dynamic data consistency verification efficiently in the absence of the original data as they have been distributed among multiple storage sensors. We investigate algebraic signature based schemes to address this challenge by exploiting its homomorphic property.

The second main research task is **distributed data access control** that ensures sensor network data only be accessed by authorized network users. We consider the worst-case scenario in which not only sensors may be compromised, but also network users may not be fully trusted as they may also be compromised or collude for illegal data access beyond their collective access right. We need a fine-grained key management solution which achieves both sensor compromise-resilience and user collusion-resistance. After analyzing the state-of-the-art symmetric key cryptography (SKC) based solution and clearly aware of its security weakness and inadequacy for fine-grained data access control, we investigate an efficient SKC based approach to realizing relatively fine-grained user access control. To support more flexible user access structure and achieve improved security strength, we further investigate attribute based encryption (ABE) based access control schemes, which allow a highly flexible and fine-grained user access structure.

4 Conclusion

Distributed data storage and access in wireless sensor networks can be key to the success of large scale sensor network deployment. The technical approaches investigated here are novel. The methodology and rationale to achieve efficiency, resilience, security, dependability, and scalability will impact the security protocol design in wireless sensor networks and beyond. The results of this research will advance the state-of-the-art technology of providing security and dependability of distritbuted data storage and access control in wireless sensor networks.