Chapter 35
Security Management in Heterogeneous Distributed Sensor Networks

Al-Sakib Khan Pathan
International Islamic University, Malaysia

ABSTRACT

A Heterogeneous Distributed Sensor Network (HDSN) is a type of distributed sensor network where sensors with different functional types participate at the same time. In this sensor network model, the sensors are associated with different deployment groups but they cooperate with each other within and out of their respective groups. The heterogeneity of HDSN refers to the functional heterogeneity of the sensors participating in the network unlike the heterogeneity considered (e.g., considering transmission range, energy level, computation ability, sensing range) for traditional heterogeneous sensor networks. Taking this model into consideration, in this chapter the authors present a secure group association authentication mechanism using one-way accumulator which ensures that; before collaborating for a particular task, any pair of nodes in the same deployment group can verify the legitimacy of group association of each other. Secure addition and deletion of sensors are supported in this approach. In addition, a policy-based sensor addition procedure is also suggested. For secure handling of disconnected nodes of a group, the authors use an efficient pairwise key derivation scheme. Side by side proposing their mechanisms, they also discuss the characteristics of HDSN, its scopes, applicability, efficiency, challenges, and future. Before concluding the chapter, the authors also talk about the applicability of our security management framework for secure mobile multimedia delivery over sensor networks.

DOI: 10.4018/978-1-4666-2919-6.ch035

INTRODUCTION

Wireless Sensor Network (WSN) is composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited computational and communication resources. Typical task of the sensors is to sense certain parameters from their surrounding environments and to send the readings to a central entity called base station or sink. The raw data collected from such a network are analyzed to extract important information about a particular area and are often used for taking important decisions. Considering today's advancements and achievements, the applicability of sensor network is very broad. With the capabilities of today's sensors, many applications can be benefited a lot. Now, we have varieties of sensors that can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise level, lighting condition, the presence or absence of certain kinds of objects, mechanical stress level on attached objects, and other properties. These tiny devices could be used for surveillance in military and public-oriented applications, target tracking, environmental monitoring, patient monitoring in hospitals, disaster management and warning systems, and in so many other applications.

With the rapid advancements of wireless technologies and sophistication of sensing technologies, many innovative applications could be thought of using the smart sensors. Though most of the applications focus on collecting a specific type of data, for some applications it is necessary to acquire different types of data from the same geographical region. Again, some applications might need collaborative operations among the sensors before producing reports to send to the base station/sink. As an example, a volcano monitoring application may require thermal, seismic, and acoustic data from the same geographic location. Though only one type of data may be satisfactory for such an application, utilization of various types of data could be more beneficial for extracting accurate and timely information. Say for example, the average temperature (already processed by a sub-set of nodes) of a certain region along with the seismic and acoustic readings can provide more precise information regarding an imminent event. Especially for disaster management and warning systems, military applications, and medical applications, use of multiple types of data can really be advantageous. To facilitate such types of applications that need more than one type of data, ExScal mote (Gu et al., 2005), (Dutta et al., 2005) is designed by CrossBow Inc. and Ohio State University. This mote is basically an extension of the well-known MICA2 mote (MICA2_Datasheet, 2010) which supports multiple sensors (i.e., sensing units) on the same radio board. However, instead of using this type of multipurpose node in the network, using different types of nodes in the same area could be more efficient considering the utilization of memory, processing, and energy resources of the network. We will provide more points in the next section to support this statement.

The key point here is that whatever the configurations of the sensors are, heterogeneous data are often required for some applications that can increase the complexity of tasks in the network. Hence, efficient methods are required for dealing with all aspects in such types of applications. Among various noteworthy aspects considered for any kind of sensor network, security is often deemed to be the most important one. It is anticipated that in most application domains, sensor networks constitute an information source that is a mission critical system component and thus, require commensurate security protection. If an adversary can thwart the work of the network by perturbing the generated information, stopping production, or pilfering information, then the usefulness of sensor networks is drastically curtailed. So, it should be made sure that the sensors that are participating in the data acquisition and supplying process are authentic and are included as legitimate entities in the network. To be specific, along with other supporting security