Protocols for Secure Node-to-Cluster Head Communication in Clustered Wireless Sensor Networks

A.S. Poornima[1] and B.B. Amberker[2]

[1] Dept. of Computer Science and Engg, Siddaganga Institute of Technology, Tumkur, Karnataka, India
[2] Dept. of Computer Science and Engg, National Institute of Technology, Warangal, Andhra Pradesh, India

Abstract. Cluster based organization is widely used to achieve energy efficiency in Wireless Sensor Networks(WSN). In order to achieve confidentiality of the sensed data it is necessary to have secret key shared between a node and its cluster head. Key management is challenging as the cluster head changes in every round in cluster based organization. In this paper we are proposing deterministic key establishment protocols, which ensures that always there exists a secret key between node and its cluster head. The proposed protocols establishes key in an efficient manner every time a cluster head is changed. The hash based protocol achieves key establishment with very minimal storage at each node and by performing simple computations like one way hash functions and EX-OR operations. Where as the polynomial-based protocol establishes key in every round by using preloaded information without performing any additional communication.

Keywords: Cluster-based WSN, Seed value, Cluster head, Sensor Node, Key Matrix.

1 Introduction

Wireless Sensor Networks (WSN) typically consist of small, inexpensive, battery powered sensing devices fitted with wireless transmitters, which can be spatially scattered. Sensors have the ability to communicate through wireless channels, and their energy, computational power and memory are constrained. WSN's have many advantages. They are easier, faster and cheaper to deploy than wired networks or other forms of wireless networks. They have higher degree of fault tolerance than other wireless networks : failure of one or few nodes does not affect the operation of the network. Also, they are self organizing or self-configuring. These advantages make them very promising in a wide range of applications ranging from health care to warfare. The envisioned growth in using sensor networks is demanding extensive research in securing these networks.

Wireless Sensor networks are used in many applications like battlefield, patient monitoring, emergence response information and environmental monitoring.

S. Ranka et al. (Eds.): IC3 2009, CCIS 40, pp. 434–444, 2009.

Providing security for WSNs presents unique challenges. In addition to unknown topography sensors have very high computation, storage and battery constraints. WSNs lack physical protection and are usually deployed in open, unattended environments, which makes them vulnerable to attacks. Cryptographic methods can be used to secure such Wireless Sensor Networks. An important issue to be addressed when cryptographic methods are used to secure WSNs is key distribution. Key pre distribution schemes are the most widely used key distribution methods in WSNs. Many such pre distribution schemes are discussed in literature [3,4,5,6,7,8,9,10,11]. The schemes proposed in the literature consider number of WSN architectures and key distribution methods that is well suited to one architecture is likely not to be the best for another, as different network architectures exhibit different communication patterns.

The available redundancy and inherent energy scarcity of a sensor network encourages the use of aggregation of data. Clustering of the Wireless Sensor Networks (WSN's) improves data aggregation ability. The cluster-based architecture is an effective way to achieve the objective of energy efficiency in Wireless Sensor networks. In a clustered WSN nodes in a neighborhood organize themselves into a cluster, with one node designated as the Cluster Head (CH) [1,2]. The CH collects sensed data from the other nodes in its neighborhood and uses an aggregation scheme to aggregate this information. It then sends the information to a neighboring CH in the direction of the Base Station (BS). Cluster based organization [12] has been proposed for ad hoc networks in general and WSNs in particular. In clustered WSNs rotating cluster heads concept is widely used for energy efficiency. The concept of rotating cluster head is introduced in [12] (which is also called as LEACH- Low Energy Adaptive Clustering Hierarchy protocol). In LEACH protocol to save energy, sensor nodes send their messages to their CH's, which then aggregate the messages and send the aggregate to the BS. To prevent energy drainage of a restricted set of CH's, LEACH randomly rotates CHs among all nodes in the network, distributing aggregation and routing related energy consumption among all nodes in the network.

Security issues in cluster-based sensor networks are addressed in [13,14,15,16]. Bohge et. al. [13] proposed an authentication framework for a concrete 2-tier network organization, in which a middle tier of more powerful nodes between the BS and the ordinary sensors were introduced in order to carry out authentication function. Oliveira et. al. [14] propose solution that relies exclusively on symmetric key schemes and is suitable for networks with an arbitrary number of levels; and Ferreira et.al. [15] proposed F-LEACH where each node has two symmetric keys ; a pairwise key shared with the BS, and the last key of a key chain held by the BS used in authenticated broadcast. In [16] SecLeach, a protocol for securing node-to-CH communication in LEACH based networks is discussed. SecLeach bootstraps security from random key pre distribution scheme which is studied extensively in [3,4,5,6,7,8,9,10,11].

In this paper we are proposing dynamic key establishment protocols to secure node-to-CH communication. Here we are proposing two protocols which deal with establishing secret key between node and its cluster head in order to