Abstract

Wireless Sensor Networks (WSN), are envisioned as an efficient alternative tool where human surveillance is restricted, due to their appealing ad hoc nature. Secure communication among sensor nodes via cryptographic keys, is a challenging problem in such resource-constrained platform. Symmetric key cryptography based key pre-distribution is observed as the most promising solution. Key Pre-Distribution Scheme (KPS) that have acceptable low memory, nominal computational and communication overheads, allow reasonable connectivity and provide better resilience in terms of node disconnection and link failure, could be ideal from practical point of view. The objective of the thesis is to design efficient KPSs where the performance of the scheme can be controlled with suitable choice of the underlying parameters depending on the priority. All the KPSs presented in the thesis are deterministic.

The thesis consists of seven main chapters and one concluding chapter. Chapter 1 is the introductory chapter and Chapter 2 contains a brief literature survey. Chapters 3 to 7 deal with the work done in the thesis. Chapter 8 is about the conclusion and the future scope of the work presented in this thesis.

Chapter 3 provides two hierarchical KPSs, where projective plane and its complementary design are considered as the underlying block designs. The orders of the combinatorial designs and the number of levels present in the network, are the two parameters those control the performance of the schemes. A group-cluster based deployment scheme is discussed in Chapter 4. The nodes are involved in three types of communications and based on that the set of nodes are divided into two categories. The number of groups, number of clusters, number of two types of nodes and the number of different types of keys are the defining factors of the scheme. Three general frameworks for constructing storage efficient and well-resilient key pre-distribution schemes in non-uniform rectangular network are presented in Chapter 5. Proper choice of the number of rows and columns in the grid yield suitable performance trade-offs in the network.

In Chapter 6, we propose two KPSs for triangular grid networks. The first KPS stores only three keys per node to develop a well-connected, scalable network and the second KPS induce Blundo's polynomial based technique to evolve an unconditionally secure KPS. Chapter 7 deals with a KPS employing location awareness. The proposed scheme exploits the advantageous t-secure property of Blundo's scheme to construct a scalable network that is fully connected and unconditionally secure involving low computation and communication overheads.

Keywords Connectivity, resilience, scalability, storage, transmission (radio frequency) range, Lee sphere and Lee distance, pairwise key establishment, projective planes.