Chapter 12

Key Generation for Wireless Sensor Networks Using Symmetric Balanced Incomplete Block Design

K. G. Srinivasa
MS Ramaiah Institute of Technology, India

V. Archana
MS Ramaiah Institute of Technology, India

V. Poornima
MS Ramaiah Institute of Technology, India

C. Reshma
MS Ramaiah Institute of Technology, India

ABSTRACT

Wireless sensor networks consist of many tiny sensor nodes deployed at a high density over region, requiring surveillance and monitoring. The sensor nodes typically consist of one or more sensing elements, battery, low powered radio transmitter/receiver, microprocessor, and limited memory. Sensor networks deployed in a hostile environment are prone to malicious attacks like eavesdropping, masquerading, traffic analysis, et cetera. Hence, security is more important in sensor networks than in traditional networks. An important challenge in sensor network security is the design of effective bootstrapping protocols for the nodes, which are pre-initialized with some secret information and have had no prior direct contact with each other. Each node has a set of keys, called a key chain, rather than a single shared key. The keys in the key chain are picked randomly from a key pool. Two neighboring nodes either share a common key or should be able to establish a key path such that every pair in the path shares a key. One problem in such a solution is to select a proper key chain so that the network remains connected with a high probability.

DOI: 10.4018/978-1-4666-0321-9.ch012
INTRODUCTION

This paper brings in the idea of deterministic approach to key generation. There is no need to assume a probability for any two nodes to be neighbors. We use combinatorial based approach for key generation using a block design technique called symmetric Balanced Incomplete Block Design (BIBD). The main contribution to this work is the use of multiple key spaces to increase resilience and decrease memory utilization and still retain connectivity. It eliminates the dependency between the number of keys in the key-chain and number of nodes in the network. OMNeT++ with Mobility Framework is used for simulating the sensor network. The simulation shows each node broadcasting its key-chain, comparing its key-chain with that of its neighbor and then disconnecting the connection with those nodes which do not have a common key with its key-chain. It also generates an optimal number of key-chains to support birth of nodes after the network is deployed.

Sensor Networks are mostly ad-hoc and mobile networks deployed for a wide variety of applications including military sensing and tracking. They are regarded as distributed autonomous systems for information gathering, performing data-intensive tasks such as environment monitoring, seismic monitoring etc. They have the ability to withstand adverse environmental conditions, communication and node failures. They can adapt to dynamic network topology, heterogeneity of nodes and mobility of nodes. They consist of one or more computationally expensive nodes called base stations and a large amount of inexpensive, low capacity nodes called sensor nodes.

The base stations are distinguishable components of wireless sensor networks with high computational capability, energy and communication resources. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They typically consist of a processing unit with limited computational power and limited memory, one or more sensing elements, a communication device (usually a low powered radio transmitter/receiver), and a power source usually in the form of a battery. The microcontroller is the processing unit which processes data and controls the functionality of other components in the sensor node. Power is used for sensing, communication and data processing. Radio communication allows each node to communicate with nodes only within a limited radius.

As sensor networks are deployed in a hostile environment they are prone to malicious attacks like eavesdropping, masquerading, traffic analysis etc. Hence, security is more important in sensor networks than in traditional networks. To provide security, communication between nodes should be encrypted and authenticated. Encryption and authentication algorithms require that the communicating nodes share a secret key. The problem here is how to set up secret keys between communicating nodes? This problem is known as the key agreement problem. There are basically three types of general key agreement schemes: trusted server scheme, self-enforcing scheme and key pre-distribution scheme. The trusted server scheme depends on a trusted server for key agreement between nodes (B. C. Neumann, T. Tso, 1994). There is no trusted infrastructure in sensor networks. Hence this scheme is not suitable. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as (R. L. Rivest, A. Shamir and L. M. Adleman, 1978) or (W. Diffie and M. E. Hellman, 1976). The third type of key agreement scheme is key pre-distribution which is nothing but symmetric key cryptography. This scheme is most widely used and suitable for sensor networks.

The secret keys are stored in the ROMs of sensor nodes prior to deployment. The keys stored must be carefully selected so as to increase the

www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Smartphones to Access Hybrid Information Spaces

www.igi-global.com/chapter/smartphones-access-hybrid-information-spaces/45267?camid=4v1a

Modulation and Coding Techniques for Inter-Vehicular Communications

www.igi-global.com/chapter/modulation-coding-techniques-inter-vehicular/62807?camid=4v1a

A Systematic Exploration on Challenges and Limitations in Middleware Programming for IoT Technology

www.igi-global.com/article/a-systematic-exploration-on-challenges-and-limitations-in-middleware-programming-for-iot-technology/221331?camid=4v1a

A Survey of IPv6 Addressing Schemes for Internet of Things

www.igi-global.com/article/a-survey-of-ipv6-addressing-schemes-for-internet-of-things/221334?camid=4v1a