A Key Predistribution Scheme for Wireless Sensor Networks Using the Small-World Concept*

Yung-Tsung Hou, Chia-Mei Chen, and Bingchiang Jeng

Department of Information Management,
National Sun Yat-Sen University, Kaohsiung, Taiwan
{ythou,cmchen,jeng}@mis.nsysu.edu.tw

Abstract. Most of wireless sensor networks (WSNs) are deployed in an environment where communication between sensors may be monitored. For applications which require higher security, it is therefore necessary to employ some cryptographic scheme in the network. However, key management in WSNs is a challenging task due to the constrained resources. In this paper, based on the concept of small worlds, we present a group-based key predistribution scheme which enables any pair of sensors to establish a unique shared key. The key path establishment uses only local information with logarithmic memory overhead to the number of groups. Other performance, including communication and computing overhead, are evaluated also. The results show that the proposed key management method performs better than other known methods.

Keywords: Key predistribution, Small worlds, Wireless sensor networks.

1 Introduction

Wireless sensor networks (WSNs) are composed of small and inexpensive sensors with limited resources in battery power, memory, computation, and communication. Recent advances in computing and communication technologies have created a variety of such applications [12] including habitat monitoring, remote climate monitoring, and other commercial and military applications. In some applications like battlefield sensing or critical infrastructure protection, sensor nodes are deployed in a hostile environment under numerous threats including information eavesdropping, sensor compromising, sensor impersonating, and even denial-of-service attacks. Secure transmission therefore becomes an important issue in WSNs.

Key management in WSNs is not trivial. The approaches used for general computer networks are not applicable for WSNs due to resource limitations in sensors. Thus, symmetric cryptography which shares a key between two parties is considered, and several schemes for pair-wise shared key establishment are developed. Among them, the key predistribution scheme which distributes key information to sensors before the

* This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 94-3114-P-006-001-Y and NSC 95-2221-E-110-083.

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 137–146, 2007.

deployment is viewed as an efficient approach to set up shared secret keys. An example is the full pair-wise approach in which each sensor node is preloaded with a set of unique keys and each of them is shared with another node in the network. Under such a scheme, a node will need to carry $n - 1$ secret keys for a network of n nodes. Hence, its memory overhead makes this scheme impractical as n goes larger.

Random key predistribution schemes [1, 2] were proposed as a remedy for the above situation. The basic idea is to preload each sensor node with a random subset of keys from a large key pool before deployment. Since the keys in different nodes are from the same pool, any two neighboring nodes will have a certain probability to share a common key and they could use it for communication. If such a key does not exist, they will instead establish a key path using intermediary nodes, and then use it to exchange a key to establish a direct link.

In this paper, we propose a group-based random key predistribution scheme for WSNs. Our scheme is based on the concept of small worlds [5, 8, 9]. A small-world network has the following properties: (1) the local neighborhood is preserved; and (2) the diameter of the network increases logarithmically with the number of nodes in the network. The network created by the proposed scheme will have pre-built secure links that satisfies the criterion of small worlds -- any two nodes in the network can be connected with just a few secure links. In the initial key preloading stage, each node is loaded with a set of keys shared with other nodes in the same group and additional keys shared with the nodes in distant groups based on a probability distribution. With the preloaded shared keys, any two nodes will be able to find efficiently a secure path connecting them in an average path length logarithmic to the number of sensor groups. This path length is shorter than others found in literature. A simulation later will demonstrate the performance.

1.1 Related Work

Eschenauer and Gligor [1] first proposed a random key predistribution scheme for key management in WSNs. The basic idea of their scheme is as described in the previous section. Several studies [2-4] later proposed new predistribution schemes. Their methods utilize the high connectivity property of a random graph when the average degree of its nodes exceeds a threshold. The performance of these schemes depends on the network's topology, which might degrade rapidly if the nodes are sparsely or non-uniformly distributed in the network.

PIKE [11] is a deterministic scheme for key predistribution. In the method, any pair of nodes in the network exists an intermediary node that has shared keys with each node. This intermediary node is used as a trusted peer to establish a key path. PIKE shows significantly improvement over random key predistribution schemes. However, PIKE might require network-wide communication to establish the key path. Its communication overhead makes it unsuitable for large sensor networks.

The small-world concept was first studied by Milgram [5-7] in the 1960's. His experiments in mail delivery using acquaintances resulted in an average of "six degrees of separation". After that, several network models have been proposed to study the phenomenon. Watts and Strogatz [8] proposed a refined network model and showed that the small world phenomenon is pervasive in a wide range of networks.