A New Scheme for Establishing Pairwise Keys for Wireless Sensor Networks

Abhishek Gupta, Joy Kuri, and Pavan Nuggehalli

Centre for Electronics Design and Technology
Indian Institute of Science, Bangalore
{agupta, kuri, pavan}@cedt.iisc.ernet.in

Abstract. This paper addresses the problem of secure path key establishment in wireless sensor networks that uses the random key predistribution technique. Inspired by the recent proxy-based scheme in [1] and [2], we introduce a *friend*-based scheme for establishing pairwise keys securely. We show that the chances of finding friends in a neighbourhood are considerably more than that of finding proxies, leading to lower communication overhead. Further, we prove that the friend-based scheme performs better than the proxy-based scheme in terms of resilience against node capture.

1 Introduction

In the last few years, wireless sensor networks (WSNs) have become a very actively researched area. The impetus for this spurt of interest were developments in wireless technologies and low-cost VLSI, that made it possible to build inexpensive sensors and actuators. Each such device has limited computational power, memory and energy supply. Nevertheless, because of the low cost, such devices can be deployed in large numbers, and can thereafter form a sensor *network*. Applications have been suggested in diverse areas, including surveillance, environmental monitoring, health care and crisis management systems.

In some application areas, security is a major concern. When sensor networks carry sensitive information, it is important to ensure privacy. For example, in a surveillance application, it would be very undesirable if intruders can access the information being carried by the network. To provide security, the well-developed public key cryptographic methods have been considered, but these generally demand excessive computation and storage from the resource-poor sensors [3]. This has led researchers to conclude that symmetric key cryptography, in which nodes share a secret key, is the only viable solution.

While cryptographically strong algorithms are available, the issue of *key distribution and management* is critical to the level of security actually achieved. At one end of the spectrum, we have a system in which all the sensors share a single secret key. But this makes the network very vulnerable; an adversary needs to capture just a single sensor node to access any information that the network carries. At the opposite end, we have a system where each node has a

S. Chaudhuri et al. (Eds.): ICDCN 2006, LNCS 4308, pp. 522–533, 2006.

distinct shared key for every other node. But for large sensor networks, such a scheme demands an excessive amount of on-board memory, which is again undesirable. It is also possible for nodes to securely generate keys on the fly using key exchange algorithms, such as the well-known Diffie-Hellman scheme. However, the computational and storage requirements for such schemes have also been deemed unacceptable for sensor networks [3].

In [4], Eschenauer and Gligor suggested a probabilistic solution to the problem of efficient key distribution. In this scheme, nodes have a secure link if they share a key in common and those which do not share a key undergo path key establishment phase to set-up a pair-wise key.A drawback of this scheme is that the secret key is known to all the nodes on the path from the source to the destination node during path key-establishment phase.

This 'per-hop key exposure' problem have been considered by several researchers. In [1], the authors proposed an elegant solution of using multiple node-disjoint paths between S and D for secure path key establishment. But the problem of discovering multiple node-disjoint paths is computationally hard, and too much overhead may be incurred in this process. In a later work [2], the authors relax the requirement of node-disjoint paths, and utilize multiple *proxies* for path key establishment. A proxy $\mathcal{P}$ is a node that shares one or more keys with the source node S and one or more keys with the destination node D.

In this paper, we propose a novel scheme to efficiently solve the 'per-hop key exposure' problem. It is based on nodes that are referred to as *friends* of the destination. A friend of the destination is simply a node that shares one or more keys with the destination. Each friend F in a neighbourhood of S sends *part-keys* back to the source, where a part-key is obtained by applying a hash function to all the keys shared between F and D. The source then chooses a number of these part-keys, say i, and uses a publicly known function to generate the shared key K_{SD} from them. S informs D about which i friends' part-keys were used, and this information is sufficient for D to generate K_{SD} using the publicly known function.

We compare our friend-based scheme with the proxy-based scheme reported in [2], and find several advantages. First, for a source-destination pair, the requirement for a node to be a friend is less stringent than for it to be a proxy. This implies that the computational and communication effort in finding a friend is less than in finding a proxy, making the friend-based approach more viable. Second, our friend-based scheme is able to achieve a level of security at least as good as the one based on proxies.

2 Related Work

The random key pre-distribution scheme was first proposed by [4]. We discuss this proposal in some detail in the next section. Based on this, several schemes with enhanced security features have been suggested. A q-composite-random key pre-distribution scheme is proposed by [5] which achieves strengthened security under small scale attack while trading off increased vulnerability in the face