

Key Management in Sensor Networks

Chorzempa, Mike

Bradley Department of Electrical and Computer Engineering

The suitability of sensor networks for military applications and the deployment of these networks in hostile environments has brought the challenge of securing the communication between these extremely resource constrained devices. In addition to battlefield deployment, there are a number of future applications that will require a high level of security. These include emergency response information, energy management, environmental monitoring, and medical monitoring. Providing security for these types of networks presents unique challenges for members of the research community. The devices that make up a sensor network have very limited computation, memory, battery and communication capabilities. This research has dealt with analyzing recently published schemes for weaknesses and shortcomings, and using a developed set of scheme criteria, establish a framework of a new and most effective scheme.

There are four major criteria that I have identified that are necessary for any deployable key management scheme. First it is necessary for the sensors to establish pairwise keys, that is, share a unique key with each of its immediate neighbors. Second, at least one more class of key must be created, either cluster keys, or a group key. This key must be available so more than one node can share the same key, and thus overhear messages. Next, it is necessary for the scheme to efficiently support node addition, that is existing nodes should allow new nodes to establish secure channels at any time. Finally, in a hostile environment there will be node capture. A good scheme will efficiently recover from, and be resilient against a detected node capture.

Another key observation is that as the size of a sensor networks increases to a very large scale (10,000 nodes), it is more likely a few higher power nodes will also be deployed for the purpose of accumulating and relaying sensor information. From this observation, an approach that can utilize a hierarchical scheme as in Figure 1, will be most effective.

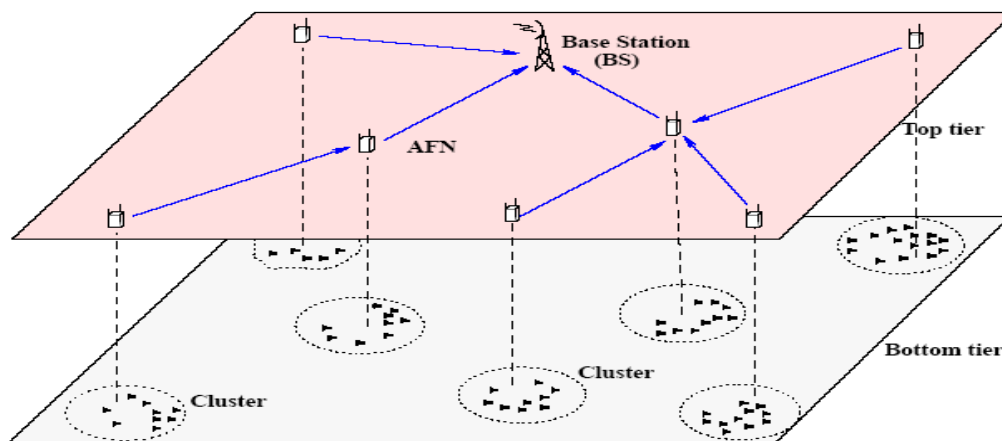


Figure 1. Example multi-tiered sensor network structure.

From the weaknesses shown in the analyzed schemes, it can be shown that ultimately a hierarchical and hybrid scheme will be the most efficient and robust method of key management in sensor networks. Most of the schemes analyzed have mostly attempted to optimize either a pairwise approach or group approach. The pairwise approach allows a great deal of security, but restricts the types of communication and is expensive to update any of the keys. Group approaches allow very good levels of communication flexibility, but is not resilient or efficient against attack. A hierarchical hybrid approach would utilize different levels of keying sophistication for the tiers of varying resource capable devices. For example, for the smallest sensors having small 8bit processors, they may utilize a lightweight group key scheme with their head node. These second tier group nodes (maybe PDA-type devices), having more capable 16 or 32bit processors, can support a more sophisticated and resilient symmetric scheme, or possibly even an asymmetric scheme. Currently, different possible schemes for the different tiers in the network are being investigated.