
Sead Muftic, Chih-Chun Chang

2 photos to follow
Captioned:
Sead Muftic
Chih-Chun Chang

Wireless sensor networks have evolved from science fiction to a budding reality in a matter of a few years. A wireless sensor network is a collection of sensor nodes, tiny devices, usually battery powered, that acts as nodes in a larger network. The use of these networks is constrained only by the power of human imagination – from sensors on our body parts alerting a doctor to an alarming change in our vital signs, to a sensor on the earth constantly on the look out for a flood, forest fires, highway traffic control or tsunami. As with all emerging technologies, security poses great challenges to the scalability and deployment of such networks. In this article we explore the particular challenges of finding cryptographic algorithms suitable to such small devices, the key management problems and architectural issues.

Problems

Wireless sensor networks are a rapidly emerging technology with potential for many different and distributed applications. Wireless sensor networks are collections of small computers, with sensing and computing capabilities, characterised primarily by limited resources for processing and communication. They function by collecting sensor data and exchanging messages using wireless links. The nodes contain sensors needed by the applications, microcontrollers and radio transceivers, all integrated on a single chip.

In real-life situations, wireless sensor networks may have a variety of different topologies due to diverse options for their deployment. In principle, there are three basic modes of network organisation, determined on the basis of the connectivity of the nodes: hierarchical, distributed and hybrid. In a hierarchical network, there is a more powerful node, usually called the base station, which performs the functions of a central authority for other nodes. Its tasks include collecting data from other sensors and passing them to wired networks, or functioning as a network management station, synchronising and controlling the operations of other nodes. Distributed networks do not have central authority, and there is no fixed infrastructure of the network. Each sensor node communicates with its neighbours, which are located within its radio coverage. A hybrid network is a combination of hierarchical and distributed topologies.

In a large-scale sensor network, where a large number of nodes are dynamically interconnected, the risks of various threats increase substantially. The nature of wireless sensor networks and their protocols make them more vulnerable to attacks, disruptions and problems than wired networks. The main problems with implementing security in wireless sensor networks range from memory and energy constraints, key management protocols and security-enhanced applications to the actual deployment environments in which the networks are used. Some of these problems are caused by limitations of sensor node technologies and thus are not relevant for networks with
PCs or PDAs. This means that standard security solutions, used today for other types of networks and devices, cannot be simply transferred to sensor networks. New ideas and new solutions are needed.

Security for wireless sensor networks is today still in its infancy. The challenges of incorporating cryptographic algorithms into sensor nodes, implementing security protocols and incorporating security in network applications are currently critical design issues. Both hardware and software components have to be co-designed for basic network functions and also for security. Therefore, the comprehensive research and development of different aspects of security for wireless sensor networks is today both timely and very important.

**Cryptographic Algorithms for Limited Resource Devices**

The research and development of cryptographic algorithms suitable for limited resource devices has intensified in the last few years. Studies aimed at developing ‘light-weight’ versions of cryptographic algorithms resulted in multiple techniques, which have been tested and evaluated in sensor networks. For instance, TinySec, developed by UC Berkley, is a default security mechanism in sensor radio boards (better known as motes) produced by Crossbow. The security is applied in the data link layer of a seven-layer OSI protocol, which means encryption and hashing mechanisms are applied when transmitting and receiving packets. TinySec performs verification of data correctness during their transmission at each hop, protecting the system against threats such as packet injection attacks on the network. The system is based on secret key cryptography.

Some research focuses on asymmetric cryptography. The TinyPK system, developed by BBN Technologies, uses the RSA cryptosystem. The implementation of TinyPK supports only public key operations (data encryption and signature verification) in sensor nodes. The Sizzle system, introduced by Sun Microsystems Laboratories, uses elliptic curve cryptography (ECC). It also runs a secure SSL web server within a sensor node. In order to save bandwidth, memory and computation, the server’s private key, corresponding certificate and static web pages are stored in program memory. Sizzle uses an abbreviated handshake protocol, if a session has been already negotiated between a client and a server, which reuses a previously established master secret and does not involve any public key operations, such as certificate exchange/verification or key exchange.

Finding suitably light cryptographic algorithms will remain a challenge as the real-life deployment of wireless sensor networks continues to impose new constraints.

**Key Distribution and Management Protocols**

Traditional key management protocols in wired networks with multiple components are usually based on usage of trusted servers, which perform bilateral or broadcast key distribution, such as secure group protocol or client-server security protocol. Establishing trusted servers in a wireless sensor network is difficult because of the nature of network constraints. Several studies have proposed alternatives, mainly based on key pre-deployment approaches, where keys are loaded into sensors prior to deployment in order to overcome the lack of computing and commutation power of sensor nodes.

The characteristics of several key establishment protocols for sensor networks are summarised in the following table:
Single master key scheme means that one single network-wide shared key is preloaded in all nodes, which is the simplest method. Contrary to this approach, in all pair-wise keys scheme, all nodes in the network share a unique key. Sensor nodes in the random pair-wise scheme share a probabilistic subset of keys from a large key pool. In order to increase probability of sharing a unique key between two nodes, the keys may be generated in a polynomial way, paired with their unique identification or assigned to a particular subset of nodes. The group-based scheme divides connections among sensor nodes into two types, in-group and inter-group, and two key sets are provided for these two types. The trusted base station scheme uses a trusted and secure base station as an arbiter to provide link keys to nodes. Authentication of nodes is performed by the base station.

Five major types of key establishment protocols and their relative performance for scalability in network size, connectivity of the key-sharing graph, resilience against node capture attack and overhead of memory usage (storage complexity) are rated from ‘perfect’ to ‘worst’ in the table above. Scalability, key sharing and resilience are constrained by the limited memory size in all pair-wise keying schemes. The table also shows that none of these keying protocols achieves perfect performances in all four areas of scalability, key sharing, resilience and storage. Moreover, a good key management protocol for a wireless sensor network also needs to consider processing complexity and communication complexity, since they are relevant for energy consumption.

Security Services and Security Architecture

Data confidentiality, data authentication, data integrity and data freshness are services most often needed in sensor networks. In addition to securing individual nodes, it is necessary to design security systems that are themselves resistant to attacks and other forms of node failures. The concept of graceful degradation has been a cornerstone of distributed and fault-tolerant systems. The applicability of this approach to sensor networks and security must be explored. In particular, security systems and network applications should be able to continue to operate even if some nodes in the network are compromised or have failed.
A composable security architecture, which supports the construction of sensor networks from smaller parts that are secure and trusted, will be invaluable for the future deployment of sensor networks. The promising approach to achieving these properties is by structuring security in the form of the security middleware. It would consist of alternative security algorithms, components and protocols, as needed by the network applications and the type of data they handle.

Conclusions

Security is one of the most important characteristics of any network, but it is especially important for sensor networks. Such networks operate in open and unprotected environments, so they are exposed to an increased level of threats. Applications of sensor networks proliferate in many areas of contemporary life, and they must be enhanced with strong security features, approaching those of wired networks. Current research and development of security solutions for wireless sensors is still in its infancy. However, many universities, laboratories and companies are already pursuing research and development activities, so positive results may be expected in the near future.

---------------

Sead Muftic is a Professor at the Royal Institute of Technology, Stockholm, Sweden

Chih-Chun Chang is a doctoral student in the Department of Computer Science, The George Washington University, in Washington, DC, USA