Bitwise key agreement using wireless channel parameters (work in progress)

Zoya Dyka, Dan Kreiser and Peter Langendoerfer

System dpt. IHP
Frankfurt (Oder), Germany

Generation, distribution and re-freshing of secret keys in wireless sensor networks are important and not simple tasks. There are many different possibilities to achieve this, for example the common secret key can be pre-distributed, or the Kerberos and Diffie-Hellmann key agreement protocols can be used, or the key can be transmitted encrypted using the public key of the receivers. In 1993 a new possibility to agree a secret key was introduced. It was proposed to use a common randomness for example caused from the location of the sender and the receiver for the key agreement. If a node A sends a signal to a node B, B receives a distorted signal due to the distance between A and B and the geometry of the room (i.e. the indoor environment) causing multi-path signal replicas at the receiver. If A and B can send an identical signal to each other in a static environment, they both receive a signal identically distorted according to the reciprocity theorem. An attacker at different position as A or B can listen to their communication but he receives signals that differ significantly from those A and B receive, since the parameters of the received signal depend on the location. So A and B can use parameters of received signals, for example the middle value of the received signal strength (RSS), for secure key agreement. Thus, one key bit can be agreed per a probe signal. To agree about a 128 bit long key at least 128 probe signals need to be exchanged between A and B. In practice a lot more probe signals need to be exchanged because A and B receive a similar but not identical signals. After A and B calculated their secret keys using all collected RSS values, these keys have to be compared to verify that they are identical. For this a hash of the new keys can be calculated and compared or A can encrypt a message with its new key and send it to B. If B can decrypt the message correctly, than both have an identical secret key.

The security strength of the key generated using channel parameters is discussed in literature because this approach is vulnerable for example to manipulation of the environment and jamming attacks. But also the key generation rate is low. The collection of RSS values, their processing and the key acknowledgement phases take relatively long. If the keys generated by A and B are different the procedure will be repeated from the beginning. Energy and time consumption are also critical parameters for WSN. To improve these parameters we propose to re-fresh secret keys bitwise after each communication using the channel parameters of the communication.

Our assumption is: during the initialization phase all sensor nodes of a WSN agree pairwise to first (initial) secret keys and a key-bit hopping scheme. The key-bit hopping scheme is a sequence of N key-bit positions. This sequence is a plan for A and B to update their secret key bitwise. The number of elements in the sequence, the distance between the elements should be different for each pair of sensor nodes. Changing the sequence according to a certain algorithm is an additional option. During the communication only one of the nodes, for example node B, obtains a new key-bit value using channel parameters. The first number in the key-bit hopping scheme defines the key-bit position that will be updated. The next message from B to A will be encrypted with the updated key. A decrypts the received message at first with the old key. If the decryption was not successful, A obtains the updated key by inversion of the key bit at the first position in the bit hopping scheme. Now A can decrypt the message with the updated key. By this approach, A and B have updated their secret key. This procedure can be repeated for the next key update at the next position the key-bit hopping scheme.