Secure and Robust loose time synchronization mechanism for Wireless Sensor Networks

Jing Deng, Richard Han and Shivakant Mishra
Department of Computer Sciences, University of Colorado at Boulder
{jing,rhan,mishras}@cs.colorado.edu

Time synchronization is required by many wireless sensor networks (WSNs) applications such as localization, data aggregtion, and cooperative target tracking. In addition, the secure sensor network protocols, such as μTESLA, also require that the sensor nodes are loosely time synchronized.

Although many accurate and light-weight time synchornization protocols have been proposed, none of them are secure. These protocols use one of two types of time synchronization mechanisms: sender-receiver approach (TPSN), and receiver-receiver approach (RBS). Both of them are able to syncrhonize time within tens of microseconds. Both mechanisms require that the nodes exchange time stamped messages. To apply these mechanisms in a global sensor network, nodes are logically organized in a hierarchical, tree-like structure, with a root node in the center. A node synchronizes its time with one of its neighbor node (which is closer to the root) by exchanging a time stamped message. However, if a malicious node n_1 sends incorrect time stamp to another node n_2, n_2 has no way to detect the incorrect time stamp. So, if a malicious node claims that it is closer to the root node, it can affect lots of downstream nodes and set wrong time in them.

In this project, we present a secure, robust and loose time synchronization mechanisms. Our goal is to provide loose time synchronization with in 100 milliseconds among all nodes in the sensor network. We think its granularity is good enough to support the secure broadcast protocol μTESLA.

To prevent an adversary from tampering with time stamps and limit adversary's capability of controling downstream nodes, we propose the following two mechanisms in our protocol: 1) We use a beacon message, called *time notification* message that is sent by a base station to inform other sensor nodes about a time synchronization event. To ensure source authentication, we make use of one-way hash chains. An adversary can block or drop this message, but cannot cheat other nodes by modifying the message. 2) The *time notification* message is flooded in the network, and so there is no tree-like network structure in WSN. A single node cannot prevent its downstream nodes from receiving a *time notification* message through some other route, as long as the sensor network is sufficiently dense. By applying bidirectionality verification, sensor nodes can defend against rushing attack as well in this mechanism.

A critical problem in using beacon message for time synchronization is its time accuracy. In a large sensor network, a *time notification* message has to be forwarded via multiple nodes to reach all nodes in the network. To synchronize its time with a base station, a node has to estimate the propagation time of the *time notification* message. We propose to use triangle localization mechanism to estimate this propagation delay.

In this method, three base stations a, b, c are used to broadcast *time notification* messages M_a, M_b, and M_c at the same time. All sensor nodes are inside the triangle. Each sensor node forwards each of three *time notification* messages only once. One-way hash chains are used to protect the authenticy of *time notification* message. Each node records the time t_a, t_b, and t_c as it first receives M_a, M_b and M_c, and computes the time differences T_{ab} and T_{ac}, where $T_{ab} = t_a - t_b$ and $T_{ac} = t_a - t_c$. We assume that the propagation speed is almost uniform in the network (which is true if the network density is almost uniform), and all the nodes know the propagation time of *time notification* message from one base station to another base station (which value can be preconfigured to each sensor node). With above assumption and knowing T_{ab}, T_{ac}, a node can compute the propagation time of *time notification* message from a base station to itself.

However, in reality, the message propagation time on each sensor node is different. Especially, the access time (the time a node occupies data transmission channel) is highly non-deterministic. The question is how these non-deterministic factors affect our method. We believe that in a uniformly distributed sensor network, propagation time of *time notification* message from a base station to a sensor node is between a certain range.

We have simulated this loose time synchronization algorithm in our simulator. We set the packet processing time varied uniformly between 30 to 45 milliseconds, and used CSMA as the MAC layer protocol. Our simulation shows that for a uniformly distributed network, as the size of the sensor network increases from 100 nodes to 900 nodes, the average time standard deviation in our estimate of propagation delay from a base station is constant (between 50 to 60 milliseconds). This preliminary experiment shows that our mechanism is feasible for loose time synchronization in sensor networks. In the future, we plan to do a thorough mathematical analysis and extensive simulation tests to evaluate our mechanism.