Energy-Efficient Hybrid Key Distribution Scheme for Wireless Sensor Networks

Majid Alshammari and Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract
Key distribution in Wireless Sensor Networks (WSNs) is challenging because a WSN is a network of resource-constrained nodes that carry limited-power batteries. Therefore, a key distribution scheme for WSNs must be an energy and memory efficient. In this poster, we proposed an energy-efficient hybrid key distribution scheme that is designed to suit the resource-constrained devices such as WSNs. We utilized Arduino UNO microcontroller and OPNET Modeler to investigate our proposed scheme in comparison to key distribution schemes in the literature. The findings show that our scheme achieves security and consumes less energy compared to other schemes in the literature, less energy.

Introduction
Recent advances in technology allow wireless sensor nodes to be cost-effective and small in size. Thus, they have become rapidly involved in a variety of applications such as in the military, health, agriculture, environment, home and commercial automation, and transportation. Key distribution plays a crucial role in the security of these applications. However, designing a key distribution scheme for WSNs is challenging because wireless sensor nodes are powered by limited-power batteries. In this poster, we present an energy-efficient hybrid key distribution scheme that is designed to suit resource-constrained devices such as WSNs.

Proposed Protocol
Pre-Deployment Phase:
\{K_s, K_a\} \leftarrow RSAGen,
K_{sink} \leftarrow A_K\text{sink} and K_a \leftarrow A_K\text{nodes}.
Sink node: \text{Pre}_{sink} and Sensor node: \text{Pre}_{nodes}.

Key Distribution Phase:
Sink node:
\begin{align*}
K_{session} & \leftarrow \{0, 1\}^{256} \text{ and timestamp } T, \\
C & \leftarrow E_{A_K\text{sink}}(K_{session} \parallel T),
\end{align*}
\text{send} \rightarrow \left\{C \leftarrow E_{A_K\text{sink}}(K_{session} \parallel T)\right\}.
Sensor nodes:
\begin{align*}
p & \leftarrow D_{A_K\text{sink}}(C \leftarrow E_{A_K\text{sink}}(K_{session} \parallel T)),
\end{align*}
\text{verify}(O) = \begin{cases} 
\text{accept, } T \leq \text{time threshold} & \text{reject, } T > \text{time threshold}
\end{cases}

Post-Key distribution phase:
Sensor Data, and timestamp T,
\begin{align*}
C & \leftarrow E_{A_K\text{sink}}(Data \parallel T),
\end{align*}
\text{send} \rightarrow \left\{C \leftarrow E_{A_K\text{sink}}(Data \parallel T)\right\}.
Sink node:
\begin{align*}
p & \leftarrow D_{A_K\text{sink}}(C \leftarrow E_{A_K\text{sink}}(Data \parallel T)),
\end{align*}
\text{verify}(O) = \begin{cases} 
\text{accept, } T \leq \text{time threshold} & \text{reject, } T > \text{time threshold}
\end{cases}

Methodology/implementation
We used real hardware implementation and simulation.

I. Hardware implementation.
We used Arduino UNO microcontroller [1] to implement key distribution algorithms of the investigated schemes, measuring the time these schemes take to perform key distribution process and then calculating the actual energy consumption.

II. Simulation.
We utilized OPNET Modeler to design and to create a model for a wireless sensor node. The model can calculate the energy consumption of a wireless sensor node as well as the energy consumption that is caused by wireless effects. The power parameters of our model is based on XBee transceiver S1 [2].

Efficiency Analysis
We examine the energy efficiency of our proposed scheme compared to the following key distribution schemes [3], [4], and [5].

Security Analysis
We utilized ProVerif, the automatic cryptographic protocol verifier to automatically analyze the security of our proposed scheme and verify it in a formal model. The Adversary model is based on Dolev-Yao model [6].

I. Reachability and Secrecy
Investigating the reachability of sensor data to an adversary.

Conclusion
Each time the distance double between two wireless sensor nodes, four times the amount of power are required. Therefore, proposing a key distribution scheme without considering the number of frames that are involved in key distribution process is not practical for such resource-constrained devices. Also, ignoring the wireless channel effects is not realistic because every wireless channel has effects that contribute to energy consumption. Therefore, when we designed our scheme, we consider all that issues.

References