Proceedings of the 5th Annual ISC Graduate Research Symposium
ISC-GRS 2011
April 7, 2011, Rolla, Missouri

ENERGY EFFICIENT SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

Vimal Kumar, Dr. Sanjay Madria

ABSTRACT

Secure data aggregation in wireless sensor networks has two main objectives which are contrasting in nature. i) Efficiently collecting and aggregating data ii) Aggregating the data securely. Many schemes do not take into account the passive adversary and allow the aggregator to decrypt data which certainly is not secure; on the other hand using public key cryptography for end to end security is not efficient. In this paper we study and analyze the performance of the secure hierarchical data aggregation algorithm which uses an efficient public key cryptosystem (elliptic curve cryptography) to achieve end to end security. Unlike many other secure data aggregation algorithms which require separate phases for secure aggregation and integrity verification, the secure hierarchical data aggregation algorithm does not require an additional phase for verification. This saves energy by avoiding additional transmissions and computation overhead on the sensor nodes. We implemented the algorithm on MICA2 and TelosB motes. We measured the execution time and energy consumption of various cryptographic functions on the motes and analyzed how an end to end scheme increases the network life time in a WSN.

***The publication of this abstract is intended for educational purposes only from an internal symposium and its content has not been peer-reviewed.**