World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:9, No:05, 2015

SA-SPKC: Secure and Efficient Aggregation Scheme for Wireless Sensor Networks Using Stateful Public Key Cryptography

Authors : Merad Boudia Omar Rafik, Feham Mohammed

Abstract : Data aggregation in wireless sensor networks (WSNs) provides a great reduction of energy consumption. The limited resources of sensor nodes make the choice of an encryption algorithm very important for providing security for data aggregation. Asymmetric cryptography involves large ciphertexts and heavy computations but solves, on the other hand, the problem of key distribution of symmetric one. The latter provides smaller ciphertexts and speed computations. Also, the recent researches have shown that achieving the end-to-end confidentiality and the end-to-end integrity at the same is a challenging task. In this paper, we propose (SA-SPKC), a novel security protocol which addresses both security services for WSNs, and where only the base station can verify the individual data and identify the malicious node. Our scheme is based on stateful public key encryption (StPKE). The latter combines the best features of both kinds of encryption along with state in order to reduce the computation overhead. Our analysis

Keywords : secure data aggregation, wireless sensor networks, elliptic curve cryptography, homomorphic encryption
Conference Title : ICISS 2015 : International Conference on Information Systems Security
Conference Location : Paris, France
Conference Dates : May 18-19, 2015

Open Science Index, Electrical and Information Engineering Vol:9, No:05, 2015 publications.waset.org/abstracts/23097.pdf