9 February 2017, Article number 7849585, Pages 71-76

Authentication of mobile Wireless Sensor Networks

Abd-Eldayem, S.S.[a], Rizk, M.R.M.[b], Mokhtar, M.A.[b]

[a] Electrical Department, Pharos University in Alex, Alexandria, Egypt

[b] Electrical Department, Alexandria University, Alexandria, Egypt

Abstract:

Wireless Sensor Network (WSN) contains a lot of sensors called nodes or motes. These sensors sense the environmental data, according to the application, and then communicate with each other, and finally send these data or readings back to the base station. WSN security is an important issue, since motes are usually left to operate unattended in the environment where they were deployed. Intruder may inject false data into the network, thus strong security mechanisms are needed to be implemented in order to protect the network against malicious intruder or attacks. This paper proposed a key distribution and authentication protocol designed to achieve some security requirements of WSNs. The paper introduces a simple protocol for shared key discovery and authentication of massage and entity. The work assumes mobile nodes and proposed a re-authentication protocol for nodes to re-authenticate themselves in the new location. The efficiency of the proposed protocol has been ensured in terms of energy consumption, packet size and the security requirements achieved. © 2016 IEEE.

Reference:
https://08105yvtj-1106-y-https-www-scopus-com.mplbci.ekb.eg/record/display.uri?origin=recordpage&eid=2-s2.0-85015854120&citeCnt=5&noHighlight=false&sort=plf-f&src=s&nlo=&nlr=&nls=&sid=9ff590a66789d9781c08c6de68f72583&sot=aff&sdt=cl&cluster=scopubyr%2c%222017%22%2ct%2bscosubjabbr%2c%22ENGI%22%2ct&sl=49&s=AF-ID%28%22Pharos+University+in+Alexandria%22+60011287%29&relpos=12