A Location-based Authentication and Key Management Scheme for Border Surveillance Wireless Sensor Networks

Authors : Walid Abdallah, Noureddine Boudriga

Abstract : Wireless sensor networks have shown their effectiveness in the deployment of many critical applications especially in the military domain. Border surveillance is one of these applications where a set of wireless sensors are deployed along a country border line to detect illegal intrusion attempts to the national territory and report this to a control center to undergo the necessary measures. Regarding its nature, this wireless sensor network can be the target of many security attacks trying to compromise its normal operation. Particularly, in this application the deployment and location of sensor nodes are of great importance for detecting and tracking intruders. This paper proposes a location-based authentication and key distribution mechanism to secure wireless sensor networks intended for border surveillance where the key establishment is performed using elliptic curve cryptography and identity-based public key scheme. In this scheme, the public key of each sensor node will be authenticated by keys that depend on its position in the monitored area. Before establishing a pairwise key between two nodes, each one of them must verify the neighborhood location of the other node using a message authentication code (MAC) calculated on the corresponding public key and keys derived from encrypted beacon messages broadcast by anchor nodes. We show that our proposed public key authentication and key distribution scheme is more resilient to node capture and node replication attacks than currently available schemes. Also, the achievement of the key distribution between nodes in our scheme generates less communication overhead and hence increases network performances.

Keywords : wireless sensor networks, border surveillance, security, key distribution, location-based
Conference Title : ICWCA 2015 : International Conference on Wireless Communications and Applications
Conference Location : Jeddah, Saudi Arabia
Conference Dates : January 26-27, 2015