Abstract

User authentication in case of wireless sensor network is a very critical task, as sensor nodes are deployed in unattached environment and are prone to possible hostile network attacks. Any authentication protocol in WSN must be designed keeping the fact that sensor nodes have limited computing power, memory, energy and communication capabilities. In this paper, an improved user authentication protocol based on Elliptic Curve Cryptography (ECC) has been introduced for hierarchical wireless sensor networks (HWSN). This paper shows that the ECC based protocol is suitable for wireless sensor networks where higher security is demanded. Besides this the proposed scheme provides mutual authentication and a secret session key for communication between the user and the cluster head. It also provides an option for addition or replacement of cluster head in the network whenever there is a need.

References

An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC

- He, D., Gao, Y., Chan, S., Chen, C. and Bu, J. "An enhanced two-factor user authentication scheme in wireless sensor networks"; Ad Hoc & Sensor Wireless Networks
An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC

2010;10(4).


- FAN, R. , HE D. J. and PAN, X. Z. Ling-di PING "An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks"; Journal of Zhejiang University-SCIENCE C (Computers & Electronics) ISSN 1869-1951 (Print); ISSN 1869-196X (Online) Received Oct. 27, 2010; Revision accepted Feb. 23, 2011; Crosschecked May 30, 2011


Index Terms

Computer Science

Wireless

Keywords

User Authentication; Security; Public Key Cryptography (PKC); ECC; Smart Card; Hierarchical Wireless Sensor Network (HWSN)