Authentication Protocols for WSN using ECC and Hidden Generator Concepts

Authors:
Ayaz Hassan Moon, Ummer Iqbal

Abstract

Authentication is an important Security primitive in any class of network both at the entity level as well as at the message level. All the network entities comprising of WSN including nodes, cluster heads and base station need to be authenticated before sending or receiving any kind of communication within them. Public Key Cryptography offers broad based solutions to address all the security concerns. However such solutions are far too expensive to be applied directly to WSN owing to its resource constraints. ECC and its variant Tiny- ECC offers the scope and the potential to build light weight solutions for WSN based networks.

In this paper, light weight authentication protocols for Base to Node, Node to Base and Node to Node have been presented. These protocols are based on Elliptical Curve Cryptography and Hidden Generator Concepts. Hash Chains which are computationally light have been also used. The protocols have been developed in TinyOS, the defacto operating system for WSN and simulated in Tossim. The protocols have been ported to WSN hardware targeting MicaZ mote. The paper also brings out performance parameters of the developed protocols.
References

12. www.certicom.com
13. TinyOS. http://www.tinyos.net
16. Moon A.H and Iqbal Ummer .2015 Light Weight Secure Key Generation Protocol with Hidden Generator Point using ECC in Transactions on Networks and Communications

Index Terms

Computer Science   Signal Processing
Keywords

Authentication, Hidden Generator, WSN, ECC