Abstract

Wireless Mesh Networks (WMNs) are multi-hop and multiradio network in which each node communicates with each other to increase the performance of network and are new emerging wireless technology, potential for strengthening internet deployment and access. However, security is the main challenge in WMNs. A well-performed security framework for WMNs will require to network survivability and strongly support the network growth. In this paper, we propose a secure, lightweight public key (two way authentication and Access Control based on Elliptic curve cryptography) based security scheme WMNs is to guarantee well-performed key management services and protection from unauthorized access. It is more scalable and
requires less memory compared to symmetric keybased schemes. Furthermore, it is much more lightweight than other public key-based schemes such as RSA-based protocols have significant problems in terms of the bandwidth and storage requirements. Currently, the RSA algorithm requires that the key length be at least 1024 bits for long term security, however, it seems that 160 bits are sufficient for elliptic curve cryptographic functions.

References

- Vipul Gupta, Douglas Stebila_, Stephen Fung Eberle “Speeding up Secure Web Transactions Using Elliptic Curve Cryptography”Sun Microsystems, Inc.2600 Casey Avenue Mountain View, CA 94043
- Patrick Longa, and Catherine Gebotys, “Efficient Techniques for High-Speed Elliptic Curve Cryptography” 2010 University of Waterloo, Canada
- IEEE 802.11 Standard Group Web Site. Available:
- IEEE 802.15 Standard Group Web Site. Available:

Index Terms

Computer Science Engineering and Technology

Keywords

Elliptic curve Cryptography security two way authentication access control wireless mesh networks