A Mathematical Model to the Security Issues of Bluetooth using Elliptic Curve Cryptography

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 161 - Number 8

Year of Publication: 2017

Authors:
Ahmad Hweishel A. Alfarjat, H. S. Sheshadri, Hanumanthappa J.

Abstract

In this research paper, we are addressing the problem of algorithms for Wireless LAN for Secured Transmission. Our research work also proposes an overview of some of the major attacks that Bluetooth has faced over the years along with some possible solutions. The main aim of our research work also investigates security features of Bluetooth using Elliptic Curve Cryptography (ECC). The ECC is the latest and fastest encryption method which offers stronger security. As we know that although a vast majority of devices already currently now communicates using Bluetooth methodology. The Bluetooth security expert provides automatic updates to its security protocol and user privacy protection technique for every security breach so that protection of the device user’s personal information becomes the primary aim. The research work also explores the Bucket Brigade Attack on Bluetooth security using Elliptic Curve Cryptography (ECC). As we know that Bucket Brigade Attack (BBA)(MITM)(WITM) is one of the amazing solution to the problem of key agreement or key swapping. The beauty of this scheme is when two parties who likes to communicate using symmetric key and an Elliptic
Curve Cryptography (ECC) an Intruder (Hacker) enters in between a sender and a receiver.

References

10. D. Kugler, Man in the Middle attacks on Bluetooth, in Proc 7th Int Conf Financial Cryptography (FC'03), Gosier, Gouadeloupe, French West Indies, Jan. 27-30, 2003, pp. 149-161.
14. W.C. Barker, Recommendation for the triple data encryption algorithm block cipher, National Institute of standards and Technology (NIST), Gaithersburg, MD, USA.

Index Terms

Computer Science

Security
Keywords

Cryptography, Bucket Brigade Attack (BBA), Elliptic Curve Cryptography (ECC), Man-in-the-Middle Attack (MITM).