Abstract

A proprietary open wireless technology standard for exchanging data over short distances from one device to another is not much secure. As in traditional method of Bluetooth communication between two or more devices a 128-bit symmetric stream cipher called E0 is used which seems to be week under some conditions it may be broken under certain conditions with the time complexity O (2^64). To improve security of data we propose a hybrid encryption technique. In
A Hybrid Encryption Technique to Secure Bluetooth Communication

this technique we use triple DES for encryption of the key for which we use Tiger algorithm. In Tiger algorithm there is double protection of Data using triple DES and with the help of this algorithm transmission of data will be more secure for exchanging data over short distances from one device to another.

References

- A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication, Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering Zhejiang Gongshang University
- Performance Analysis of SAFER+ and Triple DES security algorithms for Bluetooth Security Systems, Dr. R. Neelaveni, D. Sharmila
- Bluetooth Hacking: A Case Study, Dennis Browning, Gary C. Kessler
- Suri, P. R.; Rani, S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon, 2008.
- Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, Amit Dhir
- Cryptanalysis of Bluetooth Keystream Generator Two-level E0, Yi Lu? and Serge Vaudenay
- On the Existence of low-degree Equations for Algebraic Attacks, Frederik Armknecht?
- Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher Revised 19 May 2008 William C. Barker
- Serpent: A New Block Cipher Proposal, Eli Biham, Ross Anderson and Lars Knudsen
- Cracking the Bluetooth PIN, Yaniv Shaked and Avishai Wool.

Index Terms

Computer Science

Communication and Networks
Keywords
Bluetooth  E0 key stream  hybrid encryption algorithm  data transmission