Abstract

Securing End to End Communication in mobile ad-hoc networks are difficult than the ones for fixed, while the security requirements are same namely availability, confidentiality, integrity,
authentication and non repudiation. The difference occurs due to system constraints in mobile devices and frequent topology changes in the network. System constraints include low power architecture, small memory, limited bandwidth and limited battery power exhaustion. This paper is focus on the design and analysis a security solution for Mobile ad – hoc Network (MANET) through the authentication data encryption model. The model is analyzed under various attacks and the result shows that the proposed model is highly resistant to attack in end to end communication.

References

- Pirzada, A., Mc Donald, C.: Kerberos Assisted Authentication in Mobile Ad-hoc Networks, the 27th Australasian computer science conference 2004

December 19, 2001
- SEC 1: Elliptic Curve Cryptography: Certicom Research Contact: secg-talk@lists.certicom.com September 20, 2000 Version 1.0
- Elisabeth Oswald: Introduction to Elliptic Curve Cryptography, Institute for Applied Information Processing and Communication A-8010 Inffeldgasse 16a, Graz, Austria, July 29, 2005.

Index Terms
Keywords

Mobile Ad hoc Network  End to End Communication

Attacks