A mobile ad hoc network (MANET) is a self-organized wireless short-lived network consisting of mobile nodes. The mobile nodes communicate with one another by wireless radio links. The unconstrained nature of a wireless medium of MANETs allows the attackers for interception, injection, and interference of communication among nodes. Various secure routing protocols, such as SAR, ARAN, SAODV, SRP, ARIADNE, SEAD, SMT, SLSP, CONFIDANT, etc. are existing in the literature. But these protocols are either too expensive or have unrealistic requirements. They consume a lot of resources. Security extensions for existing routing
protocols do not contain important performance optimizations. In this paper, we propose a new security protocol, called cryptographic hybrid key management for secure routing in MANETs. The proposed security protocol has been implemented in Java SE 6 with light weight Bouncy Castle 1.6 API and empirically evaluated its performance via a security analysis and simulation assessments. The results obtained by the proposed approach have been compared with the results of other approaches. Simulation assessments have shown that the proposed approach has outperformed the others, and is a more effective and efficient way of providing security in MANETs.

References

- S. Capkun, L. Buttyn, and J. P. Hubaux, Self-Organized Public-Key Management for

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile - RFC 2459.
Index Terms

Computer Science

Keywords

- mobile ad hoc networks
- self-organization
- cryptography
- network security
- key management
- key authentication
- key repository
- certificate repository
- trust graphs