Abstract

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

- C.K. Tok, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Pearson
- C. Siva Ram Murthy and B.S Manoj, Ad Hoc Wireless Networks: Architectures and
- F. Anjum and P. Mouchtaris, Security for Wireless Ad hoc Networks, John Wiley & Sons,
  2007.
- Prasant Mohapatra and Srikanth V. Krishnamurthy, Ad Hoc Networks: Technologies and
- S. Basagni, M. Conti, S. Giordono and I. Stojmenovic: Mobile Ad Hoc Networks, IEEE
  Control for Mobile Ad Hoc Networks, IEEE/ACM Transactions on Networking, Vol.12,
- B. Lehane, L. Doyle, and D. O'Mahony, Shared RSA Key Generation in a Mobile Ad
  Hoc Network, Proceedings of IEEE Military Communications Conference (MILCOM),
- B. Zhu, F. Bao, R.H. Deng, M.S. Kankanhalli, and G. Wang, Efficient and Robust Key
  Management for Large Mobile Ad Hoc Networks, Computer Networks - Elsevier, Vol.48,
- M. Narasimha, G. Tsudik, and J. Yi, On the Utility of Distributed Cryptography and P2P
  and MANETs: The Case of Membership Control, Proceedings of IEEE International
- S. Jarecki, N. Saxena, and J.H. Yi, An Attack on the Proactive RSA Signature Scheme in
  the URSA Ad Hoc Network Access Control Protocol, Proceedings of ACM Workshop on
- S. Capkun, L. Buttyan, and J. P. Hubaux, Self-Organized Public-Key Management for
A New Security Protocol for Mobile Ad Hoc Networks


- 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