Abstract

A network that consists of several free mobile nodes competent to move in any direction and allied from end to end through wireless links is termed as Mobile Ad hoc Networks (MANETS). MANET is basically the self-configured network supporting various modernistic applications. MANET’s security is important because of wide range of multimedia programs and software running in an infrastructure-less environment, limited power and vibrant topology making it highly susceptible to severe security issues. This paper presents a review of security threats such as dynamic and reflexive attacks, threats such as black hole and wormhole, eavesdropping, spoofing, denial of service, flooding and rushing attack etc. and summarizes the proposed solutions for handling these security liabilities by debating about various routing protocols that deliver security in MANETs.

References

- Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks; IEEE, 2005.
- Claude Crepeau et al., A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes. IEEE Transactions on Vehicular Technology, Jan. 2009
- M. A. Gorlatova, P. C. Mason, M. Wang, L. Lamont, R. Liscano, Detecting


**Index Terms**

Computer Science

Security

**Keywords**

Ad-hoc Networks; MANETS; Routing Protocols