T. Anusha *et al*, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 5, November- 2013, pg. 44-50 **ISSN: 2321-8363**

Improving The Trust and Adversary Detection Process For Delay-Tolerant Networks

T. Anusha[1], N. Srihari Rao[2]
[1]M.Tech. Student, CSE Dept, CMR Institute of Technology, Hyderabad, A.P
Email-id: anushareddy.ram@gmail.com
[2]Associate Prof., CSE Dept., CMR Institute of Technology, Hyderabad, A.P
MIAENG, MCSI, MISTE
Email-id: raon2006@gmail.com

Abstract

Trust and reputation play critical roles in most environments wherein entities participate in various transactions and protocols among each other. A potential low-cost solution to the problem of connecting devices in areas, where end-to-end connectivity cannot be assumed is required, and such low-cost networks are known as Delay Tolerant Networks (DTNs). Delay/Disruption Tolerant Networks have been identified as one of the key areas in the field of wireless communication, wherein sparseness and delay are particularly high. DTNs are characterized by large end to- end communication latency and the lack of end-to-end path from a source to its destination. These characteristics pose several challenges to the security of DTNs. Iterative Trust and Reputation Management (ITRM) mechanism is an iterative malicious node detection mechanism for DTNs. This scheme is a graph-based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. ITRM mechanism is used for completing our research project work. ITRM scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and EigenTrust.

Index Terms

Trust, Reputation; DTN; Attack; Mobile Ad-Hoc Network (MANET)

Full Text: www.ijcsma.com/publications/november2013/V1I503.pdf