 Removal of Malicious Attacks using Hybrid Symmetric Cryptographic Technique

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 132
Number 7

Year of Publication: 2015

Authors:

V. Umadevi, C. Chandrasekar

Abstract

Security in Mobile Ad-hoc Network (MANET) plays an important role for providing effective network service without any malicious attack. Intrusion detection is crucial in improving the performance of mobile ad-hoc network. Intrusion detection monitors the activities in a mobile system by collecting the information and then analyzing them. Most previous works for intrusion detection use the current acknowledgement and location-based routing protocol to combat against the intrusion detection. In this work to secure the mobile network system from malicious attacks, Hybrid Symmetric Cryptography Technique (HSCT) is introduced. The HSCT uses Advanced Encryption Standard (AES) and Message Digest 5 (MD5). Advanced Encryption Standard (AES) is based on the principle of substitution and permutation keying model adapted as node ids in the mobile ad-hoc network. AES ensures higher amount of packets being transmitted with minimum packet delay. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words in mobile nodes to remove the malicious attack. AES and MD5 fused together on the mobile nodes to communicate packets with high security. The HSCT algorithms offer data security and users authenticity using a mixture of two symmetric
cryptographic techniques. HSCT measure and analyze different parameters such as true positive rate on detecting abnormal activities, packet delay, rate of intrusion being detected with respect to node density and packets being transmitted. The HSCT is simulated using NS2. Experiment results show that the proposed technique achieves better performance in considerably minimizing the packet delay rate by 33.36% and improves the true positive rate on detecting abnormal activities by 25.83% compared to the state-of-the-art works.

References

Issue 1, January 2013, Pages 51-64.


Index Terms

Computer Science Networks

Keywords

MANET, Intrusion detection, Location-based routing protocol, Symmetric Cryptography, Advanced Encryption Standard, Message Digest