Integrated Intelligent Research (IIR)
International Journal of Communication and Networking System
Volume: 05, Issue: 01, June 2016, Pages: 50-51
ISSN: 2278-2427

Transparency Minimization in Manet using Enhanced Oblique Protection Algorithm

M.Charles Arockiaraj[1], P.Mayilvahanan[2]
[1] Research Scholar, Vels University, Chennai. India.
[2] HOD,Ddept.of MCA,Vels University,Chennai

Abstract - A Mobile Ad-Hoc Network is a collection of wireless devices (say nodes) which are connected without a predetermined infrastructure such as access points or independent base stations. Due to infrastructure-less architecture, there is a necessity of integrity, confidentiality and security in the network. These networks are interlinked with all the devices in particular network in possible multihop paths. In the accordance with the characteristics of MANET, nodes are easily compromised by the adversaries. The existing trust model can make the decision for identifying the malicious nodes. However, this model did not have any misbehavior attack detection strategy. In general, the detection of misbehaving attack is complex due to the mobility of node. In order to overcome these issues, In this paper an innovative scheme is proposed to monitor and detect the malicious nodes without compromising the network performances. The major contribution is to alleviate the Watchdog (IDS for MANET) issues such as limited transmission power, packet dropping, receiver collision and false misbehavior reports generation. The proposed approach is an acknowledgement based, in which each acknowledgement packet is digitally signed with an Next Generation Cryptography (NGC) algorithm for authenticating the acknowledgement packets. Simulation results demonstrate that the proposed scheme offer more security and improve the network performances than earlier IDS approaches. The proposed system improves the packet delivery ratio and also minimizes the routing overhead even in the presence of malicious nodes in the network.*Keywords:* MANET (Mobile Ad hoc NETwork), multi hop network, ECKCDSA (Elliptic curve Korean Certificate Based Digital Signature Algorithm), SHA (Secure Hash Algorithm).

I. INTRODUCTION

MANET is a growing technology, which enables users to commune without any substantial infrastructure in their geographical location. MANET is formed by the collection of transferable wireless devices. MANETs exhibits various security goals they are privacy, authentication, non-repudiation and integrity [1].

A Mobile Ad-Hoc network is a group of devices which are connected without a predetermined infrastructure such as access points or independent base stations. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Mobile ad hoc networks (MANETs) does not possess predetermined architecture and hence it is difficult to provide security and integrity. To identify multiple black hole nodes cooperating with each other in a MANET. To discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation

II. SIGNATURE ALGORITHM

The two basic group of analysis are carried out using this signature algorithm they are signature generation and signature verification. Signature generation, to generate a signature on signing and verifying process on message m, the signer should take into account of the following parameters [23]. The basic steps of the signature generation approach is given below,

1. Select random value *k* € *(*1, *n*-1*)*
2. Compute $KG=(x_1 , y_1)$
3. The calculate $r = Hash(x_1) \bmod n$. If r=0, continue to step 1.
4. Compute $e = Hash(h_{cert} \| m)$
5. Compute the integer $w = r \oplus e(\bmod n)$
6. Computes $e = r \oplus h(W)$
7. Compute the second part s of the signature $s= d_A(k-w)$. If s=0, then go to step 1.
8. The signature m is the pair of (r,s).

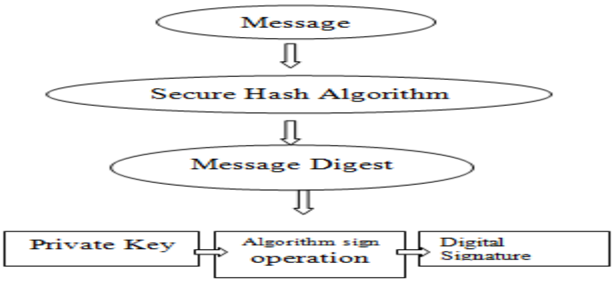

Fig 3 Signature Generation

III. SIGNATURE VERIFICATION

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. Since there are always new intrusions that cannot be prevented, IDS is introduced to detect possible violations of a security policy by monitoring system activities and response. IDSs are aptly called the second line of defense, since IDS comes into the picture after an intrusion has occurred. Intrusion detection techniques can be generally classified into two types, namely, misuse detection and anomaly detection. In misuse detection the "signatures" of known attacks are used to detect the intrusive behavior. In anomaly detection, profiles of normally behaving systems are established through automated training.

IV. CONCLUSION

In this research work, the Hybrid and secure authentication protocol methodology is proposed based on ECKCDSA SHA512 hash function which improves the detection of the misbehavior nodes with the attacker by enhancing the system security. This methodology deals with the expansion of the network protocol, which is more appropriate for Network Trust Organization Server. In this approach, the authentication protocols – RSA, ECC and modified ECC on key management which has high security encryption was discussed. Hence, this authentication protocol has more security to attacks on data transfer, highly reliable to forecast the misbehavior nodes with the following parameters by considering the performance of the proposed system based on computation storage overhead, predicting the attacker precision, and prediction of packet loss.

References

[1] Ankur O. Bang, Prabhakar L. Ramteke (2013) MANET: History, Challenges and Applications IJAIEM Volume 2, Issue 9 .pp.249-251.

[2] Kristin Lauter, (2004) “The Advantages of Elliptic Curve Cryptography for Wireless Security” IEEE vol no 20 .pp.62-67.

[3] Vijayakumar and Tamizharasan (2013) Enhancing the Secure Data Transmission for Routing Attacks in MANET IJARCSSE vol 3 no 11.pp.404-411.

[4] Rajesh Yadav and Dr. Srinivasa Rao (2015) A Survey of various routing protocols in MANETs IJCSIT vol 6 no 5.pp. 4587-4592

[5] Priyanka Goyal et al (2010) A Literature Review of Security Attack in Mobile Ad-hoc Networks IJCA vol 9 no 12.pp.11-15.

[6] Dinakar and Dr. J. Shanthini (2014) A Study on Various Features of Multicast Routing Protocols in Mobile Ad hoc Networks IJARCSSE vol 4 no 7.pp.612-616.

[7] Raju et al., (2013) A Novel Elliptic Curve Cryptography Based Aodv For Mobile Ad-Hoc Networks For Enhanced Security JATIT Vol 58 No 3.pp.349-357.

[8] Bhavna Sharma and vandhana Madaan (2015) Enhancing Security of MANETs by Implementing Elliptical Curve based threshold Cryptography IJECS Vol 4 no 7 .pp. 13346-13350.

[9] Michael Braun and Anton Kargl (2007) A Note on Signature Standards Siemens corporate Technology IEEE .pp. 1-7.

[10] Santhi Sri et al (2014) Minimizing Network Overhead in MANET Using Elliptic Curve Cryptography IJRCCT Vol 3 no 8 .pp.901-904.

[11] Edna Elizabeth et al (2013) Enhanced Security Key Management Scheme for Manets Wseas Transactions On Communications vol.13 .pp. 15-25.

[12] Greeshma Sarath et al (2014) “A Survey on Elliptic Curve Digital Signature Algorithm and Its Variants” CSCP .pp.121-136.

[13] Sathya Priya And Krishnakumari (2014) Detection Of Misbehavior Nodes In MANET Using Path Tracing Algorithm IJRASET Vol 1 No 1.pp.11-16.