Source Anonymization Using Modified New Variant ElGamal Signature Scheme

JHANSI VAZRAM. B[1], VALLI KUMARI. V[2], MURTHY J.V.R[3]
[1]Department of Computer Science and Engineering
Narasaraopeta Engineering. College
Narasaraopet - 522601
[2]Department of Computer Science and Systems Engineering
College of Engineering (A), Andhra University
Visakhapatnam - 530003
[3]Department of Computer Science and Engineering
College of Engineering (A), J N T University
Kakinada - 533003
INDIA
jhansi.bolla@gmail.com, vallikumari@gmail.com, mjonnalagedda@gmail.com

Abstract: - Mobile ad hoc networks (MANETs) have distinct features: like dynamic nodes, changing topologies, nodes cooperation and open communication media. Anonymity of message contents and participants is the most concerned task in MANET communication. Most of the existing methods face a challenge due to heavy cryptographic computation with high communication overheads. In this paper we propose an unconditionally secure privacy preserving message authentication scheme (PPMAS), which uses Modified New variant ElGamal signature Scheme (MNES). This scheme enables a sender to transmit messages, providing authentication along with anonymity, without relying on any trusted third parties. It also allows the untraceability of the link between the identifier of a node and its location. The experimental analysis of the proposed system is presented.

Key-Words: - Network security, Anonymity, Privacy, Mobile ad hoc networks, PPMAS, MNES.

1 Introduction

A set of mobile wireless devices having the capability of relaying packets for another in a cooperative manner is called as a mobile ad hoc network (MANET). The advantage of a MANET is that the disadvantages of wired networks and centralized administration issues are solved. The applications of MANET are manifold: battle ground communication, disaster recovery, conferencing and information sharing. The communication between the mobile nodes normally is performed through multi hop paths.

The main concern with the MANET is that the information about the nodes and their networks is to be made public. Many applications find this as a privacy threat. A node should be able to preserve its identity, its location and its network neighbours [8][17]. This privacy can be achieved using encryption.

The nodes in MANETs must be able to communicate messages in an authenticated manner securely. In addition to this the privacy of the node should be preserved making the node anonymous. Wireless MANETs are often found deployed where unfavorable conditions deter the deployment of a fixed wire network, where anonymity may be highly desirable for participating nodes. Consider a scenario in which members of an underground movement wish to share news about the crimes of an oppressive regime. Can an attacker detect who is producing the information and who is consuming it? Can an attacker ascertain other relationships between participating nodes and consequently punish them? Alternatively, consider a mobile combat unit operating inside enemy territory. Given that an enemy has set up a sensor network to eavesdrop on all communications, does the enemy know which node serves as a central leader or where forces are concentrated?

On account of quandaries such as these, anonymity in MANETs has become a subject of research in recent years, with several anonymization schemes