Chapter 12
Performance Evaluation of Secure Key Deployment and Exchange Protocol for MANETs

Alastair Nisbet
Massey University, New Zealand

M. A. Rashid
Massey University, New Zealand

ABSTRACT

Secure Key Deployment and Exchange Protocol (SKYE) is a new encryption Key Management Scheme (KMS) based on combination of features from recent protocols combined with new features for Mobile Ad Hoc Networks (MANETs). The design focuses on a truly ad hoc networking environment where geographical size of the network, numbers of network members, and mobility of the members is all unknown before deployment. Additionally, all key management is performed online making it distinct from most other implementations. This paper attempts to describe the process of development of the protocol and to more thoroughly discuss the simulation software design used to evaluate the performance of the proposed protocol. Simulation results show that security within the network can be increased by requiring more servers to collaborate to produce a certificate for the new member, or by requiring a higher trust threshold along the certificate request chain. SKYE works well within the limitations set by entirely online network formation and key management.

INTRODUCTION

Ad Hoc networks are distinguished from infrastructure networks in that the network members, or nodes, communicate directly with each other rather than through a fixed access point. They differ from a mesh network in that a truly ad hoc network is created 'on the fly' for a specific, sometimes spontaneous purpose, and is often disbanded soon after its usefulness has ended. Whilst a mesh network may consist of many stationary nodes, an ad hoc network will often be

DOI: 10.4018/978-1-4666-2482-5.ch012

very dynamic, with nodes frequently joining or leaving the network and with some nodes mobile throughout the network. It is this very dynamic nature of this type of network that creates such difficulties in implementing robust security.

Security implies control, whether it is by physical control of the network or control by some member or members who have power to control who may join the network. With a fixed wireless infrastructure, generally an access point or multiple access points will be preconfigured to control the network. These access points may be connected to a LAN or may simply act as a conduit for one node to communicate with another node. By forcing all communications to pass through an access point, even when nodes may be located within direct communication distance, the access point can maintain control over the network.

Security for MANETs includes five attributes: availability, authentication, confidentiality, integrity and non-repudiation. In an ad hoc environment, to achieve these five attributes firstly requires that any member of the network must be able to be identified. This is vital if malicious members are to be identified and permanently ejected from the network. A non-changeable identity can be linked to some unique physical attribute of the device such as the CPU serial number, meaning once that attribute is recorded, the node's behaviour can be monitored and if necessary the node's permission to join the network can be revoked. Additionally, robust encryption of the data is needed to prevent nodes reading messages intended only for an authorized recipient. This is especially necessary because of the nature of wireless communications. Generally, wireless devices transmit their messages omnidirectionally; meaning other similar devices within radio range can read the message. With radio ranges of at least several hundred metres for most wireless standards, preventing messages reaching unintended recipients is almost impossible to prevent. Therefore, encryption is one of the best methods for protecting the message from these unauthorized nodes. Whilst the data may be captured by unauthorized nodes, without the appropriate decryption key the message will remain unreadable and therefore secure. To encrypt and decrypt messages in a network, encryption keys must be created, distributed and when necessary revoked. Whilst several protocols have been proposed for these types of networks, one important aspect of the design is that it is both effective and efficient. Effectiveness can be measured by how well the protocol achieves its goal. The main goal is to create and distribute certificates to requesting nodes as they wish to join the network. Therefore, the success rate of the requests is a good measure. For efficiency, the measure is how the network performs as security is increased. Inevitably higher security will lead to a reduced success rate for certificate requests, and it is the impact on increasing security that can be used as a measure of efficiency.

There are two distinct encryption methods: symmetric key encryption where the same key is used for encryption and decryption, and asymmetric encryption where a public key is freely given out and is used to encrypt a message and a private key known only to the recipient is used to decrypt the message. Symmetric encryption is less computationally draining, but for total privacy of data it requires nodes to share the same secret key. This key creation and exchange can be done securely before network deployment or can be performed dynamically as required. Asymmetric encryption is robust, but requires the use of a Certificate Authority (CA) often called a Trusted Third Party, to create and distribute certificates validating the identities and the keys bound to those identities. Finding an efficient way to create and maintain an easily contactable CA is very challenging, especially when nodes in the network are mobile. However, with a truly ad hoc network where members have no prior knowledge or prior contact with each other, implementing control over the network is extremely difficult. The challenge in this area is to allow a highly dynamic network