An Efficient Certificate Management for Mobile Ad-Hoc Network

Dae-Young Lee\textsuperscript{1} and Hyun-Cheol Jeong\textsuperscript{2}

\textsuperscript{1} Dept. of Computer Science & Statistics, College of Natural Sciences of Chosun University
375 Seosuk-Dong, Dong-Gu, Gwang-Ju, 501-759, Korea
Tel.: +82-062-230-7962; Fax: +82-062-234-4326
cssna01@chosun.ac.kr

\textsuperscript{2} Dept. of Medical Engineering, Kwangju Health College
683-3 Shinchang-Dong Gwangsan-Gu Gwangju 506-701 Korea
Tel.: +82-62-958-7774; Fax: +82-62-953-4946
hcjeong@kjhc.ac.kr

Abstract. MANET has dynamic composition in which nodes are frequently changing, when a node is damaged, reliability between nodes may be changed and they may join in other administrative domains quickly they can rely on. This study suggests security requirements for MANET which can be a base of ubiquitous system and models that can prevent security threat through application of PKI without trusted certificate authority in MANET. It is also solve excessive loading found in centralized control model by dispersing CA for adjustment to dynamic changes of nodes of MANET quickly and suggests a system model which supports expansion so that existing nodes performing communication within clusters can provide active certificate service without being affected by input of new nodes. In addition, it is to evaluate its stability, effectiveness and strength through simulation of the suggested model.

1 Introduction

Mobile ad-hoc network (MANET) is composed of mobile nodes connected by wireless links. The nodes communicate through a wireless interface to forward packet data. This means that each node acts as a router that moves freely to transmit and receive data [1]. MANET does not require any fixed infrastructure. Since the nodes in the mobile ad-hoc network operate as routers and hosts without base stations or AP, they can forward packets on behalf of other nodes and run user applications [2]. The most appealing aspect of MANET is its independence from the central control, making the communication between mobile devices easier and more flexible.

All nodes are members of MANET. These node members are free to move randomly and form and reorganize even when some members are damaged by nodes dynamically joining and leaving the trusted administrative domains. MANET, however, is more vulnerable than fixed hardwired networks to information and physical security threats. Although there are an array of routing protocols and security mechanisms for mobile ad-hoc networks, wireless vulnerabilities still poses a major threat. Significant effort is underway in many research centers to resolve security problems in mobile ad-hoc networks [3][4][5].
This study proposes and evaluates a new public key-based security mechanism for MANET. The mechanism segregates the roles of certification authority to keep with the dynamic mobility of nodes and handle rapid and random topological changes with minimal overhead. That is, this model is characterized by its high expandability that allows the network to perform authentication service without the influence of joining and leaving nodes. The efficiency and security of this concept was evaluated through simulation.

2 System Composition

Once the cluster is formed, the cluster head acts as a certification authority for all its members and is responsible for establishing a new pair of public/secret keys to be used for certificate authentication. The cluster head will unicast its self-generated public key to other cluster heads through a network backbone. Thus the cluster heads hold shares of public key.

![Fig. 1. System Accomplishment process](image_url)

The certification authority verifies the feasibility of key-share by communicating all active cluster members \((k)\) using the trust relationships in the direct cross-certification. And then the cluster head unicasts its verified key value to other cluster heads for their own verification. If the verification fails, the sensor node requests the requesting cluster head to retransmit the key value. Once random numbers are successfully verified with shared secret key, the CA segregate secret key and assign a part of key to its cluster members. This means that the cluster head will request its neighboring cluster members to generate a partial certificate to sign public key certificates at the time of certificate creation. Each partial certificate is transmitted to the requesting node through cluster head. When the number of partial certificates exceeds the threshold number, the requesting node can combine partial certificates together and create a complete certificate.