Design of Modified CGA for Address Auto-configuration and Digital Signature in Hierarchical Mobile Ad-Hoc Network*

Hyewon K. Lee[1] and Youngsong Mun[2]

[1] Dept. of Computer Engineering, Daejin University, Pocheon, Korea
kerenlee@nate.com
[2] School of Computing, Soongsil University, Seoul, Korea
mun@computing.ssu.ac.kr

Abstract. The CGA (Cryptographically Generated Address) is designed to prevent address spoofing and stealing and to provide digital signature to users without certification authority or any other security infrastructures, but fake key generation and address collision appear in flat-tiered network. To solve these critical problems, CGA defines security parameter (SEC), which is set to high value when high security is required and vice versa. Although CGA with high SEC makes attackers be difficult to find fake key and to try address stealing, it brings an alarming increase in processing time to generate CGA. On the contrary, the probability to find a fake key is high if low SEC is applied to CGA. We propose modified CGA (MCGA), which is proper to mobile ad-hoc network. The proposed MCGA has shorter processing time than CGA and offers digital signature with no additional overheads. We have settled fake key and address collision problems by employing hierarchical network structure. The MCGA is applicable to as well public networks as ad-hoc networks. In this paper, we design mathematical model to analysis processing time for MCGA and CGA firstly and evaluate processing time via simulations, where processing time for MCGA is reduced down 3.3 times and 68,000 times, compared to CGA with SEC 0 and SEC 1, respectively. Further, we have proved that CGA is inappropriate for both ad-hoc networks and public networks when SEC is 3 or bigger than 3.

1 Introduction

Mobile ad-hoc network (MANET) is a multi-hop wireless network without any prepared base station. It is capable of building a mobile network automatically without any help from DHCP servers or routers to forward or to route messages. Significant difference from other wireless and wire-lined networks is continuous excessive changes of network topology without base station. Routing protocols such as DSR, AODV, TBRPF, etc. to find shortest or optimistic route have

* This work was supported by the Korea Research Foundation Grant. (KRF-2004-005-D00147).

I. Chong and K. Kawahara (Eds.): ICOIN 2006, LNCS 3961, pp. 217–226, 2006.
© Springer-Verlag Berlin Heidelberg 2006

been proposed, but these protocols assume that nodes have been pre-configured before building a network. To compensate these problems, MANETConf [1], automatic node configuration protocol [2] and prophet address allocation [3] have been proposed. [1] proposes address allocation and duplication avoidance in flat-tiered network, [2] proposes enhanced node auto-configuration protocol in hierarchical network and [3] suggests new IP address allocation algorithm, namely prophet allocation, which is expectable by initiating node; however, these protocols assume that address pool is already defined and they do not consider what kind of address is used in ad-hoc network.

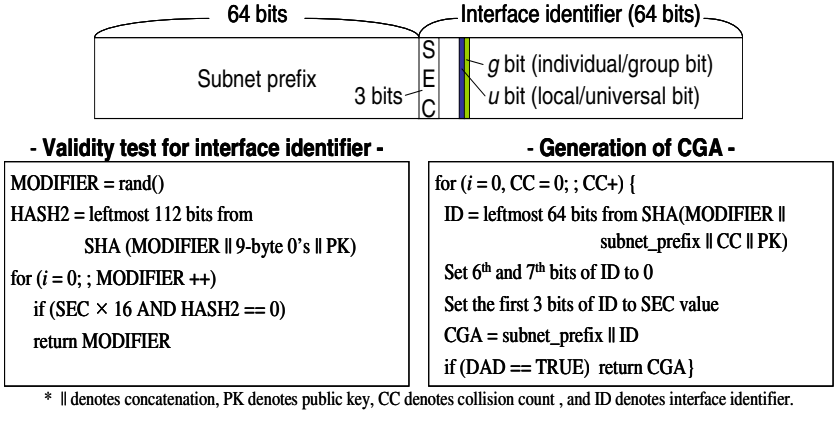

Fig. 1. CGA format

CGA (Cryptographically Generated Address) is designed to solve address spoofing and stealing attacks in IPv6. CGA offers digital signature without additional key opening process or help from certificate authority (CA), which is proper to mobile ad-hoc nodes that have low processing power and memory capacity. However, fake key generation and address collision appear in flat-tiered network due to 64-bit-taken operation from SHA's original output, as shown in Fig. 1. To solve this critical point, CGA defines 3-bit security parameter (SEC) field within IPv6 address and allows a node to generate address only when the specific condition[1] [4] in Fig. 1 is satisfied. When SEC is set to high value, it becomes more difficult for attackers to find fake key pair corresponding to origin key pair, but processing time to generate CGA increases incredibly, which eventually brings about high delay and defers communication. On the contrary, the probability to find a fake key is high when low SEC is applied to CGA. We propose modified CGA (MCGA), which is adjusted for mobile ad-hoc network. MCGA has shorter generation delay than CGA and offers digital signature with

[1] We call it as validity test for interface identifier in distinction from address validity test in section 2.4. The first test is done by an individual node on address generation, and the other is done by a receiver.