무선 네트워크에서의 초증가 수열을 통한 주소 은닉 기법 설계

천 준 호[†] · 김 성 찬[††] · 장 근 원[†††] · 도 경 화[††††] · 전 문 석[†††††]

요 약

대부분의 무선 네트워크 보안 기법은 암호학적인 안정성을 기반으로 통신 내용을 악의적인 호스트로 부터 보호하는 기밀성을 제공하지만 통신의 논리/물리적 주소를 노출시킨다. 이는 악의적인 노드에게 통신 내용은 숨길 수 있지만 대략의 전송량과 송신자와 수신자를 노출시키는 단점을 갖는다.

본 논문에서 제안하는 은닉주소 체계는 송신자와 수신자의 주소를 초증가 수열을 사용한 knapsack problem을 응용하여 생성된 은닉주소로 치환한다. 또한 은닉주소의 잦은 변환을 통해 악의적인 사용자가 공격 대상을 감시하거나 특정 호스트를 공격 대상으로 삼는 것을 원천적으로 차단한다. 이 기법은 공격 목표가 되는 호스트의 주소가 계속 변화하므로 DDoS 공격을 시도하려는 공격자가 공격 목표를 특정 할 수 없다.

키워드: 무선 네트워크 보안, DDoS, 초증가 수열, Knapsack Problem

Design of the Covered Address Generation using the Super Increasing Sequence in Wireless Networks

Junho Choun[†] · Sung-Chan Kim[††] · KunWon Jang[†††]
Kyung-Hwa Do[††††] · Moon-Seog Jun[†††††]

ABSTRACT

The General security method of wireless network provides a confidentiality of communication contents based on the cryptographic stability against a malicious host. However, this method exposes the logical and physical addresses of both sender and receiver, so transmission volume and identification of both may be exposed although concealing that content.

Covered address scheme that this paper proposes generates an address to which knapsack problem using super increasing sequence is applied, and replaces the addresses of sender and receiver with addresses from super increasing sequence. Also, proposed method changes frequently secret addresses, so a malicious user cannot watch a target system or try to attack the specific host. Proposed method also changes continuously a host address that attacker takes aim at. Accordingly, an attacker who tries to use DDoS attack cannot decide the specific target system.

Key Words : Wireless Security, DDoS, Super Increasing Sequence, Knapsack Problem

1. 서 론

무선 네트워크는 유선과는 달리 전파의 전방향성 때문에 전파 범위 내에 있는 모든 호스트에게 통신 내용을 전달 할 수밖에 없다. 현재 무선 네트워크 보안을 위해 사용되는 기법으로는 802.1x에서 사용되는 WEP과 Secure AODV에서 사용하는 Double signed message와 TESLA에서 사용되는 ACK-chain 등이 대표적이다. 대부분의 무선 네트워크 보안 기법들은 암호학적인 안정성을 기반으로 통신 내용을 악의적인 호스트로부터 보호하는 기밀성을 제공하지만 통신의 송신자와 수신자의 논리/물리적 주소를 노출시킨다. 이는 악의적인 노드에게 통신 내용은 숨길 수 있지만 대략의 전송량과 송수신자를 노출시키는 단점을 갖는다. 스테가노그래피를 사용하는 상황과 동일하게 통신 내용의 기밀성은 보장할 수 있으나 통신 내역 자체를 은폐하지는 못한다.

또한 CGA와 같이 암호학적으로 안전한 방법을 사용하면 스푸핑과 같은 공격에 효과적으로 대응하면서도 기밀성, 인증과 같은 보안 요구사항을 충족시킬 수는 있으나 송신자와 수신자의 주소를 노출시킨다는 점에서 DDoS 공격에 취약할 수 있다.

† 정 회 원 : 숭실대학교 대학원 컴퓨터학과 박사과정
†† 종신회원 : 숭실대학교 대학원 컴퓨터학과 박사과정
††† 준 회 원 : 숭실대학교 일반대학원 컴퓨터학과 공학박사
†††† 정 회 원 : 산자부 정보보안기술(JTC1/SC27) 전문위원회 운영위원
††††† 종신회원 : 숭실대학교 IT 대학 정교수
논문접수 : 2007년 5월 29일, 심사완료 : 2007년 7월 24일

본 논문에서 제안하는 은닉주소 체계는 무선 네트워크에서 송신자와 수신자의 주소를 초증가 수열을 통해 생성된 주소로 치환하여 악의적인 사용자가 공격 대상을 감시하거나 특정 호스트를 공격 대상으로 삼는 것을 원천적으로 차단한다. 또한 이 기법은 공격 목표가 되는 호스트의 주소가 계속 변화하므로 DDoS 공격을 시도하려는 공격자가 공격 목표를 특정 할 수 없다.

논문의 구성으로는 2장에서 본 논문에서 제안하는 주소체계를 생성하기 위해 필요한 배경인 초증가 수열과 knapsack 암호화 알고리즘을 설명하고, 3장에서는 제안한 주소를 생성 및 검증하는 방법을 설명한다. 4장에서는 제안한 주소체계의 성능을 평가하기 위해 전송량이 저하되는 정도를 통해 효율을 비교 평가한다. 5장에서는 제안된 주소체계의 장단점과 적용 가능한 범위를 고찰하고 향후연구를 제시하는 것으로 매듭짓는다.

2. 관련연구

2.1 Knapsack 암호화 알고리즘

Knapsack 암호화 알고리즘은 계산 복잡도가 지수승인 NP-Complete 문제 중의 하나인 Knapsack 문제에 근거를 둔다. 그러나 NP-Complete 상태를 유지하기 위해서는 250개 이상의 아이템, 즉 250개 이상의 항을 갖는 수열을 필요로하며, 각 항의 크기가 최소 200 비트 이상이어야 한다는 제약조건을 갖는다. 따라서 키의 교환과 보관과 폐기 등이 중시되는 전자서명에서는 RSA를 대신하지 못하지만 경량화된 암호화 알고리즘이 필요한 경우에 제한적으로 사용된다.

2.1.1 초증가 수열

일반적인 Knapsack 문제의 정확한 해를 구하기 위한 난이도는 아이템의 개수가 n일 때, $O(2^n)$의 난이도를 갖는 NP-Complete 문제이지만 특수한 제약 조건을 추가하여 난이도를 낮출 수 있다. 그 중 한 가지 방법이 식(1)과 같이 초증가 수열을 사용하는 것으로서, 초증가 수열 S^*는 이전 항의 모든 합이 다음 항 보다 작아야 한다.

$$S_{n+1} > \sum_{j=1}^{n} S_j \qquad (1)$$

초증가 수열의 항을 더한 수는 동일 수열 내의 다른 수를 더해서 만들 수 없다. 즉 식(2)와 같이 비트 스트림 Z^*를 적확히 알지 못하면 k를 복원 할 수 없다.

$$k = \sum_{i=1}^{n} S_i \times Z_i \qquad (Z^* = \{z_i | z_i = 0 \text{ or } z_i = 1\}) \qquad (2)$$

2.1.2 초증가 수열을 이용한 Knapsack 암호화 알고리즘

초증가 수열을 사용하는 것은 knapsack 문제의 난이도를 낮추기도 하지만 연산의 부하를 낮추는 방법으로도 사용 할 수 있다. 초증가 수열을 그대도 사용하는 것이 아니라 공개키 E를 식(3)과 같이 생성하여 암호화에 사용하고, 복호화에는 식(4)와 같이 p의 역원 p^{-1}을 사용한다.

$$E = \{e_i | e_i = S_i \times p \bmod m\} \quad (1 < n < p) \qquad (3)$$

$$p(p^{-1}) \equiv 1 (\bmod m) \qquad (4)$$

〈표 1〉 Knapsack 암호화 알고리즘의 계산 과정

암호화	복호화
S* = [2, 3, 6, 13, 27, 52]	Cipher Text C = 280
p = 31, m = 105	p = 31, p-1 = 61
2 * 31 mod 105 ≡ 62	
3 * 31 mod 105 ≡ 93	280 * 61 mod 105 ≡ 70
6 * 31 mod 105 ≡ 81	
13 * 31 mod 105 ≡ 88	70 = 2 + 3 + 13 + 52
27 * 31 mod 105 ≡ 102	
52 * 31 mod 105 ≡ 37	Plain Text = 110101
∴ E = [62, 93, 81, 88, 102, 37]	
Plain Text P = 110101	
→ 62 + 93 + 88 + 37 = 280	

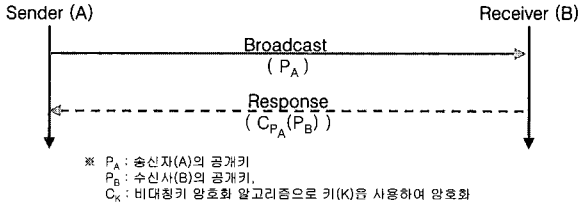
3. 제안된 은닉 주소 체계

본 논문에서는 Knapsack 암호화 알고리즘에 사용되는 초증가 수열과 Knapsack 알고리즘을 사용한다. 같은 호스트를 의미하지만 매번 다른 값을 갖는 주소체계를 만들기 위해 초증가 수열을 사용하고, 이를 복호화 및 검증하기 위해 Knapsack 알고리즘을 사용한다.

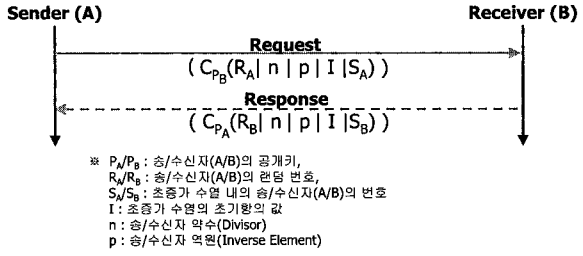
일반적인 Knapsack 문제는 NP-complete 문제이지만 초증가 수열을 사용하고 초증가 수열의 항의 개수를 비교적 작게 제한함으로써 NP-hard의 수준으로 낮추어 연산의 부하를 줄인다. 난이도의 저하 때문에 발생하는 보안성의 위협은 본 논문에서 제안하는 주소체계의 잦은 변화로 극복한다.

3.1 주소 생성을 위한 변수 교환

본 논문에서 제안하는 은닉주소의 생성 방식을 사용해서 최초로 통신을 시도하거나 갱신하고자 할 때, [그림 1]의 과정을 거친다. 통신을 시도하는 호스트 혹은 AP는 자신의 공개키 P_A를 브로드캐스팅하고, 수신측은 송신측의 공개키로 자신의 공개키 P_B를 암호화 하여 전송함으로써 응답한다.



(그림 1) 통신 요청과 응답



(그림 2) 변수 교환

수신측의 응답을 받은 송신측에서는 서로의 초증가 수열을 동기화하기 위한 변수를 [그림 2]와 같은 절차로 전송한다. 순서번호로 사용 할 난수 R_A과 초증가 수열의 생성에 필요한 약수와 역원인 n, p와 초증가 수열 내에서 몇 번째 항이 자신을 지칭하게 될지 의미하는 S_A와 초증가 수열 중 첫 번째 항이 될 I를 연접한 후 수신측의 공개키로 암호화하여 전송한다. 수신측은 자신의 개인키로 해당 메시지의 복호화에 성공하면 송신자에게 자신의 변수 R_B, S_B와 공통적으로 사용할 변수인 n, p, I를 연접한 후, 송신자의 공개키로 암호화하여 전송한다.

3.2 주소 생성

송/수신자는 식(3)과 같이 각자 임의의 초증가 수열을 생성한다. 첫 항은 3.1에서 합의된 I를 사용하며 다음 항으로 증가할 때는 난수 R을 공통적으로 사용하여 서로의 초증가 수열이 일치하도록 한다.

$$s_n = \sum_{k=1}^{n-1} s_n + R \tag{5}$$

동기화된 초증가 수열의 항을 식(4)와 같이 각자 무작위로 더한다.

단 서로를 지칭하게 되는 S_A/S_B는 반드시 포함한다. S_A/S_B만 포함시킨 후, 결과를 knapsack 알고리즘으로 복호화하며 S_A/S_B가 검출되면 서로를 인식할 수 있다. 그러나 매번 같은 항을 사용하게 되면 무작위 공격(brute-force attack)이나 사전공격(dictionary attack) 등에 취약할 수 있으므로 S_A/S_B를 제외한 나머지 항을 (표 3)과 같이 무작위로 더하여 매번 다른 합을 만든다.

$$\begin{aligned} e_A &= \sum_{i=1}^{n} (s_i \times Z_j) \times n \bmod p \\ e_B &= \sum_{i=1}^{n} (s_i \times Z_j) \times n \bmod p \end{aligned} \quad (Z_j = 0 \text{ or } 1) \tag{6}$$

$$\begin{aligned} e_A &= \sum_{i=1}^{n} (s_i \times Z_j) \times n \bmod p \\ e_B &= \sum_{i=1}^{n} (s_i \times Z_j) \times n \bmod p \end{aligned} \quad (Z_j = 0 \text{ or } 1) \tag{7}$$

〈표 2〉 초증가 수열에서 SA/SB의 배치

S_1	–	S_5	–	S_9	–	S_{13}	–
S_2	–	S_6	–	S_{10}	–	S_{14}	–
S_3	–	S_7	–	S_{11}	S_B	S_{15}	–
S_4	S_A	S_8	–	S_{12}	–	S_{16}	–

위 과정에서 얻어진 e_A/e_B는 식(3)과 같이 난수 R과 연접하여 해쉬한 후 앞의 48-bit를 취하여 본 논문이 제안한 은닉주소로 사용한다. 난수 R은 생성된 주소를 사전공격에 강인케하는 기능과 함께, 매번 전송할 때 마다 증가시켜 재전송 공격(replay-attack)을 막는데 사용한다.

$$\begin{aligned} &Covered\,Address\,of\,A = Left(Hash(e_A \mid R_A), 48) \\ &Covered\,Address\,of\,B = Left(Hash(e_B \mid R_B), 48) \end{aligned} \tag{8}$$

3.3 제안된 은닉주소의 검증

은닉주소를 수신한 호스트는 다음과 같은 절차를 거쳐 송신 호스트를 알 수 있다. 식(9)에서 초증가 수열 테이블의 S_A를 나타내는 항을 a_j, S_B를 나타내는 항을 a_k라고 할 때, aj와 a_k를 제외한 모든 항을 무작위로 더한 후, aj와 a_k는 반드시 더하도록 한다. 식(9)의 결과값 A를 식(10)과 같이 처리하여 얻은 값과 은닉주소가 일치하면 정당한 송신자의 은닉주소임을 확신한다.

$$\begin{cases} j < k \text{ and } k < n,\ A_i = \sum_{i=1}^{j-1}(a_i \times Z_i) + \sum_{i=j+1}^{k-1}(a_i \times Z_i) + \sum_{i=k+1}^{n}(a_i \times Z_i) + (a_j + a_k) \\ j < k \text{ and } k = n,\ A_i = \sum_{i=1}^{j-1}(a_i \times Z_i) + \sum_{i=j+1}^{n}(a_i \times Z_i) + (a_j + a_k) \\ j > k \text{ and } j < n,\ A_i = \sum_{i=1}^{k-1}(a_i \times Z_i) + \sum_{i=k+1}^{j-1}(a_i \times Z_i) + \sum_{i=j+1}^{n}(a_i \times Z_i) + (a_j + a_k) \\ j > k \text{ and } j = n,\ A_i = \sum_{i=1}^{k-1}(a_i \times Z_i) + \sum_{i=k+1}^{n} \end{cases} \tag{9}$$
$$(Z_j = 0 \text{ or } 1)$$

$$Covered\,Address\,of\,sender = Hash(\sum_{i=1}^{n}(A_i + R) \times n \bmod p, 48) \tag{10}$$
$$(Z_j = 0 \text{ or } 1)$$

3.4 제안된 은닉 주소 체계를 통한 통신 과정

서로의 초증가 수열을 일치시킨 두 호스트를 가정한다. 송신자는 송신자 주소를 만들기 위해 아래와 같은 절차를 거친다. 자신의 초증가 수열 표에서 자신을 지칭하는 항 k를 선택한다. 만일 항상 특정한 값으로 송/수신자 주소를 표기 할 경우 악의적인 호스트에 의해 파악 될 수 있으므로 주소를 생성 할 때 k외에도 아무 항이나 무작위로 하나 이상을 더한 후, 상대방과 교환되어 있는 난수 r을 연접하여 해쉬한다. 수신자는 상대방의 주소를 해석하기 위해 다음과 같은 절차를 거친다.

초증가 수열 표에서 모든 조합으로 얻을 수 있는 수를 미리 계산 한 후, 난수 r을 연접한 후 해쉬한 결과와 상대방의 주소를 대조하여 상대방을 확인한다.

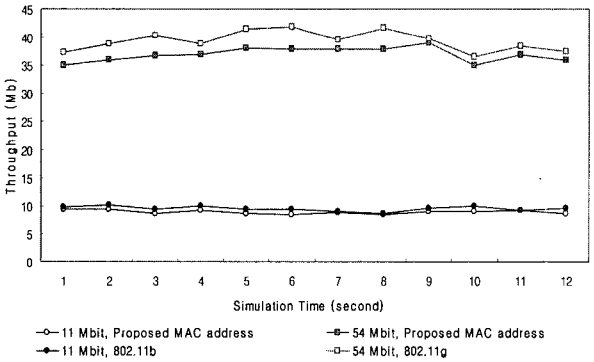
초증가 수열 표는 통신하고자 하는 모든 호스트의 수 만큼 생성 및 보관할 수도 있지만, 각 호스트를 지칭하는 k만 중복되지 않고 초증가 수열의 항을 무작위로 더하는 과정에서 다른 호스트를 지정하는 k를 제외시킨다면 단 한 개나 소수의 초증가 수열 표만으로도 제안된 은닉주소를 사용하는데 지장이 없다. 각 호스트별로 다른 난수를 사용하며 패킷이나 연결 마다 서로 다르게 무작위로 더해진 수가 사용되기 때문에 한 네트워크 내의 모든 호스트가 동일한 초증가 수열을 공유해도 무관하다. 그러나 호스트의 수가 증가하면 무작위로 더할 수 있는 수, 즉 호스트를 지칭하지 않는 항의 수가 감소하므로 중복된 은닉주소를 갖는 패킷의 수가 증가한다. 결과적으로 악의적인 노드에 의해 송신 호스트와 수신 호스트가 노출될 위험이 커지기 때문에 호스트의 수가 증가할수록 초증가 수열 표의 개수나 항의 개수를 증가시켜야 한다.

4. 제안된 은닉 주소 체계의 검증

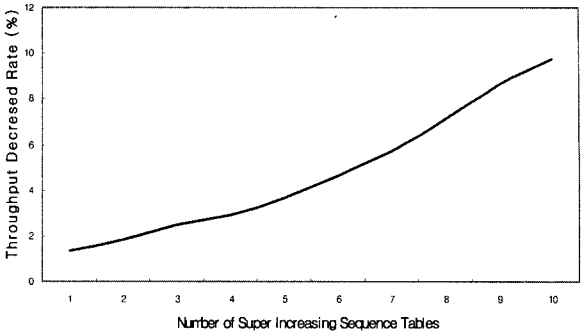
시뮬레이션은 버클리 대학 (U.C Berkeley)의 네트워크 시뮬레이터(Network Simulator 2.27)으로 구현하였으며 레드햇 계열의 리눅스 운영체제인 CentOS 8.0에서 수행하였다.

4.1 기존 주소 체계와의 전송량 비교

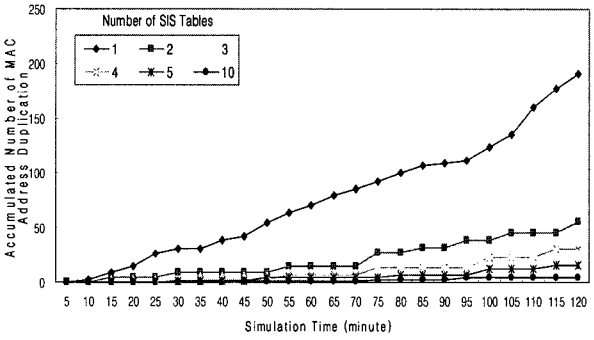
본 논문에서 제안하는 은닉주소의 실험을 위해 비교 대상으로 802.11a/g/b를 선정하고 초당 54Mbit/s와 11Mbit/s 두 가지 경우에 대해 실험하였다. 네트워크에는 40개의 호스트가 있는 것으로 가정하고 모든 호스트가 나머지 39개 호스트와 통신이 가능하도록 초증가 수열을 일치시킨 상황을 가정하였다. 초증가 수열은 120분 동안 실험한 결과 [그림 3]와 같이 평균 2.74%의 전송량 저하가 있었다. 기존의 주소 테이블을 조회하는 것에 비해 제안된 은닉주소는 탐색해야 할 항목이 많기 때문에 발생한 결과이다. [그림 4]는 위와 같은 방법으로 초증가 수열의 개수를 증가시키면서 변화하는 전송량의 추이를 나타낸 것이다. 초증가 수열 표의 개수와 반비례해서 전송량 저하가 발생하는데 이는 탬색해야 할 은닉주소의 증가가 원인이다.



(그림 3) 기존 무선 전송 방식과의 전송량 비교



(그림 4) 초증가 수열의 수에 따른 전송량 변화



(그림 5) 초증가 수열의 수에 따른 중복된 주소 발생 빈도

4.2 중복된 은닉주소의 발생 빈도

본 논문에서 제안하는 은닉주소는 각 패킷 마다 최대한 적은 빈도로 중복된 주소를 사용함으로써 악의적인 호스트가 특정 송수신 호스트를 파악하지 못하게 해야 한다. 그러나 주소의 중복을 막기 위해 n, p와 초증가 수열 표의 개수와 항의 개수가 증가하므로 주소 계산과 탐색에 소요되는 자원 때문에 전송량 저하를 초래할 수 있다. 따라서 호스트의 수가 적은 경우는 상대적으로 작은 값을 사용하고, 호스트의 수가 증가할 때는 초증가 수열 표의 개수를 증가시키면서 전송량 저하를 방지해야 한다.

[그림 5]는 120분 동안 진행한 실험에서 n, p의 크기에 따른 중복 횟수를 나타낸 것으로서 큰 값을 사용할수록 중복 빈도는 낮아진다.

4.3 DDoS 공격에 대한 대응

기존의 CGA는 암호화 기법으로 만들어진 주소체계이기 때문에 man-in-the-middle 공격이나 replay 공격에는 강인하다. 또한 spoofing을 시도해도 비대칭키 암호화 알고리즘의 특성 때문에 주소의 원래 소유자 이외에는 해당 패킷을 수신 할 수 없다. 그러나 CGA 주소가 노출되기 때문에 DDoS의 위협에 노출된다. 또한 CGA와 함께 사용되는 Credit 기반 시스템도 매우 작은 credit을 가진 무수히 많은 호스트의 공격은 방어할 수 없다.

본 논문이 제안한 주소 체계는 매번 주소가 바뀌므로 DDoS 공격의 목표 호스트를 특정 할 수 없다. 즉 공격하려

는 호스트의 주소를 찾을 수 없고, 주소 자체를 무작위로 선택하여 공격해야하므로 특정 호스트가 집중적인 부하를 받을 가능성이 매우 적어진다.

5. 결 론

본 논문에서 제안하는 은닉주소는 암호화를 통해 통신 내용의 기밀성이 보장되더라도 노출 될 수 밖에 없는 송수신 노드와 패킷 헤더의 정보 중 송신자와 수신자의 주소를 은닉함으로써 악의적인 노드의 간섭을 원천적으로 봉쇄하는데 효과적이다. 또한 무선 LAN을 통해 근거리에서 발생하는 네트워크 침해 사고나 ad-hoc network를 신뢰할 수 없는 지역에서 사용해야하는 경우에 악의적인 호스트가 특정 호스트를 공격 대상으로 선택하는 것을 방지하는데 효과적이다.

본 논문의 은닉 기법은 평문으로 전송되는 페이로드 부분의 기밀성을 보장하는 기능이 없으므로, 불특정 다수의 호스트가 섞여 있는 상황에서 자신의 통신 내역 자체를 은폐할 때, 별도의 암호화 프로토콜과 함께 사용하는 것이 바람직하다.

참 고 문 헌

[1] Leonard M. Adleman. On Breaking Generalized Knapsack Public Key Cryptosystems. In Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing. ACM, New York, 1983, pp.402-412.

[2] Gilles Brassard. A Note on the Complexity of Cryptography. IEEE Transactions on Information Theory, vol. IT-25, 1979, pp.232-233.

[3] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," Proceedings of the 27th Australasian Computer Science Conference (ACSC), vol. 26, no. 1, pp.47.54, 2004.

[4] M. G. Zapata, "Secure ad hoc on-demand distance vector (saodv) routing," IETF MANET, Internet Draft (work in progress), 2001.

[5] K. Wrona, "Distributed security: Ad hoc networks & beyond," in Proceedings of the Pampas Workshop 02, September 2002.

[6] Y.-C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security & Privacy, vol. 4, pp.28.39, May/June 2004.

[7] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002, pp.27.31.

[8] B. Preneel, Lectures on Data Security: Modern Cryptology in Theory and Practice. Heidelberg: Springer-Verlag, 1999, vol. 1561, ch. The State of Cryptographic Hash Functions, pp.158.182.

[9] 11.R.L.Rivest.RFC 1321 : The MD5 Message-Digest Algorithm, April 1992.

[10] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring", in Advances in Cryptology - EUROCRYPT'98, ed. K. Nyberg, LNCS 1403, Berlin: Springer-Verlag, pp.308-318, 1998.

[11] Guangjie Liu, Yuewei Dai, Zhiquan Wang, "Breaking Predictive-Coding-Based Steganography and Modification for Enhanced Security," International Journal of Computer Science and Network Security, Vol. 6 No. 3, pp.144-149, 2006.03.

천 준 호

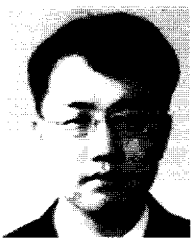
e-mail : opendr@ssu.ac.kr

2003년 숭실대학교 컴퓨터학과 졸업(학사)

2005년 숭실대학교 대학원 컴퓨터학과 졸업(공학석사)

2005년~현재 숭실대학교 대학원 컴퓨터학과(박사과정)

관심분야 : u-City, 암호학, 유무선 네트워크 보안



김 성 찬

e-mail : viper72@chol.net

2000년~현재 (주)유코레일 정보시스템부 차장

2002년 숭실대학교 정보과학대학원 정보통신학과 석사

2003년~현재 숭실대학교 대학원 컴퓨터학과 박사과정

관심분야 : 정보보호, 유무선 PKI, VPN, MPLS, 트래픽 엔지니어링, QoS 라우팅, DiffServ, 액티브 네트워크, NGN, BcN

장 근 원

e-mail : jaques@ssu.ac.kr

1998년 고려대학교 영어영문학과 졸업(학사)

2003년 숭실대학교 정보과학대학원 정보통신학과(공학석사)

2007년 숭실대학교 일반대학원 컴퓨터학과(공학박사)

관심분야 : 스테가노그래피, 센서네트워크, 정보보안 등

도 경 화

e-mail : khdo0905@nate.com

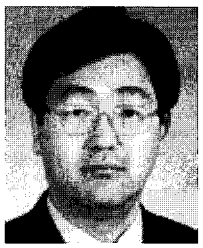
1999년~2004년 숭실대학교 컴퓨터학과 졸업(석·박사)

2001년~2003년 (주)매직캐슬정보통신 선임연구원

2004년~현재 행정자치부 전자정부본부 전문위원

2005년~현재 산자부 정보보안기술(JTC1/SC27) 전문위원회 운영위원

관심분야 : 정보보안, 전자정부, 개인정보보호, 유비쿼터스 보안, 네트워크보안, 스테가노그래피 등 차세대 기술 및 정책



전 문 석

e-mail : mjun@ssu.ac.kr

1980년 숭실대학교 전자계산학과(학사)

1986년 University of Maryland 전산과(석사)

1989년 University of Maryland 전산과(박사)

1989년 Morgan State University 전산수학과 조교수

1989년~1991년 New Mexico State University 부설 Physical Science Lab. 책임연구원

1991년~현재 숭실대학교 IT 대학 정교수

관심분야 : 컴퓨터 알고리즘, 병렬처리, VLSI 설계, 암호화, 스마트카드, 전자여권, 유무선 네트워크 보안 등