IP 스푸핑 공격 발생 시 유클리드 거리 기반의 트레이스 백 분석시간 개선 모델

유양* · 백현철** · 박재홍*** · 김상복****

요 약

오늘날 컴퓨터를 이용한 정보교환 방식은 다양하게 변화하고 있으며, 이를 이용한 불법적인 공격은 더욱 증가하고 있다. 특히 IP 스푸핑 공격은 그 특성상 DDoS 공격과 같은 자원고갈 공격을 수반하기 때문에 정확하고 빠른 탐지가 요구된다. IP 스푸핑 공격을 탐지하는 기존 방식에는 접속을 요청한 클라이언트의 트레이스 백 경로 정보를 서버에서 미리 보유하고 있는 정상적인 경로 정보와 비교하는 방식을 사용하고 있다. 그렇지만 이러한 공격 탐지 방식은 경로상에 존재하는 모든 라우터들의 IP 정보를 순차적으로 단순 비교하는 방식을 사용하기 때문에 빠르게 변화하는 공격을 탐지하고 대응하기에는 시간적 어려움이 존재한다. 본 논문에서는 이러한 문제를 개선하기 위하여 먼저 경로상에 존재하는 모든 라우터들의 IP에 해당하는 좌표값을 유클리드 거리 계산을 통하여 도출해 놓고, 이를 기반으로 트레이스 백 정보를 분석하여 공격 탐지를 위한 분석횟수를 개선할 수 있었다.

An Improved Model Design for Traceback Analysis Time Based on Euclidean Distance to IP Spoofing Attack

Liu Yang* · Baek Hyun Chul** · Park Jae Heung*** · Kim Sang Bok****

ABSTRACT

Now the ways in which information is exchanged by computers are changing, a variety of this information ex change method also requires corresponding change of responding to an illegal attack. Among these illega l attacks, the IP spoofing attack refers to the attack whose process are accompanied by DDoS attack an d resource exhaustion attack. The way to detect an IP spoofing attack is by using traceback informatio n. The basic traceback information analysis method is implemented by comparing and analyzing the nor mal router information from client with routing information existing in routing path on the server. There fore, Such an attack detection method use all routing IP information on the path in a sequential comparison. It 's difficulty to responding with rapidly changing attacks in time. In this paper, all IP addresses on the path to com pute in a coordinate manner. Based on this, it was possible to analyze the traceback information to improve the num ber of traceback required for attack detection.

Key words : IPSpoofing,Traceback, Euclidean distance

접수일(2017년 11월 30일), 수정일(1차: 2017년 12월 27일), 게재확정일(2017년 12월 29일)

* 경상대학교 컴퓨터과학과(책임저자)
** 경남도립남해대학 스마트융합정보과
*** 경상대학교 컴퓨터과학과
**** 경상대학교 컴퓨터과학과(교신저자)

1. 서 론

정보 통신 기술은 지속적인 발전 과정을 거쳐 빅데이터 서비스를 위한 네트워크 환경 구축을 요구하고 있으며, 이에 따른 네트워크 기반의 공격 기법도 새로운 네트워크 환경에 맞추어 다양한 공격 형태를 보이고 있다. 그러므로 온라인상으로 이루어지는 정보의 상호 교환에 따른 송/수신 정보 자료의 보안이 한층 필요한 시점이라고 할 수 있다[1-2].

불법적인 접근에 대한 보안 기법에는 특정 패턴을 비교 분석하여 불법적인 접근을 탐지 해 내는 기법과 OTP를 이용한 재인증 기법, 정상적인 사용자 외에는 원문을 볼 수 없도록 하는 암호화 기법을 일반적으로 사용하고 있다[3-5]. 하지만 이러한 개별 보안 기법들은 빅 데이터 서비스를 수행하는 새로운 네트워크 환경에는 많은 취약점을 보이고 있다.

빅 데이터 환경에서 원활한 정보 구축과 서비스를 수행하기 위해서는 클라우드 컴퓨팅 기술이 반드시 필요하다. 그렇지만 이러한 클라우드 환경은 불법적인 공격자들의 집중적인 공격 대상이 될 수 있다. 특히 고도의 불법적인 접근 방법을 숙지하고 있는 공격자들은 주로 IP 스푸핑 공격을 시도한다. IP 스푸핑 공격이란 클라우드를 구성하는 상호 신뢰호스트의 정보를 이용하여 클라우드 내의 다른 신뢰호스트를 불법적으로 공격하는 기술이다. 그러므로 클라우드 환경에서는 상호 신뢰호스트의 IP를 이용한 불법적인 공격 유형이 더욱 증가할 수 있다[6-7].

IP 스푸핑 공격에 대한 기존 탐지 방식에는 트레이스 백 정보를 비교하여 정상적인 접근 여부를 판정하는 방식을 사용하고 있다. 기존의 트레이스 백 분석 과정은 송/수신자 사이에 접속 요청 발생시 경유하는 라우터들의 정보를 실시간 비교 분석한 후 적절한 대응 과정을 수행하는 방식이다. 그렇지만 단순 트레이스 백 정보를 분석하는 과정은 경유하는 라우터들의 IP 정보를 모두 비교하기 때문에 이에 대한 오버헤드를 초래할 수 있다[8-10].

본 논문은 클라우드 환경에서 정상적인 사용자 분석 시간을 개선하기 위하여 수학적 유클리드 거리 계산식을 이용하였다.

본 논문의 유클리드 거리 좌표는 정상적인 경로상에 존재하는 라우터들이 보유하고 있는 IP 정보를 각 두 개씩 짝을 지어 거리 좌표로 사용하였다. 그 다음 이들 좌표 값을 기반으로 정상적인 사용자 판정 정보로 사용하여 분석시간을 개선할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문의 관련 연구를 살펴보고, 3장에서는 트레이스 백 정보를 이용한 유클리드 거리 좌표를 생성하는 과정을 보였다. 그 다음 4장에서는 유클리드 거리 계산을 통하여 도출한 좌표를 기반으로 기존의 트레이스 백 정보의 분석시간과 유클리드 거리 값을 이용한 분석시간을 비교하였다. 마지막 결론 부분은 트레이스 백 정보의 비교 분석 과정에서 요구되는 파라메터들에 대한 언급과 향후 이용 가능성에 대하여 논하였다.

2. 관련연구

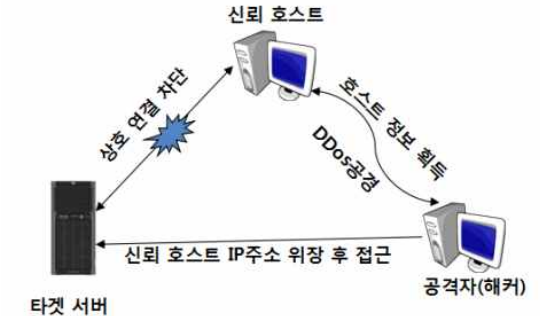
네트워크 상에 존재하는 호스트들은 상호 접속을 위하여 IP 정보를 이용한 인증 과정을 수행한다. IP 스푸핑 공격은 이러한 인증 과정의 취약점을 이용하여 신뢰호스트에 존재하는 IP 정보를 이용하여 공격자 자신이 신뢰호스트로 위장한 후 불법적인 접속을 시도하는 공격이다. 기존의 IP 스푸핑 공격을 탐지하기 위한 연구에는 정상적인 송/수신자들의 경로를 획득한 후 이를 기반으로 접속이 발생할 경우 트레이스 백을 수행하여 상호 비교하는 방식을 채택하고 있다. 그렇지만 이러한 비교 방식은 트레이스 백 정보를 이진수나 십진수 형태로 비교하기 때문에 홉 수가 증가하면 할수록 비교 과정에 많은 시간을 낭비하게 된다. 이에 따라 본 논문은 이를 개선하기 위해 유클리드 거리 계산을 통하여 이러한 부분을 개선하였다.

2.1 IP Spoofing

스푸핑이란 원래 '속이다, 사기치다'라는 의미를 가지고 있다. 네트워크를 이용한 다양한 공격 중 심각한 결과를 초래한 공격 유형에는 IP 스푸핑 공격이 거의 대부분이다.

네트워크상에 존재하는 신뢰 호스트들은 접근 과정의 인증을 위하여 상호 IP 주소를 이용하고 있다. IP

스푸핑이란 인증 과정에 필요한 특정 호스트의 IP를 강탈한 후 (그림 1)과 같은 과정을 수행하여 정상적인 호스트에 대한 불법적인 접속을 시도하는 공격이다. 또한 실질적인 타겟 호스트의 공격 과정에 IP를 강탈한 호스트를 다운시키기 위하여 서비스 거부 공격 등을 시도한다[11]. 그러므로 향후 클라우드 서비스 환경에서 집중적으로 발생할 수 있는 공격 기법이라고 할 수 있다.



(그림 1) IP 스푸핑 과정

2.2 트레이스 백

트레이스 백이란 송신자와 수신자의 상호 접속을 위하여 경로를 구축하고 있는 라우터들의 IP를 추적하여 해당 정보를 제공해 주는 프로그램이다[12].

본 논문에서는 트레이스 백 과정에서 생성되는 라우터들의 IP 정보를 유클리드 거리로 계산하고 그 결과를 분석 비교 값으로 이용하였다.

2.3 유클리드 거리

유클리드 거리는 두 점 사이의 거리 계산이 필요할 경우 일반적으로 사용하는 방법이다. 본 논문에서는 트레이스 백에 의하여 생성되는 경유 라우터들의 IP 정보를 각각 두 개의 쌍으로 조합하여 유클리드 좌표값으로 생성하여 분석 수행 자료로 사용하였다. 아울러 유클리드 좌표 값을 계산하기 위하여 유클리드 거리에 대응하는 직교 좌표계의 두 점이 필요하다. 즉, p = (p1, p2, ..., pn)와 q = (q1, q2, ..., qn)가 존재한다고 할 때, 두 점 p, q의 거리는 다음과 같이 계산할 수 있다[14-15].

유클리드 거리 좌표 유도식

$= \quad , L \ , d_E\}$

$R^2 = \{(p,q) | p,q \in R\}$

L_E 모는 직선의 집합

임의의 두 점 $p = (x_1, y_1), q = (x_2, y_2)$에 대해

$d_E(p,q) = \quad (x_1 - y_1)^2 + (x_2 - y_2)^2$

3. 제안 모델 동작 과정

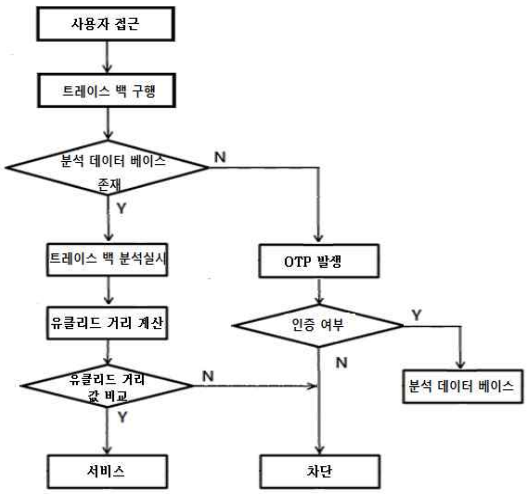
본 논문에서 제안하고 있는 분석시간 개선 모델은 일반적인 네트워크 상황에서 발생하는 과정을 기반으로 하였으며, 그 처리 과정은 (그림 2)와 같다.

먼저 클라우드를 구성하고 있는 신뢰호스트로 사용자 접근이 발생하면 해당 접속자에 대하여 트레이스 백을 수행한다. 이 때 접속자의 IP 정보가 분석데이터베이스에 없는 경우에는 OTP를 발생시켜 인증 과정을 수행하도록 한다. 그 다음 인증을 완료하면 분석데이터베이스에 새로운 정상 접근경로로 등록하고, 인증에 실패하면 공격자 정보로 등록한다.

그 다음 해당 접속자가 기존 분석 데이터베이스에 존재하는 IP 사용자이면 트레이스 백 정보의 분석 과정을 수행한다. 이러한 분석 과정은 미리 트레이스 백을 수행하여 획득한 경로상에 존재하는 라우터들의 IP 정보를 기반으로 유클리드 거리 좌표 값으로 구축해 놓은 정보를 이용하여 수행한다.

기존의 트레이스 백 정보 기반의 IP 스푸핑 탐지를 위한 연구에서는 트레이스 백 정보를 이진수나, 십진수 형태로, 각 구간 경로 정보를 분석하여 정상적인 접속자 유무를 판정하는 방식을 채택하고 있다. 그렇지만 이러한 트레이스 백 정보의 비교 분석 과정은 해당 경로상에 존재하는 홉의 수가 증가함에 따라 분석에 더 많은 시간을 요구하고 있다.

본 논문에서는 유클리드 거리 값 계산 결과를 기반으로 비교 분석을 수행하기 때문에 기존의 분석 시간을 단축할 수 있었다.



(그림 2) 제안 모델의 탐지 분석 과정

4. 실험 및 평가

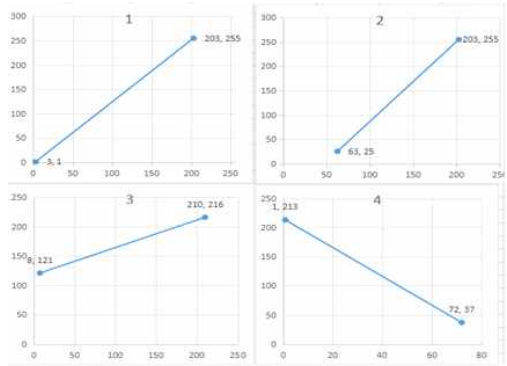
본 논문의 실험을 위한 트레이스 백 정보 획득은 본 연구자의 컴퓨터를 출발지로 하고 국내 임의 지역의 서버를 목적지로 하여 해당 정보를 (그림 3), (그림 4)와 같이 획득하였다. (그림 3), (그림 4)의 트레이스 백 정보를 분석해 보면, 동일한 출발지 IP를 이용한 접근이 발생했지만 경로상에 존재하는 라우터의 IP 정보가 동일하지 않다는 것을 알 수 있다.

(그림 3) 트레이스 백 정보 결과 1

(그림 4) 트레이스 백 정보 결과 2

즉, 공격자가 IP 스푸핑 공격을 시도하여 기존의 정상적인 트레이스 백 정보와 상이한 결과를 나타내는 과정을 보이는 것으로 가정할 수 있다. 그러므로 트레이스 백 정보의 분석 과정에서 상이한 정보를 신속하게 탐지를 하는 것이 공격 대응 시간을 단축할 수 있다.

(그림 5)는 트레이스 백 정보를 이용하여 경유 라우터들의 IP 정보를 유클리드 거리 값으로 나타낸 것이다. 이는 향후 접속자들의 트레이스 백 정보를 획득하여 이를 유클리드 거리값으로 분석한 후 상호 비교분석 과정에 사용하기 위한 자료이다.



(그림 5) IP 쌍을 이용한 거리 좌표

(그림 6)은 (그림 3), (그림 4)의 트레이스 백 과정

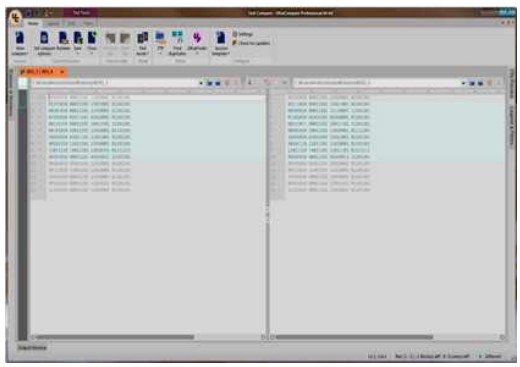
에서 존재하는 홉들의 IP정보를 이용하여 유클리드 거리로 계산한 값을 표로 나타낸 것이다.

HOP개 수	X1	X2	Y1	Y2	Euclidean distance.1
1	203	3	255	1	323.289
2	203	63	255	25	269.258
3	210	8	216	121	223.224
4	1	72	213	37	189.781
5	1	150	213	69	207.212
6	1	146	208	141	159.731
7	1	148	213	29	235.510
8	1	107	208	177	110.440
9	1	107	208	78	167.738
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

HOP개 수	X1	X2	Y1	Y2	Euclidean distance.2
1	203	3	255	1	323.289
2	112	30	174	65	136.400
3	112	73	174	149	46.325
4	112	209	174	1	198.338
5	112	205	174	53	152.611
6	112	38	174	2	187.243
7	128	10	134	178	125.936
8	203	169	246	163	89.694
9	203	170	246	242	33.242
10	1	151	208	222	150.652
11	116	67	0	102	113.159
12	116	67	0	190	196.217
13	72	2	52	184	149.412
14	72	2	52	189	153.847
15	72	4	52	122	97.591

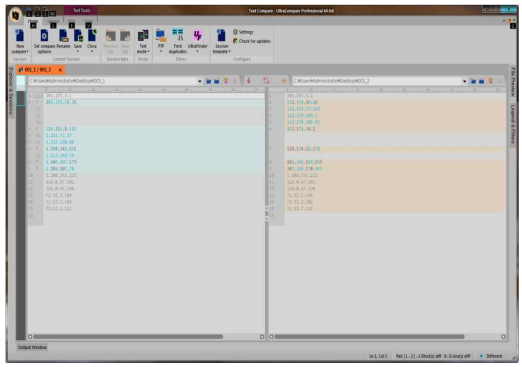
(그림 6) 유클리드 거리 계산 과정

본 논문에서는 접속자에 대한 트레이스 백 정보 분석과 관련하여 분석시간의 개선을 위하여 유클리드 거리 좌표 값을 이용하고 있다. 또한 각 홉의 IP 정보는 비교분석을 위하여 2진수, 10진수 형태로 수집되어 저장 할 수 있다. 본 논문에서는 이러한 IP 정보를 비교 분석하기 위하여 강력한 비교병합 프로그램인 울트라컴페어 프로페셔널을 이용하여 (그림 7), (그림 8), (그림 9)로 나타내었다.



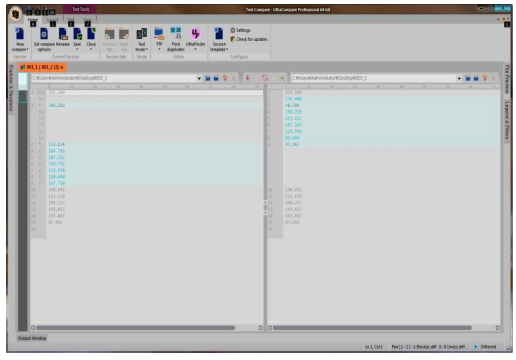
(그림 7) 2진수에 기반한 트레이스 백 분석

(그림 7)은 트레이스 백 정보를 수집한 결과 해당 정보를 2진수로 수집하여 비교한 결과를 나타낸 것이다. IP정보는 기본적으로 4개의 옥텟으로 구성되기 때문에 이를 위한 비교 횟수는 홉 1개당 32회의 비교과정을 수행하기 때문에 15개 홉에서는 총 480회의 분석이 이루어져야 한다.



(그림 8) 10진수에 기반한 트레이스 백 분석

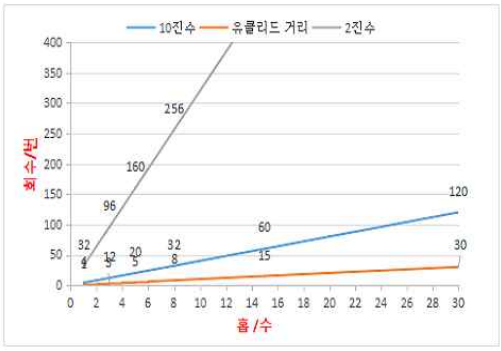
(그림 8)은 트레이스 백 정보를 수집한 결과 해당 정보를 10진수로 수집하여 비교한 결과를 나타낸 것이다. 이 경우 IP정보는 기본적으로 홉 당 10진수 4개로 구성되기 때문에 이를 위한 비교 횟수는 홉 1개당 4회의 비교과정을 수행하기 때문에 15개 홉에서는 총 60회의 분석이 이루어진다.



(그림 9) 유클리드 거리 값에 기반한
트레이스 백 분석

(그림 9)는 트레이스 백 정보를 수집한 결과 해당 정보를 유클리드 거리 값을 기반으로 분석 자료 값을

생성한 후 분석 횟수를 나타낸 것이다. 이 경우 홉의 개수에 해당하는 비교 분석 과정을 15회 수행하게 된다.



(그림 10) 홉당 비교 회수

(그림 10)은 접근을 시도한 시스템으로 트레이스 백을 수행하여 획득한 각 홉의 정보를 2진수, 10진수 형태로 수집한 것과, 본 논문에서 주장하는 유클리드 거리 좌표 값을 이용하여 그 비교 과정을 그래프로 나타낸 것이다. 그 결과 일반적인 트레이스 백 정보를 수집하여 비교 분석을 수행하는 경우보다 유클리드 거리 값을 계산한 후 해당 좌표 값을 비교하는 과정이 분석에 필요한 횟수를 감소시킬 수 있다는 것을 알 수 있었다. 이상의 내용은 다음 <표 1>과 같다.

<표 1> 홉의 수에 따른 분석 자료 비교횟수

홉 수 / 분석자료	2진수 비교횟수	10진수 비교횟수	유클리드 좌표값
8	256	32	8
15	480	60	15

5. 결 론

네트워크가 없는 우리의 일상생활은 생각할 수도 없다. 그러므로 네트워크 환경도 다양한 방향으로 발전하고 있으며 이에 따른 빠르고 안정적인 보안 서비스가 필요한 시점이다.

일반적인 트러스트 기반의 네트워크 환경에서는 불법적인 IP 스푸핑 공격에 대응하기 위하여 트레이스 백 정보의 단순 비교를 수행하는 방식을 사용하고 있다. 그렇지만 이러한 비교 방식은 트레이스 백을 수집하여 각 홉들의 IP 정보를 단순하게 비교하기 때문에 송/수신자의 네트워크 경로상에 존재하는 홉의 수가 증가할수록 비교 분석에 많은 시간이 소요된다.

IP 스푸핑 기법은 공격의 특성상 반드시 사전 공격으로 자원고갈 공격이 발생한다. 이러한 자원 고갈 공격은 빅데이터 서비스를 구축하는 클라우드 네트워크 환경에 대하여 그 공격 양상을 다양하게 나타낼 수 있기 때문에 IP 스푸핑 공격 발생시 신속한 탐지가 더욱 요구되고 있는 시점이다.

본 논문은 이러한 공격을 탐지하는데 있어 분석과정에 필요한 시간 단축과 빠른 대응을 위하여 유클리드 거리 값 계산을 통한 좌표 값을 이용하고 있다. 즉, 해당 좌표 값들은 송/수신 경로상에 존재하는 각 홉들의 IP 정보를 쌍으로 묶은 후 이를 유클리드 거리 값으로 계산해 낸 정보라고 할 수 있다. 이는 홉이 보유하고 있는 IP들에 대한 비교 분석 횟수를 감소시킬 수 있으며, 탐지에 필요한 일반적인 파라메터들을 상수로 가정할 경우 해당 트레이스 백 정보의 분석시간을 감소시킬 수 있다고 본다.

본 논문에서는 이들 좌표 값들을 사전에 구축해 두고, 접근이 발생하면 트레이스 백을 실시하여 신속한 비교 분석 과정을 수행할 수 있도록 하였다.

미래의 사회는 클라우드와 사물인터넷 환경이 네트워크 분야를 주도하게 된다. 그렇지만 이러한 네트워크 환경의 변화는 네트워크를 이용한 공격 기법의 다변화도 가져 올 것이다. 본 연구는 빠르고 다양하게 변하고 있는 공격 형태에 능동적이고 신속한 대응을 할 수 있도록 분석 횟수의 감소를 통하여 공격 탐지에 대한 시간을 개선한 연구이다.

향후 연구 과제로 공격 탐지에 필요한 일반화가 가능한 파라메터들의 정확한 분석을 통하여 효율적인 공격 탐지가 가능한 데이터베이스 구축이 필요하다고 본다.

참 고 문 헌

[1] Telecommunication Technology Association 2008. Botnat trend and respond technology present, TTA Journal, 118(Special Report) : 58-65.

[2] J.z. Li, and X.M. Liu An important aspect of big data : Data usability, School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, pp. 1147~1162, 2013.

[3] R-W. Huang, X-L. Gui, S. Yu, and W. Zhuang, Privacy-Preserving Computable Encryption Scheme of Cloud Computing, Chinese Journal of Computers, Vol. 34, No. 12, pp. 2391~2402, 2011.

[4] Lee, A (1999). Guideline for Implementing Cryptography in the Federal Government. Nist SP 800-21.112.

[5] Gueron, S. (2008). Advanced Encryption Standard (AES) Instructions Set. White paper of Inter.

[6] X-F. Meng, and X-B. Ci, Data management : Concepts, techniques and challenges, School of Information, Renmin University of China, Beijing 100872, pp. 146~169, 2013.

[7] J.H. Sun, and K.J. Kim, Cloud Computing in the Vulerability Analysis for Personal Information Security, Journal of Information and Security, Vol. 10, No. 4, pp. 77~82, 2010.

[8] H-D. Lee, H-T. Ha, H-C Baek, C-G. Kim, and S-B. Kim, Efficient detction and defence model against IP spoofing attack through cooperation of trusted hosts, Journal of the Korea Institute of Information and Communication Engineering, Vol. 24, No. 12, pp. 2649~2656, 2012.

[9] Y-T. Mu, H-C. Baek, J-Y. Choi, W-C. Jeong, and S-B. Kim, A Proposal of a Defence Model for the Abnormal Data Collection using Trace Back Information in Big Data Environments, Journal of the Korea Institute of Information and Communication Engineering, Vol. 10, No. 2, pp. 153~162, 2015.

[10] Joon Heo, Detecting Abnormal SIP (Session Initiation Protocol) Traffic using Statistical Distribution Estimation. Journal of KISS : Software and Applications 38(11), 2011.11, 606-612.

[11] Shin, Y. H. Lim, G. H and Im, E. G. 2009. A Research on the possibility of ARP spoofing attack in SCADA System Based on TCP/IP environment. Convergence security journal, 9(3) : 9-17.

[12] M-H Kim, H-C Beak, S-W Hong and J-H Park, 2015. An Encrypted Service Data Model for Using Illegal Applications of the Government Civil Affairs Service under Big Data Environments, Convergence security journal, 15(7) : 31-38.

[13] Woochan Hong, Kwangwoo Lee, Seungjoo Kim and Dongho Won. Vulnerabilities Andlysis of the OTP Implemented on a PC, DOI; 10.3745/KIPSTC. 2010.17C.4.361.

[14] Shuang Li, Seog Geun Kang, Design of 3-Dimensional Cross-Lattice Signal Constellations with Increased Compactness. Journal of the Korea Institute of Information and Communication Engineering, Vol.20, No.4 : 715~720 Apr. 2016.

[15] M-S Kim, J-H Kim, J-H Wo, L-S Lee and B-H Kim, A function of a variety of distance in accordance with the definition of a regular polygon. The Korean Soc. Math. Ed. Proceedings of the 47th National Meeting of Math. Ed. November 4-5, 2011, 259-268.

〔저자소개〕

유 양 (Liu Yang)
2014년 2월 경상대학교
컴퓨터과학과 학사
2016년 2월 경상대학교
컴퓨터과학과 석사
2016년 3월 ~ 현재 : 경상대학교
컴퓨터과학과 박사과정

email : a2633558a@naver.com

백 현 철 (Hyun Chul Baek)
1988년 2월 경상대학교
전산통계학과 학사
1998년 8월 경상대학교
전산교육 석사
2003년 2월 경상대학교
컴퓨터과학과 박사
2013년 3월 ~ 현재 : 경남도립
남해대학 산학협력중점교수

email : dosi_gas@nate.com

박 재 흥 (Park Jae Heung)
1978년 2월 충북대학교
수학교육과 학사
1980년 9월 중앙대학교
전자계산학과 석사
1989년 8월 중앙대학교
전자계산학과 박사
1984년 4월 ~ 현재 : 경상대학교
컴퓨터과학과 교수

email : pjh@gnu.ac.kr

김 상 복 (Sang Bok Kim)
1979년 2월 중앙대학교
전자공학과 학사
1981년 2월 중앙대학교
전자공학과 석사
1989년 2월 중앙대학교
전자공학과 박사
1984년 3월 ~ 현재 : 경상대학교
컴퓨터과학과 교수

email : sbkim@gnu.ac.kr