실시간 위협에서 Event 유형의 정형화 설계 및 구현*

이동휘** · 이동춘*** · 김귀남**

요 약

실시간 사이버위협에서 정형화 방법은 각 보안장비의 이벤트를 실시간 분석하여 인터넷 웜, 바이러스, 해킹 등의 사이버공격에 대한 네트워크 이상 징후를 임계치와 상관관계를 틀 통하여 탐지하고, 동 평가결과의 통계분석을 통해 정형화 방안 기능을 부여하고 실효성 있는 사이버공격대응시스템을 구축하는데 있다. 본 논문은 우선 위협지표 산출과 동 지표의 합산을 통한 위협평가 및 조기 경보 과정의 패키지화로 만들고, 사이버 위협 지표 계산의 기준을 설정 한다. 특히 보안사고 발생 시 각 보안장비의 이벤트와 트래픽 양에 대한 정의 및 데이터베이스 입력 방법을 구체화하여 실시간 대응 및 조기예경보체계의 초석이 가능한 정형화 방안을 제시 한다. 분석을 위해 축적한 90일간의 데이터 임계치 설정작업을 통해 보다 정확한 적용 값을 계산 한다. 산출한 값을 토대로 정형화가 가능한 보안이벤트 정보를 표준데이터로 적용, 각 보안장비 및 HoneyNet 시스템, 기타 취약정보 등과의 상관관계를 분석하여 보안이벤트 표준지수를 산출 한다.

Standardization Model and Implementation of Event Type in Real Time Cyber Threat

Dong Hwi Lee** · Dong Chun Lee*** · Kuinam J. Kim**

ABSTRACT

The method which research a standardization from real time cyber threat is finding the suspicious indication above the attack against cyber space include internet worm, virus and hacking using analysis the event of each security system through correlation with the critical point, and draft a general standardization plan through statistical analysis of this evaluation result. It means that becomes the basis which constructs the effective cyber attack response system. Especially at the time of security accident occurrence, It overcomes the problem of existing security system through a definition of the event of security system and traffic volume and a concretize of database input method, and propose the standardization plan which is the cornerstone real time response and early warning system. a general standardization plan of this paper summarizes that put out of threat index, threat rating through adding this index and the package of early warning process, output a basis of cyber threat index calculation.

Key words : Real Time Cyber Threat, Security Event, Standardization

---

* 본 연구는 2006년 산자부 RIC 학술연구비 사업 지원으로 수행되었음.

** 경기대학교 정보보호학과

*** 호원대학교 국방과학기술대학

1. 서 론

오늘날 국내 · 외 보안기관에서는 정보통신망에 대한 사이버공격 징후를 포착하거나 사이버공격 발생이 예상되는 경우, 그 위협 또는 위험의 수준을 평가하여 단계적으로 경보를 발령하는 대응체계를 유지하고 있다. 또한, 국내 · 외 보안업체들도 자체적인 평가를 통해 웜 · 바이러스 또는 보안취약점 등에 대한 위험등급을 게시하고 사용자의 주의를 당부하고 있다[1].

사이버위협 경보체계는 국가 · 공공기관, 민간업체, 개인사용자 등이 경보수준에 따라 사이버위협에 효과적으로 대처함으로써 사고예방 및 피해를 최소화 할 수 있고, 사이버위협 경보 수준에 적합한 대응 요령을 제시함으로써 국가적 혼란과 비효율성을 제거할 수 있다[2]. 또한 사이버안전 관련 보안 이벤트는 각각의 포맷에 따라 통합화 할 수가 없었다. 정보통신망의 보안담당자는 이러한 사이버위협 이벤트를 다루는 통합보안시스템이 출시하고 있지만 계량적으로 보여줌으로써 실시간 위협에 도움을 주지 못하고 있다.

본 논문은 실시간 사이버위협상에서 각 보안장비의 이벤트를 실시간 분석하여 인터넷 웜, 바이러스, 해킹 등의 사이버공격에 대한 네트워크 이상징후를 임계치와 이벤트 지수를 상관관계를 통하여 분석하고, 동 평가결과를 통계분석을 통해 실효성 있는 정형화 기법을 제안 한다. 특히 보안사고 발생 시 각 보안장비의 이벤트와 트래픽 양에 대한 정의 및 데이터베이스 입력 방법을 구체화하여 기존보안 시스템의 문제점을 극복하고 실시간 대응 및 조기예경보체계의 기반이 가능한 정형화를 연구 한다.

정형화 방법은 우선 위협지표 산출과 동 지표의 합산을 통한 위협평가 과정의 패키지화로 정리할 수 있으며, 사이버 위협 지표 계산의 기준을 산출해야 한다. 분석을 위해 축적한 90일간의 데이터 임계치 설정작업을 통해 보다 정확한 적용 값을 산출 한다. 산출한 값을 토대로 정형화가 가능한 보안이벤트 정보를 표준데이터로 적용, 각 보안장비 및 허니넷 시스템, 기타 취약정보 등과의 상관관계를 분석하여 보안 이벤트 표준지수를 계산한다.

2. 관련 연구

2.1 개별적 위협도 평가

개별적 위협도 평가는 웜 · 바이러스, 보안취약점, 해킹 기법 등 각각의 사이버위협에 대해서, 실제로 발생이 가능한 위해 가능성을 평가하는 단계이다. 개별적 위협도 평가는 해당 위협이 가지고 있는 특성을 중심으로 평가되며, 향후의 발생 가능성 또는 잠재적으로 확장 가능한 속성에 대해서는 평가하지 않는다. 따라서 개별적 위협도 평가는 시간의 흐름에 따라서 해당 값의 변화가 거의 없다. 개별적 위협도를 평가하기 위해서 웜 · 바이러스 위협도 평가기준, 보안 취약점 위협도 평가기준, 해킹 기법 위협도 평가기준이 요구된다.

일반적인 웜 · 바이러스의 특성은 감염대상 획득, 악성코드전송, 악성코드 실행 및 추가 작업으로 분류될 수 있다.

이러한 웜 · 바이러스특성을 통해 우리는 감염대상 획득, 감염경로, 감염 시 증상을 기준으로, 방어조치난이도, 자산유형, 국내 외 보안관련 업체의 평가결과 및 평가기관의 소견을 종합하여 개별 위험도를 평가 할 수 있다[3-5].

2.2 트래픽 정형화 연구

Hellerstein(2001)이 트래픽의 정형화를 위해 Seasonal ARIMA모형을 적용하여 기간망(Infrastructure Network)의 주간 트래픽 양을 임계치와 정형화를 통해 예측한 것이 그 사례이다[7]. 또한

F. Zang(2000)은 Seasonal ARIMA 모형을 활용하여 무선통신의 트래픽을 정형화하여 예측하였고[8] Y. Shu는 퍼지-자기회기 모형(Fuzzy AR model)으로 비선형적이고 비 정류적인 고속 네트워크 트래픽을 예측하는데 적합한 방법을 제시하였다[9].

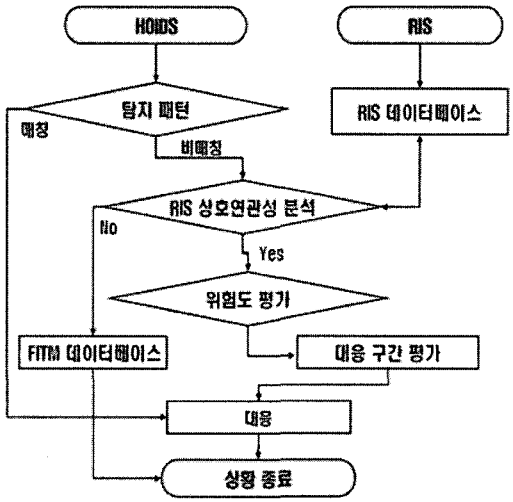
Hellerstein, F. Zang 그리고 Y. Shu 등이 사용한 기법들의 가장 큰 공통점은 대규모 트래픽 양이 폭주하는 상황 및 이상 징후 발생에 대해 임계치 분석기법에 의한 상황예측이 가능한 모델을 제시하였다는 점이다. 그러나 최근 트래픽 폭주 유발 위협의 특성이 단순한 포트공격, 또는 순차적인 공격이 아닌 인공지능적인 기법과 불규칙 공격속도에 따른 확산공격방법으로 진화하고 있기 때문에 [6] 단순히 트래픽을 계량적으로만 판별한 방법만 의존한 분석기법으로는 최근 사이버위협에 대한 예측이 어려울 수 밖에 없다. 그 때문에 보안 이벤트에 대한 정형화 방안에 대한 연구가 필요하다.

3. 실시간 사이버위협에서 이벤트 유형의 정형화

3.1 트래픽와 비 매칭 보안이벤트 상관분석을 통한 정형화 기법

사이버 보안 이벤트에 대한 정형화 기법은 기존 네트워크 구조에서 RIS(Routing Information System)와 HOIDS(HoneyNet IDS) 상관관계 동작구조 [10] 같이 개선된 보안시스템 구성도와 같이 이루어진다. 각 하위 네트워크 진입단에 HOIDS 센서를 설치하고, 그 정보를 HOIDS에 저장 한다. 여기서 실시간 저장된 정보를 RIS와 상관관계를 통해 사이버 위협 정보를 조기에 탐지하게 되어 그 정보를 각 보안장비와 연동한다.

(그림 1)과 같이 HOIDS에서 비매칭 패턴에 대하여 내부 네트워크 정보를 상관관계 함으로써 정형화 및 사이버 위협에 대한 대응이 가능하다. 첫



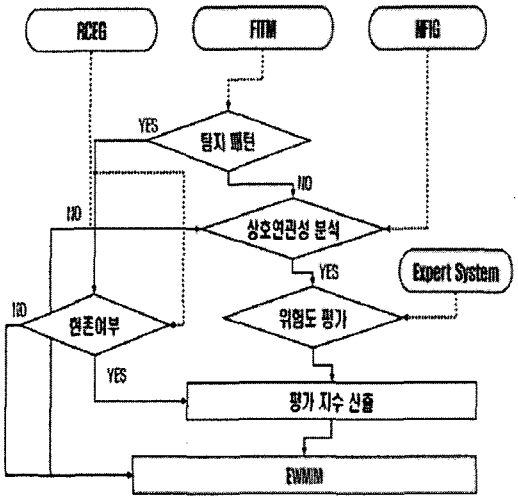
(그림 1) RIS와 HOIDS 상관관계 동작구조

번째로 이벤트가 평가되면 RIS 정보를 검색하여 트래픽 상황에 매칭되는 이벤트를 찾는다. 두번째 세부적으로 HOIDS에서 탐지된 정보 즉 특정 포트, 아이피 확산 패턴, 패킷 정보 등을 기존 보안 시스템과 비교하여 위험도를 평가하고, 여기서 검출된 정보를 RIS에서 상관관계분석을 통해 변종 이벤트에 대해 분석하여 세 번째 각 하위 네트워크에서 대응 구간을 평가하여 보안장비에 대응 명령을 내리게 된다. 네 번째 RIS에서 탐지되지 않은 정보는 정형화 데이터베이스로 보내어 진다.

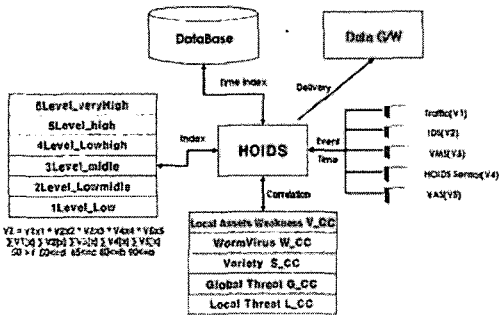
3.2 실시간 보안 이벤트 분석을 통한 정형화 기법

(그림 2)에서 RCEG(Real Critical Event Gateway)와 FITM(First Input Threat Module), NFIG (News Find Input Gateway)[11]의 상관관계를 통하여 보안 이벤트 평가지수를 산출하는 프로세스를 만든다. 또한 (그림 3)에서 내부 자산 취약 지수는 내부 네트워크에서 자체

취약성을 평가하여 V_cc외 각 가중치 값을 10단계로 결정한다. 상관관계에 의한 가중치 평가 방법은 각 보안 장비 및 네트워크 장비의 임계치를



(그림 2) 보안위협 평가지수 산출 프로세스



(그림 3) 이벤트 가중치 평가구성도[10]

〈표 1〉 가중치 평가표

Value	V_cc	W_cc	S_cc	G_cc	L_cc
1	-5%	-5%	-5%	-5%	-5%
2	0%	0%	0%	0%	0%
3	5%	5%	5%	5%	5%
4	10%	10%	10%	10%	10%
5	15%	15%	15%	15%	15%
6	20%	20%	20%	20%	20%
7	25%	25%	25%	25%	25%
8	30%	30%	30%	30%	30%
9	35%	35%	35%	35%	35%
10	40%	40%	40%	40%	40%

3개월간 시간별, 요일 별, 일 별, 평균값을 구하고, 실시간으로 대입하여 다음 <표 1>와 같이 각 가중치 평가 값을 구한다.

〈표 2〉 평가지수 산출법

ρ = 상관계수, λ = 표준화계수

$$FITM\_date = \Sigma FITM\_event\_n * EW\_cc\_n * \rho$$

$$NFIG\_date = \Sigma NFIG\_event\_n * EW\_cc\_n * \rho$$

$$RCEG\_date = \Sigma RCEG\_event\_n * EW\_cc\_n * \rho$$

$$EWMIN\_date = (FITM\_date * \lambda) + (RCEG\_date * \lambda) + (NFIG\_date * \lambda)$$

4. 성능분석

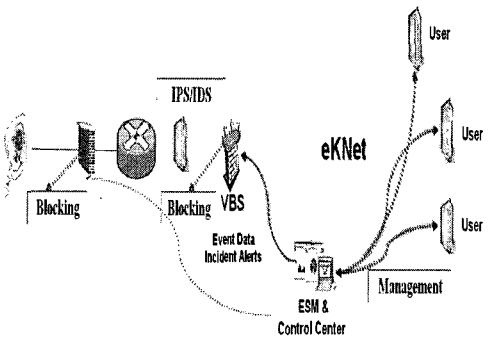
4.1 분석환경

성능분석을 위해 90일간 1G Byte속도 이상 사용하는 대형 네트워크에 보안장비를 적용하여 실험 한다. 공통된 분석환경을 위해 "K" 기관 네트워크상에서 실제 업무를 대상으로 검증을 실시했다. 인프라 구조가 개선된 보안구조가 구비된 것은 아니므로 본 검증 작업을 위해 측정 목적의 장비보강과 환경 준비 단계를 거쳤다. 인용된 "K" 기관 환경은 인트라넷 시스템 내 접속 자원 규모 각종 서버 500대, 클라이언트 Workstation급 PC 10,000대, 내부 사용자 규모는 20,000명이다.

네트워크 구조는 인트라넷과 외부 망과의 연결은 500Mbps 속도로 복수 회선 네트워크로 구성되어있으며, 인트라넷 입구에 침입차단시스템(IDS)이 구성되어 있고 침입차단시스템 이후 구간에는 인트라넷이 구성되어있고 인트라넷 내부 구조는 서버와 PC가 연결되어 있고 서버 전단에 별도의 메일 검색 시스템이 설치되었으며 PC자원을 대상으로 개별 단위 바이러스 백신이 설치되어있다.

트래픽 규모는 일간 약 5억 패킷이 처리되는 대

규모 볼륨(Volume)이고 상시 5만 정도의 네트워크 세션(Session)이 접속되고 있다. 마지막으로 보안장비는 Giga bit Firewall(기가비트방화벽) 4대(Backup라인 포함), IDS(Sun V880) 8대, Giga bit IPS 4대, VMS Server 2대, ESM(Sun ENT3500) 1대로 구성되어 있다.



(그림 4) 제안 네트워크 분석 모델 구조

(그림 4)과 같이 A네트워크에서는 ESM & Control Center에서 각 보안장비와 네트워크 장비의 이벤트를 정형화 분석하기 위하여 구성하였다.

90일간 VMS통계를 통한 검증 방법과 정형화를 통한 성능평가를 하였다. 첫 번째로 제안 네트워크에서 90일 간은 적용된 임계치를 통하여 통계를 산출 하였고, 그 이후에는 90일간 제안 네트워크에 정형화 기법으로 보안구조를 적용하여 검출 하였다. 이 실험을 통하여 실시간 사이버위협 조기경보 대응에 대한 기반 연구가 실시간 사이버 위협에 대해서 어느 정도 차단이나 방지 효과가 있는지 분석할 수 있다.

4.2 성능분석

<표 3>은 각 FITM, NFIG, RCEG에서 모아진 이벤트 정보를 수치화 되어 입력되고, 표준화 과정을 거쳐 정형화 된다 그리고 각각 정형화된 정보

〈표 3〉 각 보안장비 이벤트 표준화 값

	VAR00001	VAR00002	VAR00003	VAR00004	VAR00005	VAR00006
1	101.00	.00	-1.00	.24	33.58	-.46
2	102.00	-.45	-.65	.21	26.77	-1.14
3	103.00	.50	2.89	.25	32.40	3.27
4	104.00	-.31	2.73	.26	33.68	1.57
5	105.00	-.09	-.62	.24	28.08	-.38
6	106.00	.12	2.28	.25	24.31	2.08
7	107.00	-.70	2.57	.28	37.76	.68
8	108.00	.28	-.84	.25	29.48	.23
9	109.00	-.45	-.72	.23	29.63	-1.17
10	110.00	-.52	-.03	.30	44.81	-.75
11	111.00	.50	8.57	.29	48.81	7.29
12	112.00	-.08	4.64	.39	63.34	3.48
13	113.00	-.21	-1.00	.37	58.80	-.76
14	114.00	.80	-.60	.34	56.77	.08
15	115.00	3.67	.00	.31	46.23	7.64
16	116.00	2.42	1.00	.31	45.26	5.84
17	117.00	2.04	-.80	.33	43.77	3.84
18	118.00	1.68	-.20	.32	36.23	3.55
19	119.00	-1.00	.49	.30	31.44	-1.36
20	120.00	.33	2.20	.26	28.02	2.47
21	121.00	.61	2.07	.26	30.27	2.94
22	122.00	.00	.25	.22	31.27	.39
23	123.00	-.02	.05	.22	30.21	.22
24	124.00	.47	2.38	.25	29.50	2.84
25	125.00	-.33	.18	.26	30.81	-.28
26	126.00	.04	1.38	.27	28.91	1.30
27	127.00	.17	.05	.26	28.22	.62
28	128.00	.83	.67	.26	32.18	2.39
29	129.00	-.43	.14	.25	27.58	-.50
30	130.00	.27	-.64	.21	23.27	.30
31	131.00	.38	-.65	.29	38.45	.60
32	201.00	-.02	1.92	.29	36.98	1.60
33	202.00	.23	.56	.25	33.36	1.11
34	203.00	3.02	-.43	.34	47.67	6.07
35	204.00	2.47	-.68	.39	54.72	4.85
36	205.00	1.22	-.25	.43	68.08	2.69
37	206.00	-.38	.57	.41	65.47	.04
38	207.00	-.93	3.39	.40	60.74	.91
39	208.00	-.43	1.18	.25	46.66	.21
40	209.00	1.38	-.38	.25	41.85	2.75

는 가중치 요소를 가산하게 된다. 이때 가중치 요소중 가장 큰 가중치 요소로 증명 표준화 값의 누적 적용 하여 별도 변수로 지정 한다.

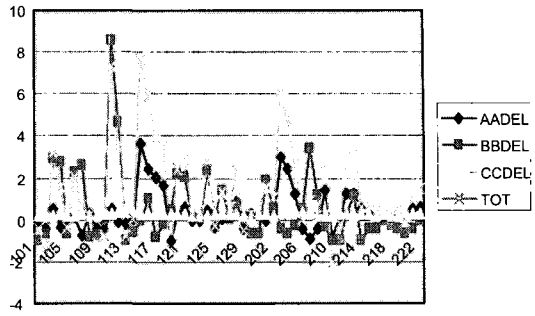
별도변수 = AAA4

보안이벤트_DATE = NFIG * CC1 + FITM * CC2 + RCEG * CC3 + AAA4 * CC4

표준화된 변수는 누적 변수로 각 보안장비의 데이터값은 100% 수치로 정형화후 임계치 수치 만큼 가감하였다.

	AADEL	BBDEL	CCDEL
101	0	-1	0.24
102	-0.45	-0.65	0.21
103	0.497	2.889	0.25
104	-0.31	2.734	0.26
105	-0.09	-0.62	0.24
106	0.117	2.2772	0.25
107	-0.7	2.5722	0.28
108	0.283	-0.835	0.25
109	-0.45	-0.721	0.23
110	-0.52	-0.03	0.30
111	0.5	8.5712	0.29
112	-0.08	4.6404	0.39
113	-0.21	-1	0.37
114	0.083	-0.6	0.34
~~	~~~	~~~	~~~
204	2.467	-0.675	0.39
205	1.217	-0.25	0.43
206	-0.38	0.5678	0.41
207	-0.93	3.3908	0.40
208	-0.43	1.1804	0.25
209	1.383	-0.38	0.25
210	-0.79	-1	0.23
211	0.133	-1	0.26
212	1.247	0.2	0.31
213	1.22	1.168	0.25
214	0.5	-1	0.28
215	0.33	-0.4	0.29
216	0.25	-0.42	0.25
217	0.1	-0.05	0.27
218	0.2	-0.235	0.24
219	0.32	-0.45	0.25
220	0.11	-0.622	0.23
221	0.55	-0.39	0.26
~~	~~~	~~~	~~~

(그림 5) 보안이벤트 통합 정형화 결과



(그림 6) 보안이벤트 통합 그래프

(그림 5), (그림 6)에서 결과 값을 그래프로 도출한 결과이다.

본 논문에서 제안한 방법은 사이버 위협 예 경보 시스템에 적용 시 적시성 있는 경보 발령이 가능하고[11]이에 따른 대응이 효율적으로 이루어질 수 있어 트래픽이 폭주하거나, 내부 네트워크의 위협요소를 차단 할 수 있었을 것이다. "K" 기관에서 각종 보안장비와 네트워크 장비의 각종 이벤트 및 수치를 임계치 설정 통해 구성하였고, 그에 따른 정형화기법이 악성 이벤트 차단에 실제적인 효과가 조기 경보 발령에 가능한 것을 검증하였다.

5. 결 론

최근에 나타나는 사이버 위협 공격은 변종 공격과 새로운 기법을 이용한 공격으로 보안관리자가 다양한 보안장비의 이벤트를 점검하여 실시간으로 대응한다는 어려움이 있었다. 상상을 초월하는 속도로 지능화 · 다양화 되고 있으며, 급속하게 확산되는 보안이벤트를 방치할 경우 사이버위협에 대한 대응의 근본이 흔들릴 수도 있다는 위기감을 인식하고, 이에 대한 대책 및 대응기술 확보에 주력해야 한다.

그러므로 본 연구에서 임계치에 의한 정형화 기법와 상관관계의 의한 기법을 제시하였고, 실제 네트워크에서 통합 보안 위협에 기반이 되는 정형화

결과를 검증하였다. 그러나 정형화방안을 효율적으로 사용하기 위해서는 체계적인 방안 마련이 필요하며, 따라서 향후 상존하는 보안 이벤트 요소에 대한 표준방안을 평가하고, 위험을 감소시키기 위한 방안과 임계치 및 상관관계 데이터를 분석할 수 있는 데이터웨어하우스의 설치 및 개발이 필요하다.

참 고 문 헌

[1] 백종욱, 남동수, 김귀남, "정량적 사이버위협 분석에 의한 전역적 위협 경보 모델", 한국사이버테러정보전학회 제4회 추계학술발표대회, 2006.

[2] 국가정보원, 국가사이버안전매뉴얼, 2005, 10.

[3] Glenn Gebhart, "Worm Propagation and Counter measures", SANS Institute, 2004.

[4] 남동수, 이도훈, 박응기, "역학 기반 웜 확산 피해 예측모델 연구", WISC05, 2005.

[5] Guofei Gu, Monirul Sharif, Xinzhou Qin, David Dagon, Wenke Lee and George Riley, "Worm Detection, Early Warning and Response Based on Local Victim Information", 20th Annual Computer Security Applications Conference, pp. 136-145, 2004.

[6] http://info.ahnlab.com/ahnlab/report_view.jsp?num = 416.

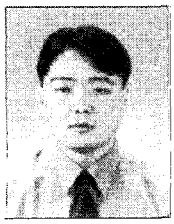
[7] J. L Hellerstein, F. Zhang, and P. Shahabuddin, "A Statistical Approach to Predictive detection", Computer Networks, vol. 1, No. 35, pp. 77-95, 2001.

[8] F. Zang and J. L Hellerstein, "An Approach to On-line Predictive Detection", In Proc. of 8th International Symposium on Modeling. AS CTS, 2000.

[9] Y. Shu, M. Yu, and J Liu, "Wireless Traffic modeling and Prediction Using Seasonal ARIMA Models", In Proc. of IEEE International Conference on Com., vol. 3, 2003, 5.

[10] Dong Hwi Lee, Kyong Ho Choi, Kuinam J. Kim, and Sang Min Park, "Routing Information System and HOIDS for Detection Method of Vicious Attack in Large Networks", Frontiers of High Performance Computing and Networking, LNCS, Vol. 4331, 2006, 12.

[11] Sang Ho Lee, Dong Hwi Lee, and Kuinam J. Kim, "A Conceptual Design of Knowledge-Based Real Time Cyber Threat Early Warning System", Frontiers of High Performance Computing and Networking, LNCS, Vol. 4331, 2006, 12.



이 동 휘

2000년 경기대학교 전자계산학과 (이학사)

2003년 경기대학교 정보보호기술공학과 (공학석사)

2004~현재 경기대학교 정보보호학과 (박사과정)

이 동 춘

연세대학교 컴퓨터과학과 (공학박사)

현재 호원대학교 국방과학기술대학 학장

관심분야: 이동/무선 통신, USN 및 보안

김 귀 남

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학교 통계학과(통계학석사)

미국 콜로라도주립대학교 기계산업공학과(기계/산업공학박사)

현재 경기대학교 정보보호학과 교수