

한국형 NCW를 위한 전술네트워크에서의 악의적인 노드 검출 모델★

양호경*, 차현종*, 신효영***, 유황빈**, 조용건*

요 약

NCW(네트워크 중심전)은 컴퓨터의 자료 처리 능력과 네트워크로 연결된 통신 기술의 능력을 NCW(네트워크 중심전)은 컴퓨터의 자료 처리 능력과 네트워크로 연결된 통신 기술의 능력을 활용하여 정보의 공유를 보장함으로서 효율성을 향상한다는 개념으로, 정보기술의 발전에 따라 무기체계 위주의 재래전에서 네트워크 기반의 네트워크 중심전으로 바뀌어 가고 있다. 이런 환경적인 변화에서 안전한 통신을 보장하기 위한 보안 알고리즘의 필요성이 중요시 되고 있다. 무선 Ad-hoc 네트워크에서의 악의적인 노드를 식별하는 방안들은 정상적인 노드들도 거짓으로 신고했을 때 확인절차 없이 경로를 재탐색하고 변경되어 최적의 전송환경을 활용하지 못하는 문제점을 가지고 있다.

본 논문에서는 NCW환경의 Ad-hoc에서 보안경로 탐색 프로토콜인 MP-SAR 프로토콜을 이용하여 경로에서 악의적인 노드를 검증하고, 유효한 최단 경로를 통해 데이터 전송을 하는 기법을 제안하고자 한다. 제안 기법을 사용하게 되면 노드에 대한 신고가 있을 경우 확인절차를 거쳐 불필요한 경로 재탐색을 막을 수 있게 된다.

Detection Model of Malicious Nodes of Tactical Network for Korean-NCW Enviroment

Ho-Kyung Yang*, Hyun-jong Cha*, Hyo-young Shin***, Hwang-bin Ryou**, Yong-gun Jo*

ABSTRACT

NCW(Network Centric- Warfare) encompasses the concept to use computer data processing and network linkage communications techniques, share information and furthermore, enhance the effectiveness of computer-operating systems. As IT(Information & Technology) have become developed in the recent years, the existing warfare system-centered conventional protocol is not use any longer.. Instead, network-based NCW is being widely-available, today. Under this changing computer environment, it becomes important to establish algorithm and build the stable communication systems. Tools to identify malign node factors through Wireless Ad-hoc network cause a tremendous error to analyze and use paths of even benign node factors misreported to prove false without testing or indentifying such factors to an adequate level. These things can become an obstacle in the process of creating the optimum network distribution environment.

In this regard, this thesis is designed to test and identify paths of benign node factors and then, present techniques to transmit data through the most significant open short path, with the tool of MP-SAR Protocol, security path search provider, in Ad-hoc NCW environment. Such techniques functions to identify and test unnecessary paths of node factors, and thus, such technique users can give an easy access to benign paths of node factors.

key word : MP-SAR 프로토콜, NCW

접수일(2011년 3월 7일), 수정일(1차: 2011년 3월 17일,
2차: 2011년 3월 22일), 게재확정일(2011년 3월 23일)

★ 2010년도 광운대학교 교내학술연구비 지원에 의해 연
구되었음.

* 광운대학교 방위사업학과

** 광운대학교 컴퓨터과학과

*** 경복대학 컴퓨터정보과

1. 서 론

최근 이동 컴퓨팅 단말기들이 보다 소형화되고, 다양한 무선 네트워크 제품과 서비스가 제공되고 있으며, 이동 컴퓨팅 기기의 휴대성과 사용자의 이동성에 대한 연구가 활발히 진행되고 있다. 이동 컴퓨팅 환경은 기존에 설치된 유선망을 기반으로 기지국이 관리하는 영역을 벗어난 지역에 존재하는 사용자들에 대해서는 서비스 지원이 불가능한 환경이다. 이에 반해 무선 ad-hoc 네트워크 환경은 기존에 설치된 유선망의 도움 없이 이동 호스트들만으로 구성 될 수 있는 임시적인 네트워크 환경이다. 이러한 네트워크의 발전과 더불어 정보기술의 발전에 따라 군에서 미래 전장 수행개념도 비접적, 비선형, 원거리 전투, 네트워크 중심 전쟁, 병렬, 동시·통합작전 그리고 효과 중심의 신속 기동전 형태로 변화하고 있다. 전쟁의 양상도 무기체계 위주의 재래식 전쟁에서 시스템 간의 서로 연결되어 있는 네트워크 중심전(NCW : Network Centric Warfare)의 개념으로 변하고 있다. 이러한 혁신적인 발전과 더불어 군의 전쟁수행 환경도 빠르고 다양하게 변화하고 있다. 군에서는 임무의 특수성으로 인해 독자적인 전용 지휘통신망을 발전시키고 있었다. 새로운 정보기술의 발전은 21세기 변화된 형태의 전쟁을 수행하기 위해 군 정보통신분야의 적용이 필수적이며 이를 통해 전술적인 감시나 추적 또한 전장정보의 실시간 수집 등의 효과를 공유하여 조직화됨으로써 전투력 발휘효과를 극대화 시켜 효율적인 전쟁을 치르기 위해서 노력하고 있다. 군에서는 임무의 특수성으로 인해 독자적인 전용 지휘통신망을 발전시키고 있었고, 새로운 정보기술의 발전은 21세기 변화된 형태의 전쟁을 수행하기 위해 군 정보통신분야의 적용이 필수적이며 이를 통해 전술적인 감시나 추적 또한 전장정보의 실시간 수집 등의 효과를 공유하여 조직화됨으로써 전투력 발휘효과를 극대화 시켜 효율적인 전쟁을 치르기 위해서 노력하고 있다.

그러나 이러한 네트워크 발전과 더불어 보안적인 위협도 늘어나고 있는 실정이다. 네트워크가 확장됨

에 따라 공격할 수 있는 경로도 증가하게 되고 이동하는 데이터의 양도 증가함에 따라 유출되면 위험한 데이터의 양도 증가하게 된다. 단순한 데이터 유출을 위한 침입이 아닌 사이버전 양상의 네트워크상의 전쟁이 일어날 가능성도 날로 증가하고 있는 실정이다. 특히 군과 같은 정보와 데이터가 중요한 집단에서는 사소한 정보 유출도 큰 위험으로 나타날 수 있기 때문에 다른 네트워크에서 보다 보안적인 요인을 중요시해야 한다. 무선 ad-hoc에서의 보안 알고리즘 설계 할 때의 특성을 볼 때, 무선 ad-hoc에서의 보안대책은 크게 사전 예방방법과 사후 조치방법으로 나뉘어서 생각을 할 수 있다. 사전 예방 방법으로는 ad-hoc 네트워크의 라우팅 경로를 설정 할 때 악의적인 노드를 제외시켜 라우팅 경로를 구성하고, 사후 조치 방법으로는 데이터의 전송이 끝난 후에 악의적인 노드를 찾아내어 조치를 하는 방식이다[5]. 본 논문에서는 보안성이 추가된 다중경로 라우팅을 이용한 사전 예방방법에 대해서 제안하고자 한다. 본 논문의 구성은 1장은 서론, 2장은 관련연구, 3장에서는 제안하는 악의적인 노드에 대한 검출 방안을 제시하고 마지막으로 4장에서 결론을 맺는다.

2. 관련 연구

2.1 군 작전환경

2.1.1 네트워크 중심전(NCW)

정보화시대에 들어서면서 미국은 군사혁신을 통하여 정보기술을 비롯한 현 시대의 기술적 성과를 군사부문에 반영하고자 노력하였는데, 그 산물 중의 하나가 네트워크 중심전이다. 현대의 발전된 컴퓨터 기술 및 네트워크가 군대에 도입되어 지휘통제통신체계의 혁신이 일어날 수 있었고, 이를 통하여 모든 부대와 각 개인들을 네트워크로 연결한다는 개념이 가능하게 되었기 때문이다. 무기체계적인 면에서도 정밀타격능력의 발전으로 인하여 이제는 표적의 위치나 형태를 식별하기만 하면 즉각적인 제압이 가능하고, 부대의 기동성이 증대되어 물리적 공간과 시간의 제한사항이 축소되고 있다. 따라서 네트워크 중심전은 이러한 현

대 군대의 발전성과를 통합할 수 있는 하나의 개념으로서 제시되었다[1][2].

2.1.2 전술정보통신체계(TICN)

TICN(Tactical Information and Communication Network)은 네트워크 중심전에서 정보의 원활한 소통을 위해 센서체계, 지휘통제체계, 타격체계에게 고속 대용량의 정보통신로를 제공하는 것을 목적으로 하는 체계이다. TICN의 부체계로서는 기간망 전송체계, 기간망 교환접속체계, 망 제어체계, 전투무선망체계, 전술이동통신체계로 구분된다. 이중 전술이동통신체계는 지휘소 및 주변지역, 원격지원의 전술용 다기능 단말기 가입자에게 음성, 데이터 및 멀티미디어 서비스를 통해 이동통신 수단을 지원해주는 것을 목표로 한다[3].

2.2 Ad-hoc 네트워크

노드(node)들에 의해 자율적으로 구성되는 기반 구조가 없는 네트워크로 네트워크의 구성 및 유지를 위해 기지국이나 액세스 포인트와 같은 기반 네트워크 장치를 필요로 하지 않는다. 애드혹(Ad-hoc) 노드들은 무선 인터페이스를 사용하여 서로 통신하고, 멀티 허브 라우팅 기능에 의해 무선 인터페이스가 가지는 통신 거리상의 제약을 극복하며, 노드들의 이동이 자유롭기 때문에 네트워크 토폴로지가 동적으로 변화되는 특징이 있다. Ad-hoc 네트워크에 제안 된 라우팅 프로토콜은 이발전인 테이블 구동(table driven) 방식과 요구 기반 구동(on demand driven) 방식으로 나눌 수 있다[4][5].

2.3 MP_SAR 프로토콜

MP-SAR 프로토콜은 AOMDV 기반에서 동작하므로 AODV 기반의 SAR 프로토콜의 원활한 보안 링크 연결의 한계점을 개선한 라우팅 프로토콜이다. SAR 프로토콜이 AODV 프로토콜을 기반으로 보안 노드만을 발견하고 단일 보안경로 채널을 설정하는데 비해, MP_SAR 프로토콜은 보안노드를 발견할 뿐만 아니라 일반노드를 경유하는 다중경로를 발견한다. 데이터 전송을 위해서 다중일반경로 중에서 최단경로를 결정하고 선택된 일반경로는 출발지 노드와 목적

지 노드간의 임시적인 보안채널을 설정하도록 데이터 암호 키 교환을 한다. 최단경로의 링크가 손실될 경우, 출발지 노드는 찾았던 경로 중 최단 경로를 결정하여 데이터를 전송하지만 첫 번째처럼 키 교환을 하지 않는다. 때문에 비 중첩된 최단경로를 통한 빠르고 안전한 데이터 전송을 할 수 있게 된다.

2.3.1 경로 발견 및 유지

(1) 출발지 노드는 목적지 노드로의 경로를 필요로 할 때 출발지 노드의 정보와 요구 보안레벨정보(보안경로 발견을 위해 필요로 하는 보안레벨)를 포함한 RREQ를 생성하고, 출발지 노드나 중간노드에서 RREQ를 전송할 때 요구 보안레벨과 출발지 라우팅 주소 정보로서 IP주소를 RREQ에 추가한다.

(2) 중복으로 도착한 RREQ는 버리지 않고 수신하는 즉시 자신의 라우팅 테이블에서 라우팅 경로를 확인하여 역경로를 설정한다. 보안레벨과 중간노드 자신의 보안레벨을 비교하여 레벨이 높거나 같다면 RREQ는 암호화된 필드를 복호화한 후 소스 라우팅 리스트에 자신의 정보를 추가한다. 레벨이 낮은 경우 중간 노드는 RREQ는 암호화 되지 않는 필드에 소스 라우팅 정보를 추가하고 이후 노드들로 브로드 캐스트한다.

(3) 목적지 노드는 처음 RREQ를 수신한 후 암호화된 RREQ의 필드를 확인한다. 이 필드의 소스 라우팅 리스트를 검사해 연속적으로 보안노드들로만 거쳐진 RREQ라면 보안 RREQ로 결정한다. 목적지 노드는 일정시간 안에 수신된 RREQ를 확인해 다중경로들 중 최단 경로를 결정한다. 자신의 수신 순서번호가 RREQ에 포함되어 있는 수신 순서 번호보다 크거나 같으면 중간 노드에서와 같은 방법으로 역 경로를 형성한다.

(4) 목적지 노드는 처음 수신한 경로를 데이터 전송을 위한 주경로로 선택한 후에 주경로와 비교해 최대의 노드 비중첩성을 갖는 대체경로를 찾는다.

(5) 주경로 및 대체경로에 대하여 수신 노드는 송신 노드를 향하여 각각의 RREP를 전송한다. 메시지의 응답으로 목적지 노드에서 결정된 경로정보를 포함한 RREP 메시지를 출발지 노드로 보내고 RREP를 수신하는 중간노드는 목적지 노드에 대한 보안경로와

다중경로 라우팅 정보를 알게 된다[6].

2.4 공격기법

2.4.1 라우팅(경로설정)에 대한 공격

라우팅에 대한 공격은 라우팅 알고리즘대로 라우팅 정보를 전달하지 않는 모든 행위를 말한다. 예를 들어, DSR에서는 공격자가 전송 패킷 내에 기록되는 source route의 목록에 대해 노드의 목록을 추가, 삭제하는 등의 행위를 통해 source route의 변경이 가능할 것이며 AODV에서는 흡수 일련번호가 중요한 라우팅 정보이므로 공격자가 잘못된 흡수, 일련번호를 전달하는 형태의 공격이 가능하다. 이러한 라우팅 공격은 공격자가 의도하는 특정 목적지로 전달되도록 유도할 수 있고 실제 존재하지 않는 경로가 설정되어 결국 라우팅 루프 및 네트워크 혼잡, 분리까지 유발할 수 있다.

2.4.2 패킷 전달에 대한 공격

패킷 전달에 대한 공격이란 경로 설정과정에서는 정상적으로 동작하지만 실제 데이터 패킷은 제대로 전달하지 않는 행위를 말한다. 이러한 공격은 자신의 자원을 아끼기 위해 다른 노드의 데이터는 전달하지 않으면서 자신의 데이터만 보내려고 하는 이기적인 노드와 의도적으로 네트워크 성능을 저하시키기 위한 악의적인 노드에 의해 일어날 수 있다. 본 논문에서는 이를 구분하지 않고 악의적인 노드라고 부르기로 한다.

패킷 전달에 대한 공격의 형태로는 전달해야 할 패킷을 버리거나 그 내용을 임의로 변경시킬 수도 있으며 많은 양의 모의미한 패킷을 네트워크에 주입시켜 무선 채널 접속을 위한 경쟁을 높이거나 혼잡을 일으킬 수 있다. 이러한 모든 형태의 공격으로부터 네트워크를 보호하기 위한 방법으로 Watchdog and Pathrater, 이기적인 노드 관리 방안 등이 있다[7][8].

3. 제안기법

관련연구에서 제시한 방식들은 악의적인 노드가

경로 상에 포함되어 있으면서 정상적으로 동작하는 노드를 거짓으로 소스 노드에게 신고하는 경우 이를 식별해 낼 수 없는 문제점이 있다. 이런 문제점을 보완하고자 악의적인 노드에 대한 신고를 검증하는 단계를 두어 거짓 신고를 걸러내는 방법을 제안하고자 한다.

3.1 가정사항

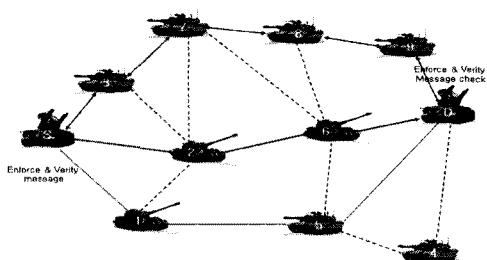
제안된 기법을 위한 기본 가정 사항은 다음과 같다.

- (a) 각 노드는 이웃 노드의 전송을 overhear 할 수 있다.
- (b) 각 노드는 자신만이 알고 있는 개인키를 가지고 있으며, 그에 대응하는 공개키는 모든 노드가 가지고 있다.
- (c) 악의적인 노드를 신고할 때의 신고자가 보내는 데이터를 신고서라고 하고, 이는 자신의 ID, 신고대상 노드의 ID를 포함한다. 임의의 노드에서 악의적인 노드를 신고할 때 신고서를 암호화해서 broadcast한다. 이를 받은 노드들은 송신 노드의 공개키로 복호화를 하여 신고서를 볼 수 있다. 또한 이 신고서는 개인키로 암호화를 하기 때문에 다른 노드에서 거짓으로 신고서를 만들 수가 없다.
- (d) 각 노드는 보안레벨을 가지고 있다.
- (e) 네트워크의 구성은 AOMDV를 기반으로 하는 MP-SAR 프로토콜을 사용한다.
- (f) 노드 간의 링크들은 양방향 통신이 가능하다.

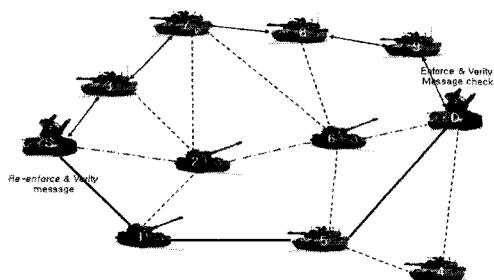
3.2 제안 알고리즘

제안 방식의 기본적인 동작은 다음과 같다.

AOMDV를 기반으로 MP-SAR 프로토콜에 의해 (그림1, 2)와 같이 보안경로 SSP(Security Shortest Path)와 일반 다중경로 중 최단 경로로 [S,2,6,D] 경로가 선택되었지만 데이터 전송을 위한 초기단계에서 검증 메시지를 전송하는 중 선택된 경로에서 온 메시지의 오류가 발견되었다. 따라서 다음 NSP인

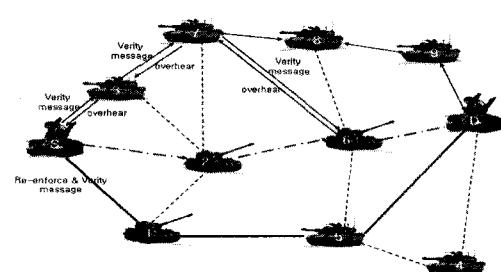


(그림 1) MP-SAR 경로설정



(그림 2)MP-SAR 경로 설정 단계
[S,1,5,D] 경로가 검증이 완료되어 데이터 전송 경로
를 강화하여 데이터 전송이 이루어진 상태이다.

강화된 전송경로로 데이터가 전송하면서 동시에
오류를 발견된 [S,2,6,d] 경로에 대해서 오류가 있거나
악의적인 노드를 검출하기 위해서 오류가 발생한
경로로 검증 메시지를 보낸다. 보내진 메시지는
Watchdog and Pathrater 기법을 이용한다.



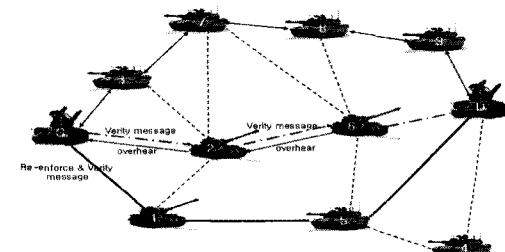
(그림 3) 보안경로는 이용한 악의적인 노드 검증

(그림 3)와 같이 검증 메시지를 다음 노드에 보내기 전에 버퍼에 메시지를 저장하고, 다음 노드에게 메시지를 보낸다. 다음 노드가 메시지를 다음 노드에

게 올바른 메시지를 보내는지 overher를 해서 원래의 메시지와 같다면 버퍼에 저장된 내용을 삭제한다. 만약 다르다면 다음 노드가 고의로 데이터를 변경시켜 보내는 것으로 판단한다. 또한 일정시간 내에 데이터를 변경시켜 보내는 것으로 판단한다. 또한 일정시간 내에 데이터를 보내는 것을 감지하지 못한다면, 고의로 데이터를 버리는 것으로 판단한다. 이러한 고의로 데이터를 변경 또는 버리는 노드를 악의적인 노드로 주위 노드에 broadcast하고, 소스노드에 알린다. 이러한 악의적인 노드의 신고는 각 노드의 개인키로 신고자와 행위자의 정보가 포함된 신고테이블을 암호화해서 신고를 하게된다.

Watchdog and Pathrater로 악의적인 노드를 발견했다고 해도 신고자가 고의로 정상적인 노드를 악의적인 노드라고 신고하는 경우가 있다. 이러한 경우를 대비해서 신고에 대한 신뢰성을 검증하기 위해 (그림 4)과 같이 MP-SAR로 확보된 보안경로(SSP)를 이용해서 이전과 같은 악의적인 노드를 검출하는 과정을 거친다. 만약 보안경로(SSP)를 이용한 검증에서 신고된 노드가 악의적인 노드가 아니라는 것으로 판단된다면, 신고를 한 노드를 고의적으로 정상적인 노드를 악의적인 노드라고 신고한 것으로 간주한다.

이렇게 판명된 악의적인 노드의 정보(ID)는 링크 내의 모든 노드가 저장하고 있다가 후에 소스노드가 바뀌고 라우팅 계산을 할 때 악의적인 노드가 거치는 경로를 제외하고 라우팅을 계산한다.



(그림 4) Watchdog을 이용한 악의적인 노드 검출

4. 결 론

본 논문에서는 다중경로에서의 보안경로는 확도하고 그 일반경로 중에서 최단 경로를 확인하여 데이터를 전송하는 MP-SAR 라우팅 프로토콜을 이용하였다. MP-SAR 프로토콜을 기반으로 일반경로와 보안경로를 이용하여 데이터를 전송하고 악의적인 노드가 있다는 신고가 들어오면 보안경로를 통한 검증으로 악의적인 노드 검출에 대한 신뢰도를 높였다. 또한 네트워크를 사용하는 측면에서 네트워크의 파괴로 인한 재탐색과 불필요한 작업을 하지 않기 때문에 기존 방법보다 자원을 절약할 수 있다. 제안하는 방법에서는 악의적인 노드에 대한 신뢰성을 높였으나, 검출된 악의적인 노드에 대한 주기적인 관리 및 조치가 없어서 경로가 바뀌었을 때 악의적인 노드가 네트워크에 다시 참여 할 수 있다는 취약성을 가지고 있다. 향후 연구에서는 검출된 악의적인 노드를 관리하여 다른 경로의 네트워크에 참여시키지 않도록 하는 연구가 이루어져야 할 것이다.

참고문헌

- [1] T. Murata and H. Ishibuchi, "Performance evaluation of genetic algorithms for flows hop scheduling problems," Proc. 1st IEEE Conf. Evolutionary Computation, vol. 2, p. 812-817, June 1994
- [2] 배달형, 조용건, "NCW 컴퓨터네트워크작전(CNO)의 작전적 원리와 한국군의 발전방향", 국방연구, 2009. 08
- [3] 고석주, "소부대 지휘자 통신체계 구현방안 연구", 배재대학교 정보통신대학원, 2005.12
- [4] Andrew S. Tanenbaum, "Computer Network," Prentice-Hall International Inc., Second Edition, pp.345-374, 1996.
- [5] C.E Perkins and P.Bhagwat, "Routing over Multi-hop Wireless Network of Mobile Computers, " SIGCOMM'94 : Computer Communications Review, pp.234-244, Oct, 1994.
- [6] In Sung Han, Hwang-Bin Ryou, Seok-Joo ng Kang, "Multi-Path Security-Aware Rou ting Protocol Mechanism for Ad Hoc Netw ork," ichit, pp.620-626, 2006 International C onference on Hybrid Information Technolog y-Vol 1(ICHIT'06), 2006
- [7] S. Marti et al., "Mitigating Routing Misbe havior in Mobile Ad Hoc Networks", ACM MOBICOM, 2000.
- [8] gajin Na et al, "Secure Mechanism to ma nage selfish nodes in Ad hoc Network", J IIC. 2004.

[저자 소개]



양호경 (Ho-Kyung Yang)
 2005년 광운대학교 컴퓨터
 소프트웨어학과(공학사)
 2007년 광운대학교 컴퓨터
 과학과(공학석사)
 2010년 광운대학교 방위
 사업학과(공학석사)
 2010년 광운대학교
 방위사업학과 박사과정
 email : porori2000@nate.com



유황빈 (Hwang-bin Ryou)
 1968년 인하대학교
 전자공학과(학사)
 1975년 연세대학교
 전자공학과(공학석사)
 1984년 경희대학교
 전자공학과(공학박사)
 1981년 ~ 현재 광운대학교
 컴퓨터소프트웨어학과 교수
 email : ryou@kw.ac.kr



차현종 (Hyun-jong Cha)
 2005년 광운대학교 컴퓨터소프트웨어학과(공학사)
 2008년 광운대학교 컴퓨터
 과학과(공학석사)
 2011년 광운대학교 방위
 사업학과(공학석사)
 2011년 광운대학교
 방위사업학과 박사과정
 email : chj826@kw.ac.kr



조용건 (Yong-gun Jo)
 1982년 육군사관학교
 전자공학과(이학사)
 1988년 국방대학원
 전산학과(공학석사)
 1998년 KAIST 전산학과
 (공학박사)
 2007년 ~ 현재 광운대학교
 방위사업학과 교수
 email : naikokr@kw.ac.kr



신효영 (Hyo-young Shin)
 1986년 광운대학교
 전자계산학과(이학사)
 1988년 광운대학교
 전자계산학과(이학석사)
 1998년 광운대학교
 전자계산학과(이학박사)
 1988년~1993년 (주)LG소프트
 연구원
 1994년~현재 경복대학 컴퓨터정보과
 부교수
 email : hyshin@kyungbok.ac.kr