전광통신망의 보안

한림대학교 최홍식 · 김 진* · 윤재우

전광통신망은 근원지에서 목적지까지 정보가 광 영역에 남아있는, 즉 근원지에서 빛의 형태로 보내진 정보가 광-전자 혹은 전자-광의 변화 없이 목적지까지 빛의 형태로 전달되는 통신망을 뜻한다[3]. 이는 매우 높은 자료 전송률과 매우 낮은 에러율을 가지고 있을 뿐 아니라 낮은 에러 비율은 부가적으로 통신 프로토콜의 하위 계층을 없앨 수 있는 장점이 있다. 이로 인해 광 통신망은 현재 부분적으로 이용되고 있지만 가까운 미래에는 기반 통신망의 근간이 될 것으로 기대된다. 국가의 군사 경제적 경쟁력이 통신망에 대한 의존도가 높아지고 있음으로 이러한 통신망의 보안이 점차 중요해지고 있다. 그러나 전광 통신망에서의 보안은 새로운 물리적 기전 때문에 통상의 통신망에서 다루어진 보안과는 다른 특성들을 포함한다. 물론 기존의 통신망에서 나타나던 보안 문제와 중복되는 문제도 많이 있지만 여기서는 전광통신망에서 특별히 다루어져야 할 보안 문제에 대해서만 언급하겠다. 따라서 전광통신망의 보안 중 특별히 정보의 물리적인 보안에 대해 언급할텐데 이는 종래의 통신망과 구별되는 보안의 문제들이 기본적으로 전광통신망의 물리적인 특성에 관계되어 있기 때문이다. 이러한 물리적인 보안은 크게 두 가지 면에서 살펴볼 수 있는데[1] 이는 개개 정보 보호와 전체 시스템의 QoS로 구분할 수 있다. 물리적인 정보보안은 최소한의 프라이버시와 QoS를 보장하는 것으로 이것들이 침해받거나 불가능해질 때 사용자에게 적절한 경고를 줄 수 있어야 한다. 이러한 경우를 야기하는 공격에는 태핑(tapping) 공격과 서비스 단절 공격이 있는데 서비스 단절은 통신을 불가능하게 하거나 QoS를 나쁘게 하는 공격을 의미하고 태핑 공격은 부적절한 접근을 통해 프라이버시를 손상시키는 것으로 이를 통해 타인의 비밀을 엿듣거나 통화량 분석 등을 할 수 있다. 중요한 것은 서비스 단절 공격이나 태핑 공격을 막을 뿐 아니라 공격이 무위로 끝나더라도 공격이 일어났다는 사실을 인지하는 것이다. 그래야만 적당한 대응이 이루어 질 수 있을 것이기 때문이다. 따라서 전광통신망에서 다루어져야 할 보안 문제는 크게 공격을 막는 것(prevention of attacks)과 공격을 감지하는 것(detection) 그리고 공격이 일어난 곳을 찾아내는 것(localization), 공격에 대한 대응(reaction)으로 나눌 수 있겠다. 공격의 진원지를 밝히는 것이 전광통신망과 같은 초고속의 통신망에서 특별한 의미를 갖는 것은 진원지에 대한 파악 없이 이루어지는 대응은 공격 자체보다 더 큰 문제를 일으킬 수 있기 때문이다. 따라서 일단 공격의 진원지가 밝혀진 후, 적절한 대응책이 실행되어야 한다.

1. AON의 특성

AON은 TDM CDM 혹은 WDM 등을 사용할 수 잇는데 WDM 이 가장 낙관적인 방법이라 하겠다 이는 WDM 기술이 다른 기술보다 진보해 있을 뿐 아니라 광섬유가 제공하는 영역을 모두 사용할 수 있는 유리한 기술이라는 점에서 그렇다. 동축케이블의 수천 배에 해당하는 광역 폭 전체를 사용할 수 있는 전자적인 장치가 없는 현

* 정회원

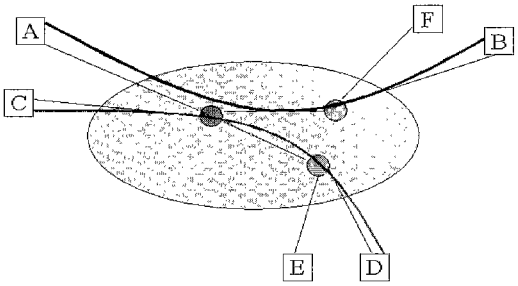

그림 1 Wavelength Routing Network w/o switch

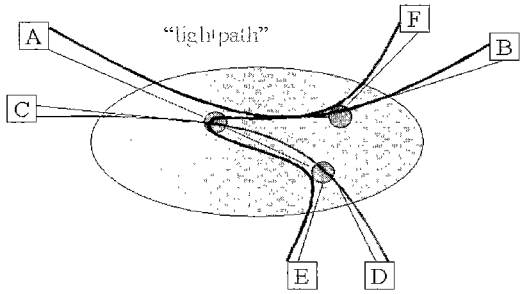

그림 2 Wavelength Routing Network

실에서 다른 방식은 약 100Gbps 정도의 속도를 보이고 있지만 WDM은 채널 당 10Gbps로 수 개에서 수백 개의 채널을 만들어 사용하고 있어 전체 가역 폭을 사용할 수 있는 가장 현실적인 방법이라 하겠다. WDM은 전체 가용 대역폭을 파장대로 나누어 여러 개의 채널을 만들어서 이 채널들을 병렬로 사용하여 광통신이 제공 할 수 있는 대역폭을 가장 많이 사용할 수 잇는 방법이다. 성형 커플러를 이용한 근거리 통신망에서 WDM을 이용하는 전광통신망에 대한 많은 연구와 시제품이 있고[3,4] 원거리 통신망에서의 광통신 망은 파장 라우팅 방식을 채택하여 효율적인 파장 활용을 위한 연구가 이루어지고 있다. 특히 파장 변환 능력이 있는 노드를 채택하면 이 효율을 더욱 높일 수 있다. 그림 1은 A-B(red), C-D(blue)의 파장으로 통신이 이루어질 때 새로운 통화 요구인 E-F는 파장 변환능력이 없는 노드로 이루어진 통신망이라면 새로운 파장을 이용해야만 하거나 여분의 파장이 없을 때는 통신이 불가능해진다. 반면 그림 2에서와 같이 노드가 파장 변환 능력이 있다면 부분적으로는 blue를 다른 부분은 red를 이용하여 E-F의 요구가 충족되어짐으로 해서 파장 재활용이 가능해진다. 현재는 광 장치와 전자적인 장치 혹은 광-전자, 전자-광 장치 등을 이용하여 이루어진 광-전자 통신망이 실용화되고 있지만 가까운 장래에는 모든 구성요소가 광 장치로 이루어진 전광통신망으로 통신망이 대체될 것으로 기대된다. 이러한 전광통신망은 다양한 구조로 구현될 수 있고 그 서비스의 종류도 다양하다. 그러나 이러한 구현들에 공통적으로 중요하게 생각되는 요소들에는 광섬유(optical fiber) 광 증폭기(optical amplifier), 파장 전환 노드(Switching node) 등이 있다. 따라서 여기서는 특별한 구조나 구현에 관계없이 공통적으로 갖고 있는 물리적인 특성에 관계된 문제만을 다룬다. 우선 보안의 측면에서 통상의 전자적인 통신망이나 전자-광 통신망으로부터 전광통신망을 구별하는 특징들은 크게 두 가지를 들 수 있는데 하나는 매우 높은 자료율(high data rate)이고 다른 하나는 투명도(transparency)라 할 수 있겠다. 우선 매우 높은 자료율은 보안의 측면에서 세 가지정도로 그 중요성을 생각할 수 있다. 첫째는 아주 짧은 순간에 이루어지는 간헐적인 공격으로도 많은 양의 자료를 쓸모 없이 만들 수 있다는 점이고, 둘째는 낮은 통신속도에 운용되는 지금까지의 통신망에 적당하게 개발된 전통적인 프로토콜이 높은 자료율을 갖는 통신망에서는 서비스 거부공격에 효과적으로 사용될 수 있다는 것을 뜻한다. 셋째는 전광통신망이 광역 통신망으로 사용될 때 그 지역적인 넓은 분포와 고속의 자료 율로 인해 높은 잠재(latency)를 갖는다는 것이다. 즉 많은 비트의 정보가 빛의 형태로 통신망상에 통과하는 중이 되고 이는 설사 공격이 감지되고 적절한 대응이 이루어졌다해도 본래대로 고칠 수 있는 한계를 넘어설 수 있다는 것이다. 투명성이란 광 노드가 투명하다는 뜻이다. 즉 광 노드에서 자료가 전자적인 형태로 변환 없이 빛의 형태 그대로 유지된다는 것을 뜻한다. 이는 서로 이질적인 신호 시스템이 한 노드에 공존할 수 있고 전자적인 속도에 의한 병목현상을 없앨 수 있다는 큰 장점이 있지만 본질적으로 서비스 거부에 대해 취약한 점을 갖고 있다. 이는 광 노드에서 신호를 재생산하지 않고 증폭하기만 하는 데에서 기인한다.

악의적인 신호를 이러한 투명한 노드에 보내면 통신망의 일부분 혹은 전체를 사용할 수 없게 할 수도 있다. 이는 노드에서 자료 스트림을 재구성할 수 없기 때문이며 이는 링크의 고장을 부분 부분 테스트하는 것을 복잡하게 할 뿐 아니라 공격의 감지를 어렵게 한다. 결국 자료를 재구성, 재생산하는 기존의 통신망에서는 생기지 않을 문제가 생기는 것이다. 왜냐하면 재생산을 하는 노드에서의 출력은 특정한 신호 방식과 프로토콜을 준수하기 때문에 잘못된 신호가 수정되거나 잘못의 확산을 국한시키기 때문이다. 그러나 투명한 통신망에서는 이렇게 자료를 재생산할 수 있는 능력이 없다 즉 각 노드가 개개 신호의 코딩 방법이나 모듈레이션 방법을 이해할 수 없기 때문이다[5].

2. AON의 취약성

광 통신망의 물리적인 문제점은 광 통신망을 이루는 광 장치들이 전자적인 장치에 비해 그 발전의 정도가 아직 완숙하지 못하다는데 있다. 파장 분할 방식의 각 채널들 간의 높은 혼선은 태핑이나 서비스 단절공격에 쉽게 이용될 수 있고 광섬유나 광 장치들이 보여주는 비 선형 성이나 광 증폭기의 획득 경쟁(gain competition) 또한 이러한 공격에 이용될 수 있을 만큼 취약하다. 장치의 문제 외에도 광 통신망은 통상 여러 가지 트래픽이 섞여 있는걸 가정하기 때문에 통일된 보호 방법의 저용이 어렵다. 또한 지역적으로 넓게 퍼져 있음으로 통신 선로에 대한 물리적이 접근도 무시할 수 없을 뿐 아니라 중요한 정보가 신뢰 할 수 없는 집단의 통화와 같이 link를 공유해야 하기 때문에 더욱 보안의 문제가 생긴다. 가장 좋은 것은 신뢰할 수 잇는 집단만이 이용하는 분리된 선로 혹은 독립된 통신망을 이용하는 것이 가장 좋겠지만 이는 여러 가지 이유로 현실적이지 못하다. 예를 들자면 호수나 산들의 이유로 링크를 개설하지 못할 경우, 링크에 오류가 생겨서 다른 링크들을 사용해야만 하는 경우, 보안 수준의 변화에 따른 논리적인 위상의 변화에 대처해야 할 경우, 동적인 트래픽을 수용하고자 논리적인 위상을 변화 시켜야 하는 경우 등의 이유 때문에 항상 독립된 통신망을 구성하기가 어렵다는 것이다.

3. 공 격

전술한데로 서비스 단절 공격과 태핑 공격으로 나눌 수 있는데 서비스 붕괴에 대한 공격은 광섬유, 광 증폭기, 전환 노드에 모두 이루어 질 수 있다. 광섬유에는 물리적인 접근을 통한 것 즉 광섬유를 자르는 경우와 이보다는 덜 직접적인 방법으로 광섬유를 휘어서 신호를 집어넣는(in band jamming) 경우를 생각 할 수 있겠다, 이는 광섬유의 비 선형성과 더불어 가능한 공격점이 될 것으로 생각된다. 광 증폭기에 대한 공격으로는 광 증폭기의 특성상 고 에너지 수준의 광입자를 공유함으로서 획득 경쟁이 일어나게 된다. 이는 광섬유에서의 에너지 손실이 매우 작은 것을 감안하면 멀리 떨어진 곳에서도 소량의 힘을 이용해서 쉽게 서비스 붕괴공격을 성공시킬 수 있게 한다. 그림 3의 예는 블루 신호가 다른 신호에 비해 아주 적은 량의 이득이 있는 상태로 보내졌을 때 몇 개의 증폭기를 거치면서 획득 경쟁의 결과가 누적되어 전체 에너지를 차지해 다른 신호가 존재하지 못하게 하는 경우를 보여주고 있다. 전환 노드에서의 서비스 붕괴 공격은 그림 4에서와 같이 노드의 양끝 단에 위치하게 되는 먹스나 디먹스의 혼선(crosstalk)이 가능한 공격점이 되는데 문제의 심각성은 이러한 혼선 역시 누적된다는데 있다[2].

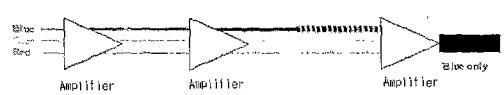

그림 3 Gain Competition (Lincoln Lab)

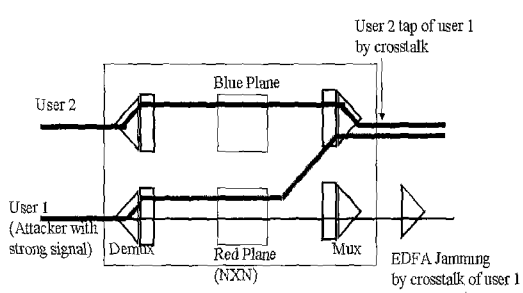

그림 4 Crosstalk at WSS

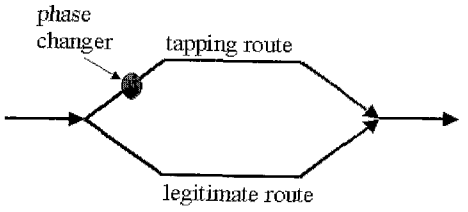

그림 5 Example of Correlated Jamming

태핑 공격 역시 광섬유, 증폭기, 전환노드에서 이루어 질 수 있는데 Fiber나 EDFA에서 공격은 광섬유를 휘어서 방출되는 정보를 얻거나 EDFA에서는 혼선을 이용하여 태핑을 할 수 있다. 이때 태핑과 재밍이 결합하는 상호 협조 재밍의 경우 매우 낮은 신호 대 잡음비를 이용해서 서비스 붕괴에 큰 효과를 볼 수 있다. 예를 들자면 그림 5에서와 같이 자기 밴드에 대한 자기 신호 재밍은 상호간의 다중 경로 문제 등을 야기해서 신호의 해석을 어렵게 할 수 있다. 전환 노드에서도 비슷한 경우를 볼 수 잇는데 이는 뒤에서 자세히 설명하겠다. 이외에도 높은 신호 레벨의 혼선도 광섬유의 상호 전파되는 성질을 이용하여 태핑에 이용될 수 있다.

이러한 혼선에 의한 태핑 공격에 대한 방어책으로 단순하게 생각한다면 통신망 운영 레벨에서 처리할 수 있다고 생각할 수 있으나 이러한 대응책들이 또 다른 취약점이 될 수도 있고, 여러 가지 공격에 대한 대응책들의 상호 작용으로 인한 취약점이 생길 수 있어 보다 종합적이고 체계적인 대응책의 개발이 필요하다.

그림 6은 R 파장에서 이루어지는 아이크와 딕의 대화가 혼선에 의해 B 파장으로 흐르고 태핑으로 나타샤가 도청할 수 있거나 그 통화의 조정권을 일부 획득할 수 있음을 보여준다. 이 경우 해결책으로 통신망 운영 체제에 미리 등록되지

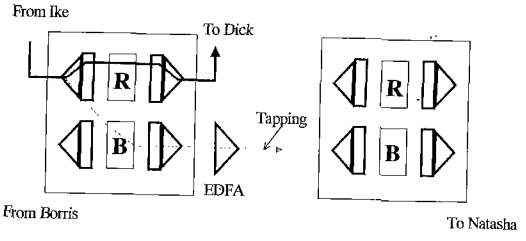

그림 6 Tapping Attack using WSS 1

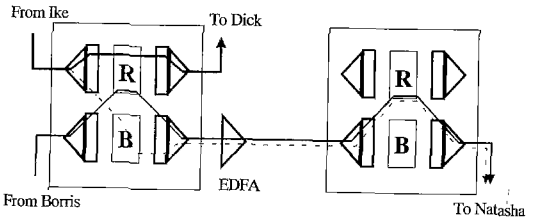

그림 7 Tapping Attack using WSS 2

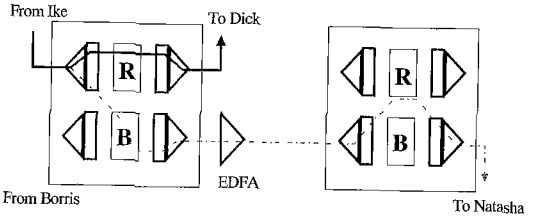

그림 8 Tapping Attack using WSS 3

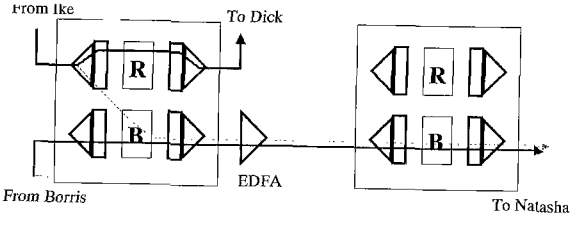

그림 9 Tapping Attack using WSS 4

않은 연결에 대한 증폭이나 스위치에서의 통과를 거부하게 하는 소프트웨어를 생각할 수 있다. 이러한 해결책에 대한 새로운 공격시도로 그림 7은 보리스가 나타샤와의 통화를 정당하게 신청하여 갑과 을간의 통화의 혼선에 영향을 받은 신호가 나타샤에게 전달되는 모습을 보여준다. 그림 8은 이때 보리스가 나타샤와의 통화를 중단하면 아이크에서 보내지는 통화가 나타샤에 의해 획득되어지거나 그 조정 권을 같게 되는 경우이다. 이에 대한 해결책으로 증폭기가 일정 수준 이하의 신호를 증폭시키지 못하게 한다면 그림 9에서와 같이 보리스와 나타샤 사이의 일정 수준 이상의 다른 파장의 신호를 흐르게 함으로써 이 해결책을 무위로 끝나게 할 수 있다. 따라서 이 예는 단편적인 해결책은 또 다른 취약점이 됨을 보여주고 있다.

4. 대응책

광 장치들 특히 광 증폭기가 보여주는 획득

경쟁에 의한 취약점은 기술의 발달에 따라 해결될 수 있을 것으로 생각되며 태핑에 의한 도청은 암호화에 의해서 해결될 수 있을 것으로 생각된다. 그러나 종래의 기법은 광 통신망에 비하면 비교적 느린 통신망에서 사용되는 암호화 기법으로 수백 Gbps 이상의 채널에는 적당하지 못하다. 결국 매우 빠른 암호화 장치 혹은 빠르게 동작되는 무작위 순열을 만드는 장치를 필요로 하게 된다. 잘못의 감지는 광 통신망의 각 노드가 투명하고 고속임으로 짧은 시간에 많은 양의 자료를 오염시킬 수 있고, 공격이 감지되는 때까지의 시간에 따라 회복이 불가능해 질 수도 있으며, 잘못된 공격 지의 결정이 매우 빠르게 통신망 전체의 성능에 영향을 줄 수 있기 때문에 중요하다. 현재의 통신망을 위한 방법은 파워 감지(power detection), 광 스펙트럼 분석(optical signal spectrum) 비트 에러 비율 시험(Bit Error Rate test), 파일럿 톤(Pilot Tone), OTDR 등이 있다. 이러한 방법은 통신 부하의 통계적인 분석이나 특별한 목적의 신호를 보내어 이상 유무를 알아내는 것이기는 하지만 WDM을 이용하는 광통신 망에는 본질적으로 적용하기 힘들다. 결국 암호화의 문제와 마찬가지로 광통신망의 속도에 접근하는 계산능력을 갖는 광 장치의 개발이 현재까지 알려진 대안이다.

이상의 장치들이 가능해지면 즉 악의적인 공격에 대한 감지가 가능하다는 것을 가정하면 공격이 이루어졌을 때 공격의 근원지를 알아내는 공격을 지역화를 위한 알고리즘이 개발되어야 한다. 이는 감지의 장치가 공격과 공격에 의한 파생을 구별하지 못할 뿐 아니라 감지 장치는 광 계산장치가 현실적으로 복잡하지 않은 회로로 구성되는 것 정도로 구현될 수밖에 없음으로 일종의 경보장치의 수준이 될 것임으로 더욱 필요하다. 목적은 근원지를 색출한 후 자동적인 회복을 가능하게 하기 위함인데 주지해야 할 것은 지역화가 초고속의 통신망인 전광통신망을 위한 것임으로 매우 빨라야 한다는 점이다. 그렇지 않다면 이미 너무 많은 자료가 영향을 받아서 회복이 불가능해질 수 있다. 따라서 분산환경에 적용되어 실행됨으로써 확장성을 유지해야 한다. 그림 10은 왜 공격의 지역화가 필요한지에 대한 예를 보여주고 있다. 공격은 노드 i에서 블루 채널 1을 통해 이루어졌지만 이 영향이 블루 채널 2를 통해 노드 j도 잘못을 감지하게 된다. 이때 노드 j는 노드를 폐쇄함으로서 공격을 막으려 시도한다면 공격을 당한 곳이 노드 i임으로 이 공격은 유효하게 다른 곳으로 전달될 수 있게 된다. 따라서 현재 공격을 당한 것처럼 감지기 되더라도 실제 공격이 일어난 곳을 찾아야 전체 통신망을 회복시킬 수 있게 된다.

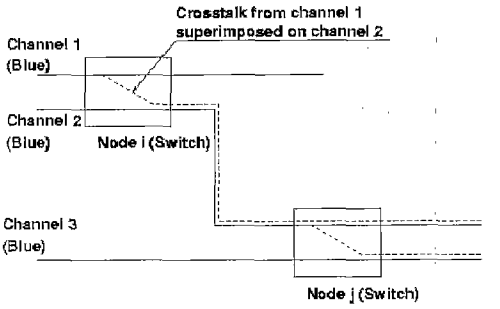

그림 10 Need for Attack Localization

5. 결 론

현재의 통신망은 부분적으로는 광 통신망이고 이들 사이에 전자적인 장비로 연결되어 있는 전자-광 통신망이라 하겠다. 그러나 투명성과 속도 그리고 전환 노드에서의 전환 가능성으로 인한 효율 등의 특성으로 인해 전광통신망은 멀티미디어 및 그래픽 기반의 사회에서 요구되는 필요를 충족시켜줄 수 있는 가장 실현 가능한 대안으로 기대되어지고 있다. 그러나 전광통신망은 기존의 통신망과는 다른 특이점들로 인해 통신망의 새로운 통신망 보안 문제를 안고 있다. 기반 통신망이 국가의 경쟁력과 안보에 미치는 영향이 커져감에 통신망 보안의 문제가 보다 체계적으로 다루어져야 할 것이다. 이 글에서는 사생활의 관점뿐 아니라 품질로 표현되는 통신망 자체의 보안의 관점에서 전광 통신망의 보안 문제를 다루어 보았다.

참고문헌

[1] MIT Lincoln Lab. Secure all optical Network, 1998.

[2] MIT Lincoln Lab. All optical Network Security 1998.
[3] Hongsik Choi, H, -A. Choi and M. Azizoglu, "On the All-to-All Broadcast Problem in Optical Network" Journal of Photonic Network Communication, p. 227-246, Vol. 2, Issue 3, August 2000.
[4] Hongsik Choi, S. Subramaniam, H.-A Choi, "Off-line wavelength assignment for permutation and all-to-one traffic in multifiber ring networks," Proceedings of SPIE, Nov. 2000.
[5] Rajiv Ramaswami, Kumar Sivarajan, Optical Network - a practical perspective, M. kauffmann Publishers 1998.

최 홍 식

1987 한림대학 전자계산학과 학사
1992 Michigan State University CS 석사
1996 George Washington University EE&CS 박사
1997~현재 한림대학교 정보통신공학부 조교수
1999 여름 GWU-NSA 연구원
2000~2001 GWU 연구원
E-mail:choi@sun.hallym.ac.kr

김 진

1984 고려대학교 물리학과 학사
1992 Michigan State University CS 석사
1996 Michigan State University CS 박사
1997~2000 건국대학교 전자계산학과 조교수
2000~현재 한림대학교 정보통신공학부 조교수
E-mail:jinkim@center.ce.hallym.ac.kr

윤 재 우

1983 전북대학교 전자공학과 공학사
1985 전북대학교 전자공학과 공학석사
1997~현재 전북대학교 전자공학과 박사과정
1998~현재 한국전자 통신연구소 부설 국가보안기술연구소 기반 4팀장
관심분야:정보보호, VPN, 네트워크 관제 시스템
E-mail:jyoon@nsri.etri.co.kr