무선 채널 특성을 이용한 비밀키 생성 기술 동향

백선엽
한국전자통신연구원 부설연구소

요 약

최근 안전한 무선 통신 시스템을 위하여 기존의 암호학적인 접근에서 벗어나 다양한 방식의 물리 계층 보안 기술이 제안되고 있다. 본고에서는 현재 사용되고 있는 암호학 기반의 키 생성 기술을 간략히 설명하고, 물리 계층 보안 기술 중 하나인 무선 채널 특성을 이용한 비밀키 생성 원리 및 기술 동향을 소개한다.

Ⅰ. 서 론

무선 통신 시스템은 언제 어디서나 인터넷에 접속할 수 있는 편의성을 제공한다. 수년 동안 무선 데이터 전송 속도도 급격히 증가하였다. 이제 사용자들은 시간과 공간의 제약 없이 친구들과 소통하며 회사 업무를 수행하고, 정보를 검색하며 은행 거래나 쇼핑을 즐길 수 있다. 이러한 이유로 인하여 무선 데이터 트래픽 사용량은 〈그림 1〉과 같이 해마다 폭발적으로 증가하고 있다[1].

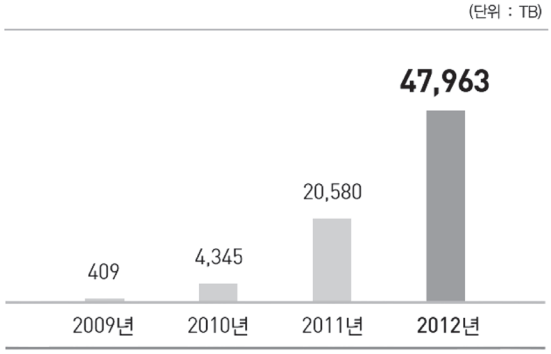

그림 1. 무선 데이터 트래픽 사용량

하지만, 자연적으로 개방되어 있는 무선 채널은 악의적인 사용자가 전송되는 무선 신호를 손쉽게 획득하거나 변경할 수 있다는 취약성이 존재한다. 최악의 상황에는 사용자들의 사생활이 공개되거나 신용카드 및 은행계좌 정보, 회사 기밀 자료가 외부로 유출될 수 있다. 무선 통신 시스템은 이런 보안 취약성을 해결하기 위해 응용, TCP, IP등의 다양한 계층에서 암호알고리즘을 활용한다. 암호알고리즘은 무선으로 전송되는 정보의 기밀성 (Confidentiality) 유지, 무결성 (Integrity) 보장, 사용자 인증 (Authentication) 등의 다양한 역할을 수행하고 있다.

암호알고리즘을 적용하기 위해 사용자들은 동일한 비밀키를 공유해야 한다. 현재까지는 물리적으로 비밀키를 직접 공유하거나, 키분배 센터(Key Distribution Center, KDC) 또는 공개키 인프라구조(Public Key Infrastructure, PKI)를 이용하여 비밀키를 분배 및 관리하는 방법을 주로 사용하고 있다. 하지만, 무선 통신 환경은 사용자의 이동으로 인하여 유선 통신 환경에 비해 보안 통신을 위한 키분배 및 관리가 쉽지 않다. 특히, 대표적인 분산 통신 환경인 무선 애드혹(Ad-hoc) 네트워크에서는 P2P 통신을 위한 키분배 인프라를 별도로 설치하기가 어렵다.

이러한 단점을 해결하기 위해 최근 무선 채널 특징을 이용한 비밀키 생성 기술들이 제안되고 있다. 두 사용자 사이의 무선 채널은 다른 사용자 사이의 무선 채널과 독립적으로 형성되며, 시간에 따라 변화하고, 위치에 따라 상관성이 급격히 줄어드는 특징을 갖는다. 또한, 무선 채널은 상반성(reciprocity)으로 인하여 두 사용자가 특정 시간 동안 유사한 무선 채널 상태 정보를 획득할 수 있다. 따라서 시분할 듀플렉스 (Time Division Duplex, TDD) 모드는 이용하면, 무선 링크를 형성하는 두 사용자만 알 수 있는 공통의 무작위한 정보를 공유할 수 있다.

무선 채널 특성을 이용하는 키 생성 기법으로 수신 신호 세기 또는 위상 정보를 이용하는 방식들이 주로 제안되고 있다. 현재까지 비밀키 생성 속도를 증가시키고, 랜덤성을 강화하기 위해 다단계 양자화, 다중 안테나, 중계기, 협력 통신 등을 이용하는 다양한 키 생성 기법들이 제안되고 있다.

본고는 다음과 같이 구성된다. Ⅱ장에서는 암호학 기반의 키 생성 프로토콜에 대하여 설명하고, Ⅲ장에서는 무선 채널 기반의 키 생성 원리에 대하여 설명한다. Ⅳ장에서는 다양한 무선 채널 특성을 이용한 키 생성 기술 동향에 대하여 설명한다. 마지막으로 Ⅴ에서는 결론을 기술한다.

Ⅱ. 암호학 기반 키 생성

키 생성은 두 명 이상의 사용자가 암호알고리즘에 공통으로 사용할 비밀키를 생성하는 과정을 의미한다. 인터넷 통신에서 세션이 시작될 때마다 새롭게 생성되는 세션키나 암호운용모드의 초기 벡터(Initial Vector, IV) 값이 대표적인 비밀키이다. 비밀키는 수명이 정해져 있기 때문에 정해진 데이터 사이즈를 초과하거나 시간이 경과하면 업데이트를 해줘야 한다.

암호알고리즘은 적용 환경에 적합한 암호운용모드와 결합되어 데이터 암·복호화에 사용된다. 〈그림 2〉는 일반적인 암·복호화 과정을 보여준다. 평문이 입력되면 사용자들 사이에 약속된 비밀키로 암·복호화가 수행된다. 이때, 도청자는 비밀키를 알 수 없기 때문에 획득한 암호문에서 평문을 복원할 수 없다. 암호알고리즘의 안전성은 비밀키 획득을 위한 계산 복잡도에 의해 결정되므로 비밀키의 길이가 충분하다면, 도청자에게 평문이 노출되지 않는다.

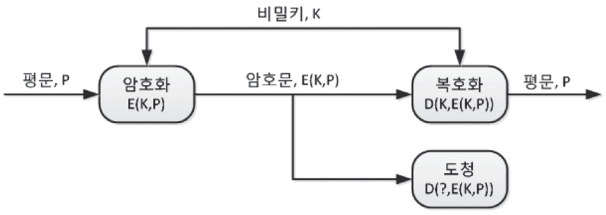

그림 2. 암호화와 복호화

앨리스가 N명의 사람과 교환을 하려 한다면, N개의 서로 다른 키가 필요하다. 만약 N 명의 사람들이 통신을 하려고 한다면, 전체 키의 수는N(N−1)/2개가 필요하다. 관리해야 하는 키의 개수가 사람 수의 증가에 따라 N^2로 증가한다는 단점이 존재한다. 이때 키의 길이가 증가할수록 저장할 용량도 커지게 되고, 키분배도 복잡해진다. 그 결과 효율적인 비밀키 분배를 위하여 키분배 센터(KDC)가 제안되었다[2].

KDC가 N명의 사용자들과 대칭키를 공유하게 되면, 관리해야 할 전체 키의 수는 N개로 줄어든다. 〈그림 3〉은 KDC를 이용하여 두 사용자, 앨리스와 밥이 비밀키를 생성하는 절차를 보여준다. 앨리스가 KDC에게 앨리스와 밥 사이의 비밀키를 요청하면, KDC는 공통 비밀키(K)를 생성하여 밥의 대칭키(K_B)로 암호화를 수행하고, 여기에 비밀키를 덧붙여 앨리스의 대칭키(K_A)로 한번더 암호화를 수행해 앨리스에게 전송한다. 앨리스는 수신된 암호문을 복호화해서 비밀키를 추출하고, 밥에게 나머지 암호문을 전송한다. 밥은 자신의 대칭키를 이용해 암호문을 복호화해 비밀키를 추출한다. 이후 앨리스와 밥은 공통 비밀키를 이용해 보안 통신을 수행한다.

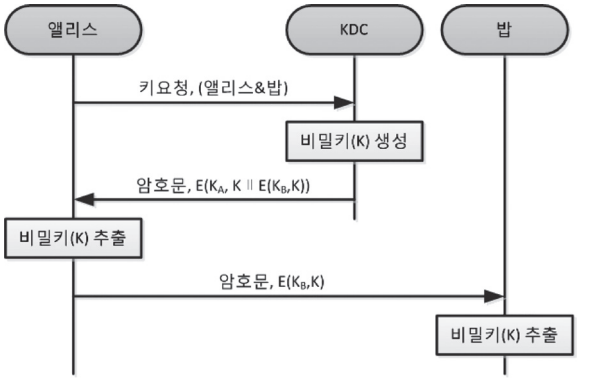

그림 3. KDC를 이용한 키 생성

한편, 〈그림 4〉와 같이 공개키를 이용하여 비밀키를 생성하는 기법도 제안되었다[3]. 앨리스가 밥의 공개키(K_P)를 획득해 공통 비밀키(K)를 암호화한 후에 전달하면, 밥은 자신의 개인키(K_S)를 이용하여 비밀키를 복원하게 된다. 이때, 개인키는 밥만 알고 있기 때문에 타인에게 앨리스가 전송한 비밀키가 노출되지 않는다. 하지만, 이러한 키 생성 방식은 인증되지 않은 공개키가 사용되는 것을 방지하기 위해 별도의 인증기관이 필요하다.

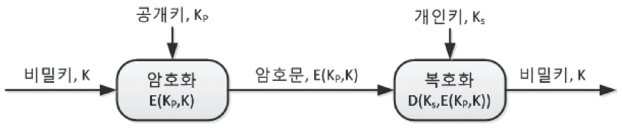

그림 4. 공개키를 이용한 키 생성

공개키를 인증하고 분배하는 PKI 구조는 〈그림 5〉와 같은 4단계의 계층으로 구성되며, 각 기관의 역할을 다음과 같다[4][5].

- PAA(Policy Approving Authority, 정책승인기관): 공인인증서에 대한 정책을 결정하고 하위 기관의 정책을 승인
- PCA(Policy Certification Authority, 정책인증기관): RootCA를 발급하고 기본 정책을 수립
- CA(Certification Authority, 인증기관): PCA의 하위 기관으로 인증서 발급과 취소 등의 실질적인 업무를 수행
- RA(Registration Authority, 등록기관): 사용자의 신분을 확인하고 CA간 인터페이스를 제공

분산형 네트워크에서는 KDC와 PKI 구성이 쉽지 않아서 두 사용자가 대칭 세션키를 직접 생성하는 방안으로 이산대수문제에 기반한 Diffie-Hellman 방식이 제안되었다[6]. 사용자가 p와 g를 선택하고, 두 사용자가 개별적으로 g의 지수가 되는 x와 y를 랜덤하게 발생시켜 키를 생성한다. 〈그림 6〉은 Diffie-Hellman 기반의 키 생성 방식을 보여준다.

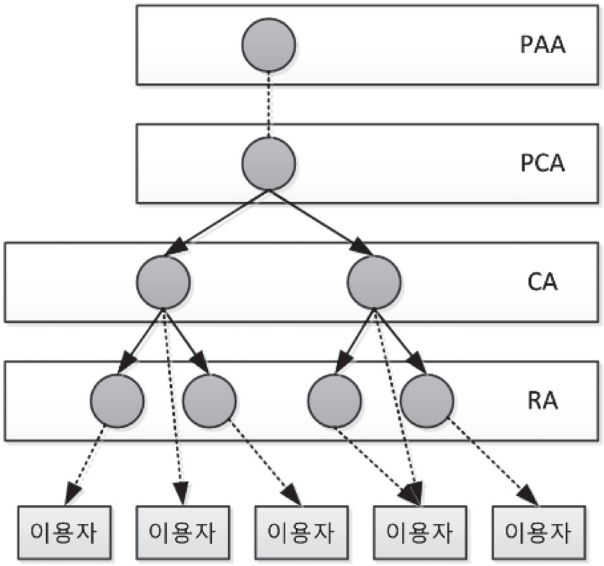

그림 5. PKI 구조

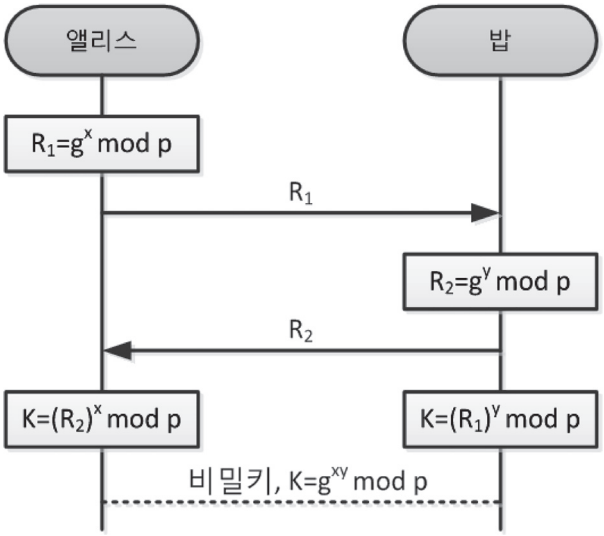

그림 6. Diffie–Hellman 방식의 키 생성

암호알고리즘의 키 생성은 공격자의 연산 능력으로 유효시간 내에 비밀키를 추출할 수 없다는 가정하에 안전성이 검증된다. 추후 비밀키를 효율적으로 추출하는 방법이 등장하거나, 양자 컴퓨터와 같이 연산 능력을 획기적으로 증가 시킬 수 있는 장비가 나온다면 계산 복잡도를 훨씬 증가시켜야 한다.

Ⅲ. 무선 채널 기반 키 생성 원리

무선 채널 기반의 키 생성은 다음의 무선 채널 특성을 최대한 활용한다[7].

- 랜덤성: 다중 경로 채널 페이딩은 반사, 회절, 산란 등의 원인으로 인하여 전송 시간에 따라 랜덤하게 변이한다.
- 독립성: 반파장 이상 떨어진 위치에서는 확률적으로 독립적인 무선 채널이 형성되고, 상관관계가 없는 페이딩을 경험한다.
- 상반성: 상관 시간(coherence time) 이내에 두 사용자가 송 · 수신하는 신호는 동일한 페이딩을 경험한다.

앨리스(Alice,A)와 밥(Bob,B)이 생성하는 다중 경로 무선 채널은 〈그림 7〉과 같이 형성된다. 앨리스가 밥에게 전송하는 무선 신호는 다중 경로에서 여러 물체의 반사와 회절, 산란이 발생하여 시간과 위치에 따라 변화한다. 도청자 이브(Eve,E)가 관찰하는 신호는 앨리스와 밥의 다중 경로와 독립적으로 형성된다.

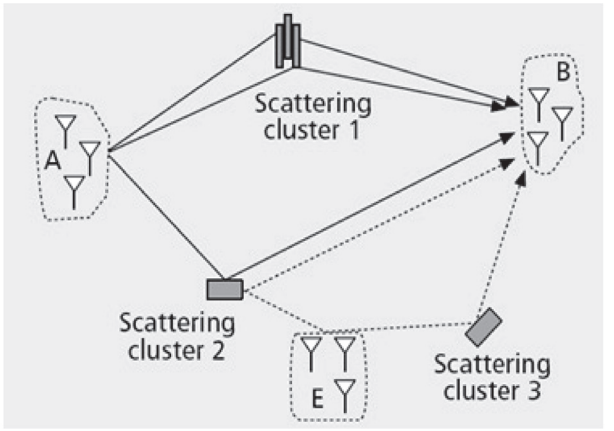

그림 7. 다중 경로 무선 채널 환경

무선 채널 상반성으로 인하여 〈그림 8〉과 같이 앨리스와 밥은 기준 신호를 교환하여 둘 사이의 무선 채널에서 동일한 채널 상태 정보를 획득할 수 있다. 하지만, 도청자 이브가 앨리스 또는 밥과 형성하는 무선 채널이 앨리스와 밥이 형성하는 무선 채널

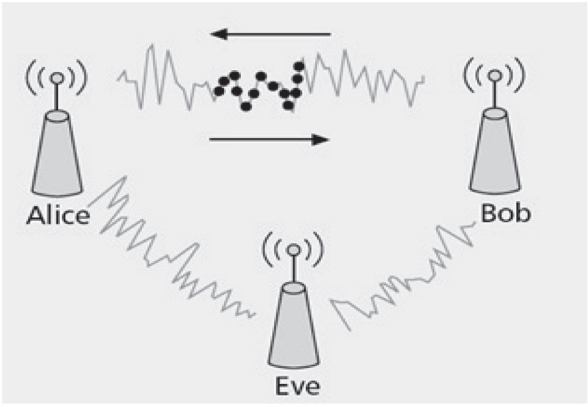

그림 8. 무선 채널 상반성

과는 확률적으로 독립이고, 상관관계가 적다. 따라서 이브는 앨리스와 밥의 무선 채널 상태를 유추하기 힘들다. 이러한 특성을 활용하여 앨리스와 밥은 둘 사이의 무선 채널 상태 정보에서 유일한 비밀키를 생성하게 된다.

Mauer와 Ahlswede, Csizar은 공통의 무작위 변수를 통한 비밀키를 생성하는 연구했다[8][9]. 두 사용자가 공통의 무작위 변수로부터 도청자가 알 수 없는 비밀키를 생성하기 위해 다음 4단계 과정이 순차적으로 수행된다[10].

1. Randomness Sharing: 랜덤 정보를 공유하는 과정으로 무선 통신에서는 무선 채널 상태 정보가 랜덤 정보가 된다. TDD와 같은 방식으로 동작하면, 두 사용자가 동일한 무선 자원을 사용하게 된다. 이때, 두 사용자가 기준 신호를 교환하면 동일한 무선 채널 상태 정보를 공유할 수 있다.

2. Advantage Distillation: 앨리스와 밥 사이의 공통 정보량이 앨리스와 이브 혹은 밥과 이브 사이의 공통 정보량보다 많도록 하는 과정이다. 무선 채널 상반성과 반파장 이상의 위치에서 채널 상관관계가 급격히 줄어드는 특성을 이용하면 별도의 단계를 거치지 않고도 대부분 요구 조건을 충족한다.

3. Information Reconciliation: 두 사용자가 공유하는 무선 채널에서 잡음 및 간섭, 국부 발진기(Local Oscillator, LO)의 오프셋 등으로 인하여 동일한 정보를 추출하지 못할 수 있다. 이를 해결하기 위하여, 공개 채널을 통해 둘 사이의 차이, 즉 오류를 정정하는 메시지를 교환하고 이를 통하여 동일한 비트 시퀀스를 추출한다[11].

4. Privacy Amplification: 공개적으로 교환된 오류정정부호에 의해 노출된 정보를 없애거나 추출한 비트 시퀀스의 랜덤성을 강화시키는 과정이다. 앞 단계에서 추출된 비트 시퀀스가 랜덤성을 만족시키지 못하면 해쉬함수 등을 적용하여 비밀키의 랜덤성을 증가시킨다[12]. 비트 시퀀스가 해쉬함수를 거치게 되면 일반적으로 비밀키의 길이는 줄어들게 된다.

무선 채널 특성을 이용한 비밀키 생성 연구는 다음과 같은 목적을 갖는다. 첫 번째는 견고한 키 생성을 위하여 키일치율(Key Agreement Probability)을 최대화 하는 것이다. 두 번째는 키 생성 속도(Key Generation Rate)의 증가시키는 것이다. 동일한 자원에서 보다 빠르게 비밀키를 추출하는 것이 목적이다. 세 번째는 키의 랜덤성을 확보하는 것이다. 안전한 비밀키는 랜덤해야 하는데, 무선 채널의 특성상 확률적으로 생성된 비밀키 사이에 상관관계가 존재할 수 있다. 이를 방지하기 위해 Privacy Amplification를 수행하여 랜덤성을 증가시킨다. 만약 추출된 비트 시퀀스가 충분히 랜덤하다면, Privacy Amplification 단계를 생략할 수 있기 때문에, 키 생성 속도 또한 증가한다.

무선 채널 기반의 비밀키 생성은 정보 이론 관점에서 키 생성의 한계점을 찾는 연구와 실제 무선 환경에서 효율적으로 키를 추출하는 연구로 나눌 수 있다. 본고에서는 실제 환경에 적용 가능한 비밀키 생성 기술을 중점으로 설명한다. 다음 장에서는 다양한 무선 채널 특성을 이용한 비밀키 생성 기술 동향에 대하여 서술한다.

Ⅳ. 무선 채널 특성 기반 키 생성 기술

다양한 무선 채널 채널 특성을 이용한 비밀키 생성이 제안되고 있다. A.-Sadjadi 등은 〈그림 9〉와 같이 실측을 통해 채널 상반성 가능성을 확인하고, 수신 신호 세기(Received Signal Strength Indicator, RSSI)가 깊은 페이딩(Deep Fading)에 빠지는 순간을 이용해 키를 추출하였다. 이러한 접근은 채널의 상반성이 완전히 보장되지 않는 경우에 좀더 견고하게 키를 생성할 수 있다. 또한, PUF(Physically Unclonable Function)의 에러 정정에 주로 사용되던 'Fuzzy Extractor'에 Privacy Amplification를 추가한 'Secure Fuzzy Information Reconciliation'기법을 제안해 추출된 비트 시퀀스의 엔트로피를 증가시켰다. 하지만, 이 방식은 깊은 페이딩에 빠지는 무선 채널 상황에서만 비밀키가 생성되기 때문에 상대적으로 낮은 키생성률을 갖는다[13].

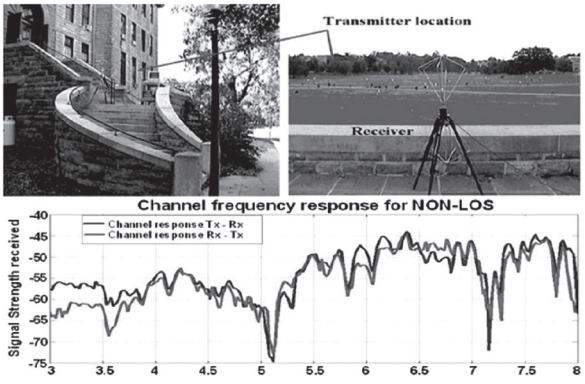

그림 9. RSSI 상반성 측정

Mathur 등은 〈그림 10〉과 같이 특정값을 기준으로 RSSI값이 교차하는 특성(Level Crossing)을 이용하여 키를 추출하였다[14]. 단말의 RSSI 평균과 표준편차를 이용하여 특정값을 설정하였다. Jana 등은 RSSI 기반의 낮은 키생성률을 극복하기 위

하여 적응적인 키 생성 기법을 제안하였다[15]. 측정된 RSSI값은 작은 블록으로 나뉘어지게 되고, 다단계 양자화를 수행한다. Gray Code 시퀀스를 이용하여 한 개의 RSSI 샘플에서 다중 비트를 추출하지만, 생성되는 비트 수가 증가할수록 키일치율이 감소하게 되는 단점이 존재한다.

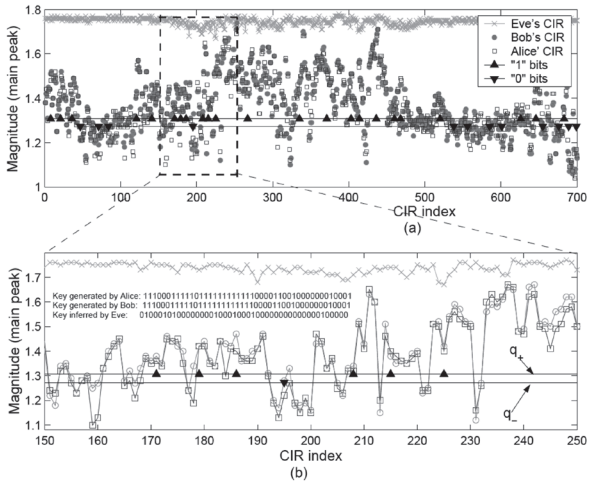

그림 10. RSSI를 이용한 키 생성

Zeng 등은 키생성률을 증가시키기 위하여 〈그림 11〉과 같이 다중 안테나 환경을 이용하였다[16]. 안테나의 수에 따라 안테나들이 독립적으로 형성하는 채널의 수도 증가한다. 〈그림 12〉와 같이 채널 측정을 위한 송·수신 안테나를 변화시켜 RSSI 샘플을 추출하고, 다단계 양자화를 통해 키를 생성하였다. 실제 다양한 무선 환경에서 무선랜 하드웨어를 이용하여 실험을 수행한 결과, 다중 안테나로부터 추출된 RSSI 샘플의 랜덤성이 향상되어 키생성률이 증가하는 것을 확인했다.

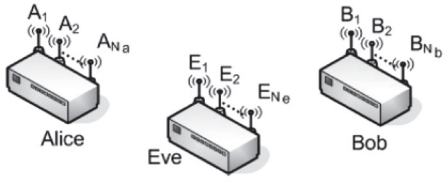

그림 11. 다중 안테나 환경

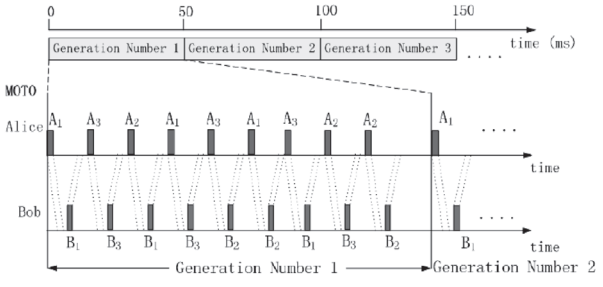

그림 12. 다중 안테나를 이용한 키 생성

한편, 무선 채널의 RSSI 특성 외에 위상 정보를 이용한 키 생성 기법들도 제안되었다. 위상 정보는 균일한 분포의 특징을 갖는 점이 랜덤성을 필요로 하는 키 생성에서 가장 큰 장점을 갖는다. 또한, 동기가 적절히 이뤄진 상환에서는 RSSI에 비하여 다단계 양자화를 쉽게 적용시킬 수 있다. Koorapaty 등은 이 분야의 개척자로 다중 반송 주파수(Multiple Carrier Frequency)의 위상 차이를 이용한 키 생성 기법을 제안하였다[17]. 이 방식은 LO오프셋에서 발생하는 측정 오류를 극복할 수도 있다. Sayeed 등은 OFDM을 이용하여 다중 반송파를 통해 위상 샘플 수를 늘려 키 생성 속도를 증가시켰다[18].

Ren 등은 무선 채널의 위상 정보를 이용하여 정적 채널에서 키생성률을 증가시키는 방법과 그룹키 생성 방안을 제안하였다[19,20]. 〈그림 13〉, 〈그림 14〉는 A, B, C 세 사람이 2단계에 거쳐 동일한 그룹키를 생성하는 과정을 보여준다. A가 랜덤 위상을 생성한 후, 시계 방향과 시계 반대 방향으로 총 6번의 전송을 통하여 세 사람 모두 동일 위상 정보 $\phi_A + \phi_A' + \theta_{AB} + \theta_{BC} + \theta_{CA} \bmod 2\pi$를 획득하고, 이를 양자화시켜 그룹키를 생성한다. 하지만, 그룹내 사용자수가 증가하면 그룹키를 생성하기 위한 전송 기간이 길어져 상관 시간을 만족하지 못하는 경우가 발생할 수 있다. 이를 해결하기 위해 Baek 등은 그룹키 생성 마스터 개념을 도입하여 상관 시간 이내에 그룹키를 생성하는 방안에 대하여 제안하였다[21].

Huang 등은 정적인 채널에서 다중 안테나의 전송 신호 세기

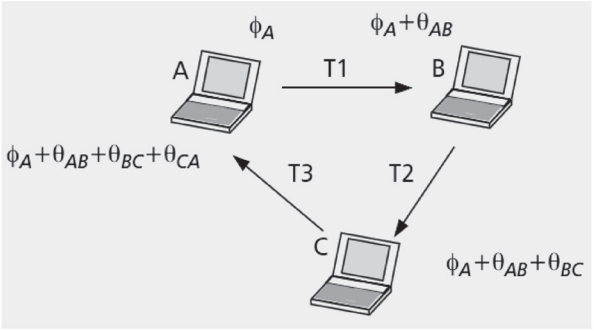

그림 13. 그룹키 생성 1단계

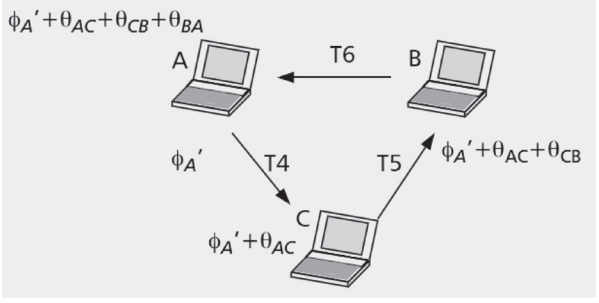

그림 14. 그룹키 생성 2단계

와 위상을 조절하여 인위적인 채널 변화를 유발시키고, 이를 통하여 키 생성 속도를 증가 시키는 방안에 대하여 연구하였다[22]. Baek 등은 다중 사용자의 스케줄링에 따른 랜덤성 성능을 평가하였다[23]. 표 1은 사용자 수(N)에 따른 NIST 랜덤성 테스트별 성능 평가 지표(p-value)를 나타낸다[24]. p-value가 0.01과 0.99 사이에 존재하면 생성된 비밀키의 랜덤성을 충족한다. 사용자의 수가 증가할수록 랜덤성을 향상시켜 비밀키 생성 시 Privacy Amplification 단계를 최소화할 수 있다.

표 1. 사용자 수에 따른 랜덤성 성능 평가

Test	N=1	N=2	N=5	N=10
Frequency	0	0.437274	0.637119	0.834308
Block Freq.	0	0	0	0.122325
Runs	0	0.066882	0.739918	0.534146
Rank	0	0.090936	0.002043	0.911413
FFT	0	0	0	0.122325
Serial	0	0	0.437274	0.012650
Linear Complex.	0	0.437274	0.213309	0.534146
Cusum (Fwd)	0	0.035174	0.275709	0.534146
Cusum (Rev)	0	0.017912	0.739918	0.964295

Zan 등은 〈그림 15〉와 같이 무선 주파수 채널을 도약(Hopping)하면서 두 사용자가 동일할 채널 정보를 공유하면 ACK를 전송해 키를 생성하는 방안을 제안하였다[25]. 하지만, 이 방식은 도청자가 모든 채널은 도청하고 있다면, 공격이 가능하기 때문에 동일한 시스템 사용자의 공격에만 적용이 가능하다.

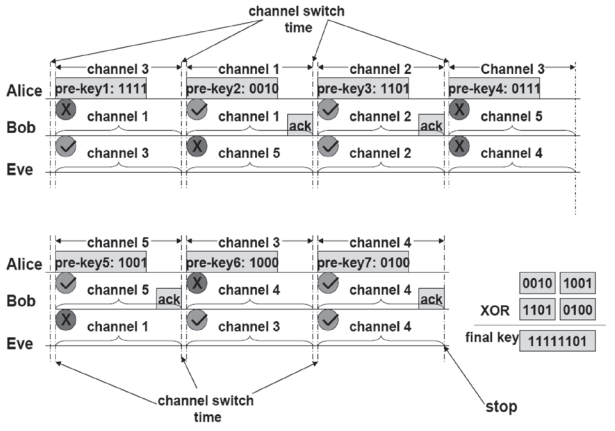

그림 15. 채널 도약을 이용한 키 생성

한편, 중계기가 협력 통신을 수행해 비밀키를 생성하는 다양한 방안들도 제안되었다. Xu 등은 시간 동기가 이뤄지지 않는 통신 환경에서 위상 정보를 이용할 때 발생하는 LO의 오프셋 문제를 해결하기 위하여 신뢰할 수 있는 중계기를 도입하였다[26]. Lai 등은 정적인 채널 환경에서 랜덤성을 향상시켜 키 생성률을 증가시키기 위하여 다수의 중계기를 이용하였다[27]. 중계기 수와 선형적으로 멀티플렉싱 이득이 발생하는 것을 확인하였다. Liu 등은 노드들 간의 협력을 이용하여 RSSI 기반의 그룹키를 생성하는 방안을 제안하였다[28]. 노드들의 분산 형태에 따라 Star 방식과 Chain 방식의 장 · 단점을 평가하였으며, 실내 · 외 다양한 무선 환경에서 ZigBee 하드웨어를 이용해 실제 그룹키 생성을 실험하였다.

Ⅵ. 결 론

본고에서는 물리 계층 보안 기술 중 하나인 무선 채널 특성을 이용한 비밀키 생성의 원리 및 기술 동향을 살펴보았다. 향후 분산형 무선 통신 시스템이 확산되면, 기존 키분배 프로토콜을 대체할 후보 기술로 예상된다. 앞으로 무선 통신 시스템에 적용하기 위해서는 보다 효율적이고 견고한 키 생성 기술에 대한 연구가 필요하며, 다양한 무선 채널 환경에서 제안된 방식으로 생성된 비밀키의 안전성 검증도 필요하다.

참 고 문 헌

[1] 미래창조과학부, 과학기술과 ICT를 통한 창조경제와 국민행복 실현, 2013.
[2] W. Stallings, Cryptography and Network Security, Pearson, 2013.
[3] B. A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2007.
[4] W. Stallings, Network Security Essentials: Applications and Standard, Pearson, 2010.
[5] 양대일, 정보보안개론, 한빛아카데미, 2013.
[6] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976.
[7] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the Physical Layer for Enhanced Security," IEEE Wireless Communications, vol. 17, no. 5, pp. 63-70, October 2010.
[8] U. M. Mauer, "Secret Key Agreement by Public Discussion from Common Information," IEEE Transactions on Information Theory, vol. 39, no. 3,

pp. 733-742, May 1993.
[9] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography, Part I: Secret Sharing," IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 1121-1132, July 1993.
[10] M. Bloch and J. Barros, Physical-Layer Security, Cambridge, 2011.
[11] G. Brassard and L. Savail, "Secret-Key Reconciliation by Public Discussion," in Proc. EUROCRYPT'93, LNCS, vol. 765, pp. 410-423.
[12] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized Privacy Amplification," IEEE Transactions on Information Theory, vol. 41, no. 6, pp. 1915-1923, November 1995.
[13] B. A.-Sadjadi, A. Kiayais, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks," in Proc. ACM CCS, Alexandria, USA, 2007, pp. 401-410.
[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik,"Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in Proc. ACM MobiHoc, San Francisco, USA, 2008, pp. 128-139.
[15] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," in Proc. ACM MobiCom, Beijing, China, 2009, pp. 321-332.
[16] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," in Proc. IEEE INFOCOM, San Diego, USA, 2010, pp. 1-9.
[17] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure Information Transmission for Mobile Radio," IEEE Communications Letters, vol. 4, no. 2, pp. 52-55, February 2000.
[18] A. M. Sayeed and A. Perrig, "Securing Wireless Communication: Secret Keys through Multipath," in Proc. IEEE ICASSP, Las Vegas, USA, 2008, pp. 3013-3016.
[19] K. Ren, H. Su, and Q. Wang, "Secret Key Generation Exploiting Channel Characteristics in Wireless Communications," IEEE Wireless Communications, vol. 18, no. 4, pp. 6-12, August 2011.
[20] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks," in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 1422-1430.
[21] S. Y. Baek and J. Park, "Group Key Establishment Scheme Using Wireless Channel Status," in Proc. IARIA ICSNC, Lisbon, Portugal, 2012, pp. 83-87.
[22] P. Huang and X. Wang, "Fast Secret Key Generation in Static Wireless Networks: A Virtual Channel Approach," in Proc. IEEE INFOCOM, Turin, Italy, 2013, pp. 2292-2300.
[23] S. Y. Baek and J. Park, "A Study on Wireless Secret Key Randomness in Multiuser Networks," in Proc. IEEE ICTC, Jeju, Korea, 2013, pp. 1048-1052.
[24] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST SP800-22 Rev.1a, April 2010.
[25] B. Zan and M. Gruteser, "Random Channel Hopping Schemes for Key Agreement in Wireless Networks," in Proc. IEEE PIMRC, Tokyo, Japan, 2009, pp. 2886-2890.
[26] K. Xu, Q. Wang, and K. Ren, "Wireless Key Establishment with Asynchronous Clocks," in Proc. IEEE MILCOM, Baltimore, USA, 2011, pp. 1410-1415.
[27] L. Lai, Y. Liang, and W. Du, "Cooperative Key Generation in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 30, no. 8, pp. 1578-1588, September 2012.
[28] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks," in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 927-935.

약 력

백 선 엽

2003년 KAIST 공학사
2010년 KAIST 공학박사 (석박통합)
2010년 KAIST 정보전자연구소 박사후연구원
2010년~현재 한국전자통신연구원 부설연구소 선임연구원
관심분야: 물리계층보안, 네트워크보안, 이동통신보안, 임베디드 시스템