시간값을 이용한 경량의 Pair-wise 키 생성 기법

정진호, 이종협, 송주석
연세대학교 컴퓨터과학과
e-mail : {jin10058, jhlee, jssong}@emerald.yonsei.ac.kr

A Light-weight Pair-wise Key Generation Scheme using Time value

Jin-Ho Jung, JongHyup Lee, and JooSeok Song
Department of Computer Science, Yonsei University

요 약

본 연구에서는 하드웨어적으로 제한사항이 있는 장비에서 최소한의 보안성을 제공하기 위해 XOR 방식의 Pair-wise 키값을 생성하는 간단한 보안기법을 제안한다. 제안한 보안 기법은 Random Key Predistribution 을 통하여 장비별 시간값과 고유값을 XOR 하여 서로 교환한 후, 상호 교환한 값을 다시 XOR 하여 두 장비간의 Pair-wise 키값을 생성한다. 이후, 지속적으로 변화되는 시간값으로 인해 매 통신시마다 다른 Pair-wise 키값을 사용할 수 있을 것이다. 기존의 보안알고리즘(DES, AES 등)의 연산 보다 매우 간단하고, 노드별 독특한 키 변화패턴을 통하여 키 유출이 어려우며, 장비가 캡처당하는 공격이 발생하더라도 전체 네트워크의 보안성이 저하되지 않는다는 장점을 가진다.

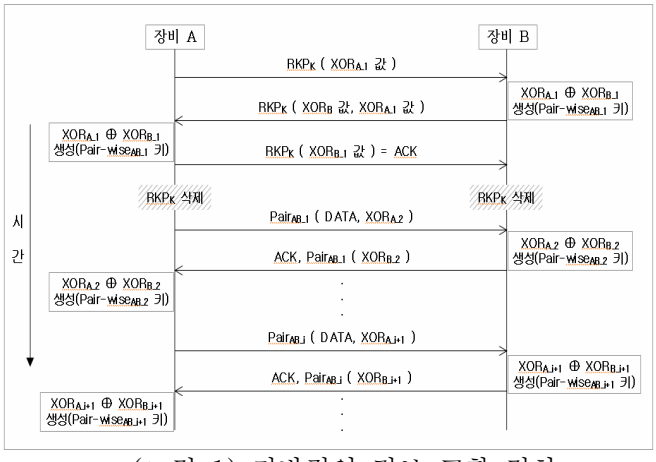
1. 서론

센서, RFID 등 하드웨어의 용량이 제한적인 여러 장비에서는 보안성이 높은 알고리즘을 사용하기에 제한점이 많다[1][2]. 또한 일부 네트워크에서는 보안을 고려하지 않은 채 구성하기도 하지만 보안의 필요성은 절대 간과될 수 없으며, 앞으로도 더욱 중요시 될 것이다. 그렇기 때문에 어떠한 네트워크라도 최소한의 정보보호가 요구되고, 우리는 이렇게 저장공간, 메모리, 전원용량 등의 제한 요소가 많은 장비에 대한 아주 간단한 보안 기법을 제안하려고 한다. 우리는 네트워크를 구성하고 있는 장비별 시간값과 고유값을 XOR 하는 방법을 통해 노드간 Pair-wise 키를 생성하여 데이터를 보호하고, 변화되는 시간을 통한 One-Time Pad 키를 지속적으로 생성하여 통신 암호화에 적용한다. 제안하는 방법은 센서네트워크와 같이 성능이 제한적인 네트워크 환경에서 안전한 보안서비스를 제공할 수 있다.

2. 제안하는 키생성 및 암호화 기법

본 절에서는 XOR 기반의 경량 암호화 기법을 제안한다. 제안하는 기법에서는 장비별로 고유값과 시간값을 XOR 한 후 통신하고자 하는 장비끼리 그 값을 교환한다. 이후 두 값을 다시 XOR 하여 키값을 생성한다. 여기서 키값의 지속적인 변경을 유도하기 위해 시간값을 키 생성 과정에 적용한다. 장비별 최초로 XOR 한 고유값은 Random Key Predistribution (RKP)[3] 방식을 이용하여 상호 동일한 키를 선분배(predistribution)한 장비간에만 안전하게 통신이 가능하다. 만일 장비 A 와 장비 B 가 RKP 방식을 통해 동일한 키를 보유하고 있다면, A 와 B 는 최초 서로의 XOR 값을 교환한 후 공유하고 있던 키를 삭제한다. 그림 1 은 RKP 를 통한 공유키 전달 과정의 절차를 나타낸다.

RKP 방식은 완벽한 연결성을 보장하지 못한다는 문제점을 가지고 있지만, 전체 연결성(Global Connectivity) 측면에서 최종 목적지까지의 충분한 데이터 전달률을 보장 받을 수 있다[3]



(그림 1) 전반적인 정보 교환 절차

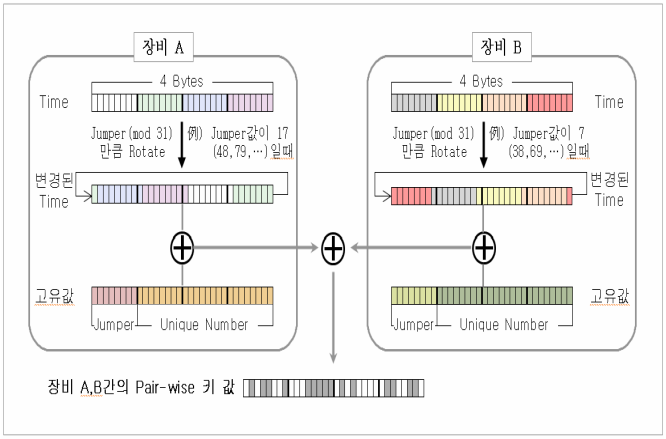
모든 장비는 최초 분배 전에 Jumper(1Byte)와 Unique Number(3Bytes) 라는 4Bytes 의 임의 고유값을

이 논문은 2008 년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10614-0).

가지게 된다. 장비 A 는 현재의 시간값(4Bytes)을 Jumper(mod 31) 값만큼 오른쪽으로 Rotate 하고, Rotate 하여 변경된 시간값(4Bytes)과 고유값[Jumper + Unique no. / 4Bytes]을 XOR_{A_1}(장비 A 의 첫번째 XOR 값)한다. 장비 B 도 위와 같은 과정을 통해 XOR_{B_1} 값을 생성한다. 두 장비(A, B)가 각각의 XOR 값을 RKP 키 값에 의해 서로 교환한 이후, 두 장비의 XOR 값을 다시 XOR 하여 서로간에 같은 키($Pair\text{-}wise_{AB\_1}$: 장비 A, B 의 XOR 값들을 처음으로 XOR 한 값)를 생성한다.

제안하는 기법에서는 센서(또는 장비)가 필드에 설치되는 경우, 정확한 시간동기화가 이루어지기 어렵다는 점에 착안하여[4], 두 장비간에 자연스럽게 발생되는 시간적 오차를 이용하여 randomness 를 적용하고 이를 통해 보안성을 높이고자 한다.

위에서 언급한 첫번째 Pair-wise 키의 생성과정은 그림 2 와 같다.



(그림 2) 첫번째 Pair-wise 키 생성과정

이후, 송신을 하고자 하는 장비는 DATA 와 다음 사용할 키값을 $Pairwise_{AB}$ 키로 암호화하여 전송한다. 여기서, 다음 사용할 키 $NewPairwise_{AB}$ 는 송신하고자 하는 노드가 본인의 XOR 값을 31 로 모듈러하고, DATA 송신시 시간을 XOR(mod 31)값만큼 오른쪽으로 Rotate 한 후, 고유값(Jumper + Unique No.)과 XOR 하여 생성한다. DATA 를 수신한 장비 또한 자신의 $NewPairwise_{AB}$ 를 같은 방법으로 생성하여 ACK 에 포함하여 전송한다. 이후 DATA 를 송신할 때 마다 각 장비는 새로운 Pair-wise 키로 갱신하여 암호화 통신을 수행한다.

전송 실패와 연결 재설정과 같은 상황에 대비하여 서로 통신을 주고 받는 장비들은 이전의 Pair-wise 키 값과 현재의 Pair-wise 키값을 메모리에 임시 저장하고, 연결에 문제가 생긴 경우 저장된 값을 이용하여 빠른 복구를 실행한다.

송신시의 비동기적인 시간을 이용하는 알고리즘의 특성상 제안하는 기법은 DATA 전송주기가 비정기적이고 빈번하지 않은 환경에서 더욱 효과적일 것으로 예상된다.

3. 향후 연구과제

제안하는 기법은 다양한 공격에 대한 안전성과 실용성 분석을 기반으로, 기존의 보안알고리즘인 DES, AES 보다 연산이 간단하고 robust 하다는 것에 대한 수치적 분석 등을 추가적으로 연구할 계획이다. 또한, 키값(4 Bytes → 16 bytes)을 확장하기 위한 방법, Brute-Force Attack 에 대한 안전성 분석, 키 생성과정상에 나타나는 Weak Keys, Sensor 등 하드웨어적으로 제한사항이 있는 장비에서의 실제 구현(필요한 메모리 요구량, Computation 오버헤드 등) 등의 측면에서도 지속적으로 연구를 수행할 예정이다.

4. 결론

제안한 보안 기법은 실시간 전송이 가능한 Stream Cipher 기법으로써, 각 장치의 시간값과 고유값을 XOR 한 후 Pair-wise 키를 생성, 매 통신시마다 다른 Pair-wise 키를 사용한다는 특징을 가진다. 특히, 성능이 제한된 환경을 고려하여, 기존 보안알고리즘의 연산보다 간단한 방식을 사용하면서도 One-Time Pad 형태의 key stream 을 제공하여 높은 안전성을 보장한다. 또한, 고유값인 Jumper, Unique no.가 초기에 노출되지 않는다는 가정하에서, 각 노드마다 독특한 키 변화 패턴을 통하여 키 유출이 어렵고 Pair-wise 키 방식을 도입하여 일부 장비가 캡처당하는 공격이 발생하더라도 전체 네트워크의 보안성이 저하되지 않는다는 장점을 가지고 있다.

참고문헌

[1] H. Chan, A. Perrig, and D. Song, “Random Key Pre-distribution Schemes for Sensor Networks,” IEEE Symposium on Security and Privacy, pp. 197-213, 2003.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications Magazine, Vol.40, No 8, pp. 102–114, 2002.

[3] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” the 9th ACM Conference on Computer and Communication Security, pp. 41-47, 2002.

[4] M. Maróti, B. Kusy, G. Simon, and Á. Lédeczi, “The Flooding Time Synchronization Protocol”, ACM conference on Embedded networked sensor systems (SenSys), pp 39-49, 2004.

[5] B. Forouzan, “Cryptography and Network Security”, McGRAW HILL, 2008