웨어러블 센서데이터를 위한 시각 동기화 기반 암호화 방법

최종화, 안상현*
서울시립대학교 컴퓨터과학과
e-mail : david13@uos.ac.kr, ahn@uos.ac.kr*

An Encryption Method for Wearable Sensor Data Based on Time Synchronization

JongHwa Choi, Sanghyun Ahn*
e-mail : david13@uos.ac.kr, ahn@uos.ac.kr*
Dept. of Computer Science, University of Seoul

요 약

웨어러블 기기들의 환경은 저성능부터 고성능으로 다양하게 있다. 성능이 제한적인 기기에 대해서는 공개키 암호화 방식을 사용하여 지속적으로 통신하기에 어려움이 있다. 본 연구에서는 시각정보를 이용한 비밀키 암호화 방식을 제안한다.

1. 서론

웨어러블 분야가 발전함에 따라, 다양한 분야에서 사용되고 있으며, 센서 데이터는 민감한 개인정보를 다루어지며 보안위협이 증대하고 있다.

웨어러블 기기들의 환경은 저성능부터 고성능으로 다양하게 존재한다. 성능이 제한적인 기기에 대해서는 공개키 암호화방식을 지속적으로 사용하기에는 어려움이 있다.

기존의 공개키 암호화 방식을 저성능 기기에 적용하기 힘든 문제점을 해결하고자 ID-PKC[1], CL-PKC[2], IBE[3]와 같은 연구가 진행되었다. 그러나 ID 기반의 암호의 단점으로 비밀키가 신뢰 기관에 위탁되기 때문에 개인이 사용하는 웨어러블 기기에는 적합하지 않다. 따라서 신뢰기관에 의해서 위탁되지 않으면서 비밀키를 사용하여 저성능에서도 안전하게 데이터를 전달할 수 있을 것으로 기대한다.

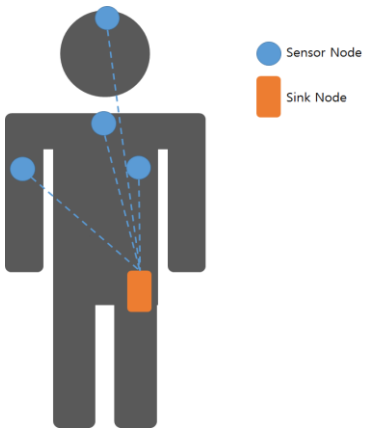

그림 1

웨어러블의 경우에는 싱크노드가 마스터, 센서노드가 슬레이브로 1-hop 으로 구성되어 있는 경우가 대다수 이다. 따라서 본 연구에서는 그림 1 과 같이 싱크노드와 센서노드가 주종관계의 환경에서 동작하는 것으로 가정한다.

2. 본론

본 논문에서 제안하는 암호화의 주 기반은 대칭키 암호화 방식으로 진행되며, 대칭키인 비밀키를 안전하게 전송하기 위해 초기화 부분에서만 공개키를 사용하고자 한다. 비밀키를 안전하게 전송 후에는 해당 비밀키를 가지고 암호화 하여 전송을 하도록 한다. 센서 데이터의 값의 경우에는 나올 수 있는 값의 범위가 한정적이기 때문에 같은 센서 값 이여도 다른 암호문으로 전달해야한다. 따라서 시각(time) 정보와 IV(Initialization Vector)를 이용하여 블록암호를 적용하고자 한다. 시각정보를 사용하기 위해서는 Sink Node 와 Sensor Node 간 시각동기화가 이루어 져야 한다.

WSN(Wireless Sensor Network)의 시각 동기화 프로토콜에 관한 연구는 TPSN[4], FTSP(Flooding Time Synchronization Protocol)[5], RBS[6], IBS[7]이 있다. IBS 가 다른 프로토콜에 비해 오버헤드와 소비전력이 적고 정확도가 높기[8] 때문에 본 논문에서는 IBS 를 사용한다고 가정한다.

* 교신저자

PbK : Sink Node 의 공개키
PrK : Sink Node 의 개인키
Ki : i 번째 Sensor Node 가 생성한 비밀키
IVi : i 번째 Sensor Node 가 생성한 Initialization Vector
T : 동기화된 현재 시각

제안하는 암호화 과정은 다음과 같다.

1) Sink Node 는 PbK, PrK 를 생성 후 PbK 를 Sensor Node 들에게 전송

2) Sink Node 로부터 PbK 를 받은 i 번째 Sensor Node 는 Ki 와 IVi 을 생성하고, Ki 와 IVi 를 PbK 로 암호화 하여 전송한다.

3) Sink Node 는 i 번째 Sensor Node 로부터 받은 암호문을 PrK 로 복호화 하여 Ki 와 IVi 를 얻는다.

4) Sensor Node 에서는 Ki = Hash(Ki, T+IV)로 키를 갱신하여 데이터를 Ki 로 암호화하여 Sink Node 로 전송한다.

5) Sink Node 에서도 Ki = Hash(Ki, T+IV)를 통하여 키를 갱신하고 Sink Node 로 받은 암호문을 Ki 로 복호화 하여 센서 값을 얻는다.

6) Time Synchronization 을 위한 다음 동기화 시까지 4), 5)를 반복하여 값을 송수신 한다.

7) Time Synchronization 을 위한 다음 동기화 시에는 1)~6)을 반복한다.

시각 동기화 때마다 새로운 키를 생성하기 때문에 시간 영역 별로 다른 공개키를 가진다. 따라서 공개키로 개인키를 알아내더라도 일부시간에 유효한 비밀키만 알 수 있다. 예를 들어, 동기화를 5 분 간격으로 하고 개인키를 알아내는 데 1 년이 걸린다 하였을 때, 1 년으로 계산하여 얻을 수 있는 값이 5 분뿐이고 또 다른 5 분을 계산하기 위해 1 년을 소비해야 한다. 하나의 센서에 대한 하루치 값을 알아내기 위해서 누적 288 년이 소비된다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-R0992-16-1012)

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-H8501-16-1007)

참고문헌

[1] A. Shamir, “ Identity-based cryptosystems and signature schemes,” Advancesin Cryptology, Lecture Notes in Computer Science, Vol. 196, 1984.

[2] S. S. Al-Riyami and K. G. Paterson, “ Certificateless public key cryptography,” International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT ’ 03), Lecture Notes in Computer Science, Vol. 2894, 2003.

[3] D. Boneh and M. Franklin, “Identity-based encryption fromthe weil pairing,” SIAM Journal on Computing, 2003.

[4] S. Ganeriwal, R. Kumar and M. B. Srivastava, “TimingSynch Protocol for Sensor Networks,” ACM Sensys, 2003.

[5] M. Maroti, B. Kusy, G. Simon and A. Ledeczi, “The Flooding Time Synchronization Protocol,” ACM SenSys’04, 2004.

[6] J. Elson, L. Girod and D. Estrin, “Fine-grained Network Time Synchronization Using Reference Broadcasts,” ACM OSDI, 2002.

[7] S. Bae, “Time Synchronization by Tree-based Indirect Broadcasting for Wireless Sensor Networks,” Journal of Korean Institute of Information Scientist and Engineers, 2012.

[8] S. Bae, “A Time Synchronization Protocol for Wireless Body Sensor Networks,” 2016.