애드혹 네트워크에서 안전한 통계정보수집 기법에 관한 연구

조관태*, 이병길*
*한국전자통신연구원 사이버보안연구본부
e-mail:{kwantaecho, bglee}@etri.re.kr

A Study on Secure and Statistical Data Aggregation in Ad Hoc Networks

Kwantae Cho* and Byung-Gil Lee*
*Cyber Security Research Division, Electronics and Telecommunications Research Institute

요 약

애드혹 네트워크(Ad Hoc Network)는 최근 이슈가 되고 있는 사물 간 인터넷(Internet of Things), 스마트그리드(Smart Grid), 사람 중심 도시 센싱(People-Centric Urban Sensing), 해상 통신(Maritime Communications) 환경에서 다양하게 활용되는 네트워크 구조다. 이러한 환경에서의 애플리케이션들은 사용자들에게 다양한 편의성을 제공하기 위하여 사용자의 민감한 프라이버시 정보를 요구하기도 한다. 하지만, 만약 수집되어지는 프라이버시 정보가 인가되지 않은 공격자에게 노출된다면, 사용자는 불안함을 호소할 수 있을 것이고, 동시에 해당 데이터를 수집하고자 했던 서비스제공자는 경제적으로 커다란 손실을 입을 수 있다. 이러한 프라이버시 정보 노출을 방지하기 위하여 안전한 데이터 수집 기법들이 연구되어 왔다. 하지만, 대부분의 기법들은 기밀성만 제공할 뿐, 부인방지 및 익명성은 제공하지 않는다. 그리고 더 나아가 기존 기법들은 통계정보 수집과 개별적인 정보 수집을 동시에 제공하지 않는다. 본 논문은 개별정보수집 및 통계정보 수집을 모두 지원하며 동시에, 사용자에게 강화된 익명성 개념인 비연결성을 제공하는 새로운 데이터 수집 기법을 소개한다.

1. 서론

애드혹 네트워크(Ad hoc Network)는 최근 이슈가 되고 있는 사물 간 인터넷(Internet of Things), 스마트그리드(Smart Grid), 사람 중심 도시 센싱(People-Centric Urban Sensing)을 지원하기 위한 필수적인 서브 네트워크 개념으로, 사용자에게 다양한 서비스를 제공하기 위하여 구축된다. 많은 수의 센싱 장비들이 사용자 주위에 설치되고, 장비들 간 자동화된 통신 기능을 통하여 사용자가 의식하지 못한 상황에서도 공공안전, 환경 감시, 의료 서비스 등을 제공하기 위하여 다양한 프라이버시 정보가 수집된다. 이러한 프라이버시 정보 수집은 사용자에게 보다 나은 서비스를 제공하는데 커다란 기여를 하지만, 반면 악의적인 목적을 지닌 공격자에 의해 사용자의 프라이버시 정보가 노출될 수 있다. 또한 공격자가 자신에게 유리한 상황을 만들기 위한 의도적인 데이터 조작을 통해, 잘못된 통계결과를 도출할 수도 있다.

이러한 공격들로부터 안전하게 데이터를 수집하기 위해, 기존에 여러 기법들이 연구되었지만, 기존 기법들[1-2]은 데이터에 대한 기밀성만 제공할 뿐, 부인 방지 및 비연결성을 제공하지 않는다. 비연결성이란, 하나의 객체로부터 생성된 두 개의 메시지가 주어졌을 때, 두 개의 메시지가 같은 객체로부터 생성된 것인지 판별할 수 없어야 하는 것으로, 익명성에 비하여 한층 강화된 개념이다. 또한 기존 기법들[3-5]은 전체적인 통계정보만 산출 가능할 뿐, 개별적인 정보 수집은 지원하지 않는다. 따라서 본 논문에서는 애드혹 네트워크 환경에서 안전하고 다양한 데이터 수집 서비스를 제공하기 위하여, 기밀성, 비연결성 및 부인방지를 제공하고, 통계정보수집 및 개별정보수집이 가능한 데이터 수집 기법을 제안한다.

2. 제안하는 개별정보 및 통계정보 지원 데이터 수집 기법

2.1 시스템 파라미터 설정

본 절에서 정보수집서버는 제안하는 기법과 관련된 시스템 파라미터들을 설정한다. 정보수집서버는 먼저 세 개의 커다란 소수 $, p_1, p_2$를 선택하고, $n_0 = p_0 \times p_1$, $\phi(n_0) = (p_0 - 1) \times (p_1 - 1)$을 계산한다. 여기서, p_2는 n_0보다 매우 작아야한다. 그리고 두 개의 정수 $e_0, e_1 \in Z^*_{\phi(n)}$를 무작위로 선택한 후, $e_0 \times d_0 \equiv e_1 \times d_1 \equiv 1 \pmod{\phi(n_0)}$을 만족하는 정수 d_0, d_1을 설정한다. 이외에 단방향 충돌 회피 해시 함수인 $H_0 : \{0,1\}^* \rightarrow Z_{n_0}$와 $H_1 : \{0,1\}^* \rightarrow Z_{n_0}$, $(H_0 \neq H_1)$을 생성한다. 정수 $x_0 \in Z_{n_0}$을 무작위로 선택한

후, 공개키인 $\equiv x_0^{-e \times e_1} \pmod{n_0}$을 연산한다. 정보수집 정보의 보장 내용을 포함한 파라미터 $c_0 = {}_0(W, n_0, v_0, e_0, e_1, y_0)$을 생성한다. W는 정보수집서버가 각 노드에게 무엇을 수집하는지, 그리고 무엇을 위임하는지 등에 대한 사항을 정의하고 있다. 결론적으로 정보수집서버의 개인키와 공개키는 각각 (x_0, d_0, d_1), $(n_0, p_3, e_0, e_1, y_0, c_0)$이며, 추가적으로 (W, H_0, H_1)을 공개한다.

정보수집서버는 위에서 설정한 시스템파라미터들을 바탕으로, 각 노드 N_i (i번째 노드)에게 프록시키를 분배한다. 정보수집서버는 먼저 N_i를 위한 정수 γ_i Z_{n_0}을 무작위로 선택한 후, $x_i \equiv H_0(\gamma_i)^{-d_0} \times x_0^{c_0} \pmod{n_0}$을 계산한다. 여기서 γ_i는 N_i를 식별하기 위한 값으로, 유일한 값이다. 정보수집서버는 생성된 프록시키(x_i, γ_i)을 안전한 채널을 통해 N_i에게 전달한다.

2.2 수집된 데이터 암호화

N_i은 정보수집서버로부터 받은 프록시키를 사용하여 원문 메시지 M을 암호화한다. 먼저 정수 $r_1 \in Z_{n_0}$을 무작위로 선택한 후, 정보수집서버로부터 전달받은 프록시키를 이용하여, 원문 메시지 M에 대한 암호메시지를 생성한다. 암호메시지는 정보수집서버가 얻고자하는 통계정보에 따라 연산을 달리한다.

1) 개별정보수집 : 정보수집서버가 제공하는 서비스를 위하여 각 노드마다 개별적으로 데이터를 획득해야 하는 경우로, N_i는 암호메시지 $C_i = M_i \otimes r_1^{-1}$을 생성한다.

2) 덧셈정보수집 : 개별정보수집과 달리, 정보수집서버가 제공하는 서비스를 위하여 전체 원문데이터의 합을 필요로 하는 경우로, N_i는 암호메시지 $C_i = (1 + M_i \times p_3) \times r_1^{-1} \pmod{n_0}$을 계산한다.

3) 곱셈정보수집 : 정보수집서버가 제공하는 서비스를 위하여 전체 원문데이터의 곱을 필요로 하는 경우로, N_i는 암호메시지 $C_i = M_i \times r_1^{-1} \pmod{n_0}$을 계산한다.

2.3 암호메시지에 대한 서명 생성

N_i은 정보수집서버로부터 할당받은 프록시키를 사용하여 서명값을 생성한다. 데이터 암호화 시, 사용한 r_1을 사용하여, $r_2 = H_1(r_1)$을 계산한 후, $b \equiv r_1^{e_1} \pmod{n_0}$, $t \equiv H_0(\gamma_i)^{r_2+1}$, $\theta = H_0(C_i, , n_0, p_3, e_0, e_1, y_0, c_0, b, t)$, $s \equiv r_1 \times H_0(\gamma_i)^{-r_2 \times \theta} \times x_i^{e_0 \times \theta} \pmod{n_0}$을 계산한다. 따라서 C_i에 대한 서명메시지는 $\Omega_i = \{\theta, b, s, t\}$로 정의된다.

2.4 생성된 메시지 전송

N_i는 2.2절과 2.3절에서 생성한 암호 메시지와 서명 메시지 , Ω_i)을 정보수집서버로 전송한다.

2.5 서명메시지 검증

정보수집서버는 다수의 노드들로부터 수많은 서명메시지를 수신하게 된다. 본 논문에서 제안하는 기법은 서명메시지 검증 시, 개별적인 검증이 아닌 일괄검증을 가능하게 함으로써, 검증소요시간을 효과적으로 줄였다.

정보수집서버가 n개의 서명 메시지 $(\theta_i, b_i, s_i, t_i) \in \Omega_i, (1 \le i \le n)$을 받았을 때, 먼저 모든 암호메시지 C_i에 대해 $\theta_i = H_0(C_i, n_0, p_3 e_0, e_1, y_0, c_0, b_i, t_i)$가 성립하는지 확인한다. 만약 성립한다면, $\prod_{i=1}^{n} b_i \equiv ((\prod_{i=1}^{n} s_i) \times (\prod_{i=1}^{n} t_i^{\theta_i}))^{e_1} \times (y_0^{c_0})^{\sum_{i=1}^{n} \theta_i} \pmod{n_0}$가 성립하는지 확인한다. 성립한다면 n개의 모든 서명메시지는 정당한 프록시키에 의해 생성된 서명메시지다. 만약 등식이 성립하지 않는다면, n개의 메시지 중 1개 이상의 서명메시지가 위조 또는 변조되었다는 의미이므로, 각각의 서명메시지에 대하여 위변조 여부를 검사한다.

2.6 암호메시지에 대한 복호화

정보수집서버는 서명메시지 검증 후, 원문메시지에 대한 통계정보 획득을 위해 메시지를 복호화 한다. 메시지 복호화 유형은 2.2절에서 정의된 수집 유형에 따라 세 가지로 분류된다.

1) 개별정보수집 : 정보수집서버는 자신의 개인키를 이용하여 각각 암호메시지에 대한 원문메시지 $M_i = C_i \otimes b^{d_1}$을 획득한다.

2) 덧셈정보수집 : 정보수집서버는 자신의 개인키를 이용하여 n개의 암호메시지 $C_i (1 \le i \le n)$에 대해 $C = \prod_{i=1}^{n} (C_i \times b_i^{d_1}) = \prod_{i=1}^{n} (1 + M_i \times p_3) \equiv 1 + p_3 \times \sum_{i=1}^{n} M_i \pmod{p_3^2}$을 계산한 후, 모든 원문메시지에 대한 합 $SUM(M_i) = \sum_{i=1}^{n} M_i \equiv (C-1)/p_3$을 연산한다. 만약 평균값을 얻길 원한다면, $AVG(M_i) = (\sum_{i=1}^{n} M_i)/n \equiv (C-1)/(p_3 \times n)$을 통해 간단히 계산할 수 있다.

3) 곱셈정보수집 : 정보수집서버는 자신의 개인키를 이용하여 n개의 암호메시지 $C_i (1 \le i \le n)$에 대해 $\prod_{i=1}^{n} M_i = \prod_{i=1}^{n} (C_i \times b_i^{d_1}) \pmod{n_0}$을 계산하면, 모든 원문메시지에 대한 곱을 구할 수 있다.

2.7 악의적인 목적을 지닌 노드 식별

정보수집서버는 복호화된 원문메시지가 악의적인 목적을 지닌 원문메시지를 포함하였을 경우, 원문메시지를 생성한 노드 ′을 식별할 수 있어야 한다. 노드 식별은 서명메시지 ′ (θ', b', s', t')을 이용하여 이루어진다. 정보수집서버는 자신의 개인키를 이용하여 $r' \equiv b'^{d} \pmod{n_0}$을 도출한 후, $r_2' \equiv H_1(r_1')$을 계산하고, 자신이 생성한 $\forall \gamma$에 대하여 $t' = H_0(\gamma_j)^{r_2'+1}$을 만족하는 γ_j을 검색한다. 만족하는 γ_j를 지닌 노드는 폐기 방송을 한다.

3. 결론

본 논문에서는 기반 구조가 없는 해상에서의 선박 간 통신, 사물 간 인터넷 환경 등 다양한 애드혹 네트워크 환경에서 기밀성, 비연결성, 부인방지를 제공하는 안전한 통계정보수집 기법에 대하여 소개하였다. 또한 제안한 기법은 개별적인 데이터 수집뿐만 아니라, 준동형 암호 성질을 이용한 덧셈과 곱셈에 대한 통계정보 수집 기법을 제안하였다.

4.Acknowledgement

본 연구는 해양수산부/한국해양과학기술진흥원 해양안전 및 해양교통시설기술개발사업 연구비지원(ETRI 수행과제번호 20090403)에 의해 수행 되었습니다.

참고문헌

[1 R. Zhang, J. Shi, Y.Zhang, and C. Zhang, “Verifiable Privacy-preserving Aggregation in People-Centric Urban Sensing Systems,” IEEE Trans. Selected Areas in Communications/Supplement, Vol. 31, No. 9, 2013, pp. 268-278.

[2] . Sung, "Confidential aggregation for wireless transmissions," Information Networking (ICOIN), 2014 International Conference on, 2014, pp. 390-394.

[3] V. Kumar and S. Madria, "PIP: Privacy and Integrity Preserving Data Aggregation in Wireless Sensor Networks," Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on, 2013, pp. 10-19.

[4] . Li, G. Cao, and F. La Porta, "Efficient and Privacy-Aware Data Aggregation in Mobile Sensing," IEEE Trans. Dependable and Secure Computing, Vol.11, No. 2, 2014, pp. 115-129.

[5] T Jung, XF Mao, XY Li, SJ Tang, W Gong, L Zhang, “Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation,” INFOCOM, 2013, pp. 2634-2642.