스마트그리드에서의 효율적인 멀티캐스트 인증 기법1)

유지민*, 김지현**, 김호원**
*부산대학교 물류IT협동과정
**부산대학교 컴퓨터공학과
e-mail : jmyu@pusan.ac.kr

Effcient Multicast Authentication Scheme for Smart Grid

Ji-Min Yu*, Ji-Hyun Kim**, Ho-Won Kim**
*Dept of Logistics Information Technology, Pusan National University
**Dept of Computer Engineering, Pusan National University

요 약

오늘날 기존의 전력망에 IT가 융합되어 전력 공급자와 송배전 컨트롤러 사이에 정보 교환이 가능한 스마트그리드가 부각되고 있다. 스마트그리드 환경은 전력 공급자와 송배전 컨트롤러 사이의 정보 교환의 빈도가 높고, 정보 교환이 실시간으로 이루어 져야하는 특성을 가진다.

이러한 정보 교환이 주어진 시간 내에 정확하게 이루어지지 않거나 정보 교환 중에 공격자로 인해 악의적 변경이 일어나는 경우 대규모 정전이나 전력의 공급에 막대한 영향을 미치게 된다. 따라서 송신자 인증과 정보 교환 중에 정보의 악의적 변경이 이루어지지 않았다는 정보의 무결성 인증이 이루어 져야 하며, 이를 임계시간 이내에 처리할 수 있는 인증 프로토콜이 요구된다.

본 논문에서는 이러한 요구조건을 만족시키기 위해 타임-크리티컬(time-critical)한 특성을 가지면서 메세지 인증 기능을 제공하는 TV-HORS 멀티캐스트 인증 기법을 스마트그리드 시나리오에 적용하고, 이에 따른 문제점을 제시한 후, 이에 대한 해결책을 제시한다. 제안하는 방법은 키입력(keyed) 해쉬 함수를 이용해 기존 TV-HORS 기법이 가지는 키 저장 문제를 효율적으로 해결한다.

1. 서론

스마트그리드는 기존의 전력망에 IT 기술을 접목시켜 전력 공급자와 송배전 컨트롤러가 양방향으로 정보를 교환하여 기존 전력망에 비해 보다 효율적으로 전력의 공급이 이루어지는 형태이다. 전력 공급자와 송배전 컨트롤러의 정보 교환이 실시간적으로 이뤄지고 교환되어지는 정보를 가로채 정보를 변경하여 정당한 송신자가 보내는 것처럼 공격하는 등의 공격 위험 또한 발생될 수 있다. 따라서 안전한 정보 교환이 이루어 질수 있도록 정보 교환에 있어서의 메시지 인증이 필요로 하게 된다. [3],[4],[5]

TV-HORS(Time Valid Hash to Obtain Random Subsets) 멀티캐스트 인증 기법[1]은 TESLA[2]와는 달리 서명 검증에 있어 버퍼링이 없고 타임-크리티컬한 특징을 가지면서 스마트그리드 환경에서 이뤄지는 메시지의 서명과 검증에 사용하기 적절한 멀티캐스트 인증 기법이다.

본 논문에서는 스마트그리드 환경에 TV-HORS 멀티캐스트 인증 기법을 현실적으로 적용하고 그에 따른 문제점과 해결 방안에 대해 논의해 보겠다.

1) 이 논문 또는 저서는 2010년 교육과학기술부로부터 지원받아 수행된 연구임 (지역거점연구단육성사업/차세대물류IT기술연구사업단)

2 TV-HORS 멀티캐스트 인증 기법

Qiyan Wang이 제안한 TV-HORS(Time Valid Hash to

<표 1> Notation Table

T	전송 세션의 기간
E	각 $epoch$의 기간
P	$epoch$의 총 개수
$\{K_j\}_{0 \le j \le P}$	$epoch$ j의 heavy 체인 요소들
$\{S_{(u,i)}\}$ $0 \le u \le N, 0 \le i \le$	$epoch$ j의 light 체인 요소들
$S_{(-,j)}$	$epoch$ j에서의 light 체인 전체
t_j^R	$epoch$ j에서의 서명 시작 시간
H	일방향 해쉬 함수
M_a	a번째 메시지, a는 메시지 인덱스
m_a	송신자가 a 번째 메시지 서명에 사용할 substring 만들기 위해 계산 하는 값
m_a'	수신자가 a 번째 메시지 서명에 사용할 substring 만들기 위해 계산 하는 값
t	m_a를 $\log_2 N$bit로 나눴을 때 나오는 substring 개수
t^R	수신자가 패킷을 수신한 시간
T_{Adv}	공격자(Adv)가 송신자가 보낸 서명을 찾아 낼 수 있는 시간

Obtain Random Subsets) 멀티캐스트 인증 기법[1]은 Time Valid One-Time Signature (TV-OTS)[2],[8]를 기반으로 한 효과적인 멀티캐스트 인증 기법으로 해쉬 체인을 이용하여 인증에 사용할 키를 생성한다.

전송 세션을 epoch 단위로 나누고 각 epoch 마다 epoch에 해당하는 해쉬 체인 요소를 사용하여 송신자가 패킷을 서명할 수 있도록 한다.

1) 초기화

전송 세션을 epoch 간격으로 나눈다. epoch의 총 개수는 $P=\frac{E}{P}$가 된다. 랜덤한 Seed K_p를 선택하고 $P+1$ 길이의 $\{K_j\}_{0 \le j \le P}$ Heavy 체인을 생성한다.

< Heavy 체인 생성 : $K_{j-1}=H(K_j), 0 \le j \le P$ >i)

Heavy 체인 생성 후 랜덤한 seed S_p를 선택하고 light 체인을 생성한다. $(1 \le i \le N, 0 \le j \le P)$

< Light 체인 생성 :

$$S_{(i,j)}=h_{k_j}(S_{(i,j+1)})=H_w(S_{(i,j+1)}||K_j) \quad >\text{ ii)}$$

각 epoch j에서는 K_j와 $S_{(-,j)}$가 활성화되고 시간이 지나 epoch j가 만료되면 $j+1$의 해쉬 체인이 활성화 된다.

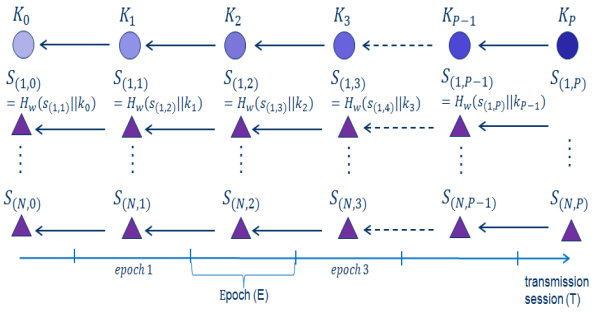
송신자는 수신자에게 초기화 정보를 전달한다.

$$\text{송신자}\rightarrow\text{수신자}: \langle K_0, \{S_{(u,0)}\}_{0 \le u \le N}, E, t_0^s, P \rangle \quad (1)$$

2) 메시지 서명

초기화 단계가 끝나면 송신자는 수신자에게 보낼 메시지 M_a를 서명하게 된다.

송신자가 수신자에게 메시지를 보낼 때 활성화되어 있는 epoch이 epoch c 라면 서명에는 c번째 heavy 체인인 K_c와 K_c의 light 체인 $S_{(-,c)}$의 요소가 사용되어진다.



(그림 1) TV-HORS의 해쉬 체인 생성과 epoch

① m_a를 계산한다.

$$m_a=H_l(a||M_a||K_c)$$

② 계산한 결과값 m_a를 t개의 $\log_2 N$ bit 크기의 substring으로 나눈다.

③ substring $\{b_1,\ldots,b_t\}$ b_u를 정수 i_u로 변환한다. 정수 i_u를 $S_{(-,c)}$의 요소를 선택하는 인덱스 $S_{(i_u,j)}$로 사용한다.

④ substring $\{b_1,\ldots,b_t\}$에 해당되는 light 체인의 요소를 선택하고 메시지 M_a와 함께 M_a에 대한 서명 $\{S_{(i_u,c)}\}_{1 \le u \le t}$과 관련 정보를 전달한다.

$$\text{송신자}\rightarrow\text{수신자}: \langle a, M_a, c, K_c, \{S_{(i_u,c)}\}_{1 \le u \le t} \rangle \quad (2)$$

3) 메시지 M_a 검증

① 수신자는 송신자가 보낸 메시지M_a와 서명정보가 담긴 $\langle a, M_a, c, K_c, \{S_{(i_u,c)}\}_{1 \le u \le t} \rangle$ 패킷을 받으면 패킷을 수신한 시간 t^R을 확인하고, 공격자(Adv)가 송신자가 보낸 서명을 찾아 낼 수 있는 시간T_{Adv} 안에 도착했는지 검사한다. T_{Adv}이후 도착한 패킷은 폐기한다.

② 이전에 받은 초기화 정보가 담긴 패킷을 통해 수신자는 이미 검증에 사용할 해쉬 체인을 준비해두기 때문에 바로 검증에 들어간다.

③ $m_a^{'}$를 계산한다.

$$m_a^{'}=H_l(a||M_a||K_c)$$

④ substring $\{b_1^{'},\ldots,b_t^{'}\}$ $b_u^{'}$를 정수 $i_u^{'}$로 변환한다.

⑤ substring $\{b_1^{'},\ldots,b_t^{'}\}$에 해당되는 light 체인의 요소를 선택한다. 이것을 송신자가 보낸 서명$\{S_{(i_u,c)}\}_{1 \le u \le t}$과 같은 결과가 나오는지 확인한다.

4) 새로운 수신자의 초기화

새로운 수신자는 송신자와의 통신에 있어서 메시지 서명의 검증을 위해 필요한 해쉬 체인을 생성하기 위해 초기화 정보를 아래와 같이 전달 받는다.

i는 최근에 사용한 epoch의 인덱스, t_i^s는 최근 사용 epoch의 서명 시작 시간이다.

$$\text{송신자}\rightarrow\text{수신자}: \langle i, K_i, \{S_{(i,0)}\}_{0 \le u \le N}, E, t_i^s, P-j \rangle \quad (3)$$

3. 스마트그리드에 TV-HORS 멀티캐스트 인증 기법 적용했을 때의 문제점

<시나리오> A발전소는 (가)지역의 전력공급을 담당하고, B 발전소는 (나)지역의 전력공급을 담당하는데 B 발전소에서 (나) 지역에 전력을 공급할 수 없는 문제가 발생하였다. B 발전소는 A 발전소로 (나)지역으로의 전력 공급 요청의 메시지를 전송하고 A 발전소는 신속히 그 메시지가 정당한 메시지인지 판단하고 (나) 지역으로 전력을 공급해 줘야한다. 그리고 A, B 발전소 사이에는 메시지가 거쳐 가게 되는 많은 스위칭

소자가 존재하며 기존 전력망에서의 스위칭 소자는 부가적인 메모리가 필요 없었지만 스마트그리드에서의 스위칭 소자는 전력 스위칭 관련 메시지를 검증하기 위한 메모리를 가지고 있다.

B 발전소에서는 자신이 보내는 메시지의 무결성을 위해 메시지의 서명을 담아 전달하고 A 발전소에서는 그 서명을 검증하여 메시지의 정당성을 판단하는데 이 서명과 검증에 사용하는 키를 TV-HORS 멀티캐스트 인증 기법에서는 $epoch$의 변화에 따라 다른 해쉬 체인의 요소를 사용하여 서명하기 때문에 공격자가 서명에 사용한 키를 알아내기가 힘들다.

TV-HORS 멀티캐스트 인증 기법에서는 송신자와 수신자의 전송 세션에서 사용할 해쉬 체인을 메시지를 주고받기 전에 미리 형성하고 저장하여 전송 세션이 끝날 때까지 $epoch$의 변화에 따라 다른 해쉬 체인의 요소를 사용한다.

해쉬 체인을 형성할 때 seed K_P를 해쉬해서 다음 요소 K_{P-1}를 생성하고 또 그것을 해쉬하는 형식으로 해쉬 체인이 형성되기 때문에 seed값 K_P, S_P가 공격자에게 노출되면 공격자도 해쉬 체인을 만들 수 있다.

그러므로 해쉬 체인 전체를 미리 생성하고 사용 할 때는 seed값 K_P, S_P가 아닌 마지막에 생성된 K_0, $S_{(-,0)}$부터 사용한다. 그러므로 전송 세션이 끝날 때까지 계속 해쉬 체인을 유지하고 있어야하므로 키의 저장비용(storage cost)이 매우 높다.

위에서 가정한 시나리오에 TV-HORS 멀티캐스트 인증 기법을 이용하여 B 발전소에서 A 발전소로 보내는 전력 요청 메시지를 서명하고 검증한다면 A, B 발전소 사이에 존재하는 수많은 스위칭 소자는 전력 요청 메시지를 검증하기 위해 A, B 발전소의 전송 세션이 끝날 때 까지 해쉬 체인을 저장하고 있어야한다.

TV-HORS 멀티캐스트 인증 기법을 그대로 적용했을 때의 해쉬 체인의 키 사이즈는 <표2>와 같다. 메시지를 주고받는 A, B 발전소와 스위칭 소자는 대략 2.7GB의 해쉬 체인을 저장하고 있어야한다. 이러한 사이즈의 키를 수많은 스위칭 소자가 가지고 있는 것은 비현실적이고 효율적이지 못하다.

그러므로 본 논문에서는 스마트그리드에 적합한 TV-HORS의 장점을 유지하면서 비현실적인 키 사이즈를 줄일 수 있는 방안을 제시한다.

4. 해쉬 체인의 키 사이즈를 줄이기 위한 제안 아이디어

TV-HORS 멀티캐스트 인증 기법은 해쉬 체인의 seed값을 공격자에게 들키면 해쉬 체인 전체를 공격자가 만들어

<표 2> 시나리오에 TV-HORS 멀티캐스트 인증 기법 적용 시 해쉬 체인의 키 사이즈

T(전송 세션)	1hour(A발전소, B발전소 사이의 전송 세션 기간을 1 시간이라 가정)
E(epoch)	10_{ms}
P	3600000(전송 세션(T)을epoch(E)만큼의 크기로 나눈 개수←이 개수만큼의 키를 미리 만들어 놔야 한다.)
Heavy 체인요소 하나당 사이즈	80 bit
Light 체인요소 하나당 사이즈	40bit
N (light 체인 요소 개수)	1358
전체 Heavy 체인 사이즈	10 byte * 360001 = 3515.6KB
Heavy 체인 하나당 light 체인 사이즈	6 byte * 1358 = 8.0KB
전체 Light 체인 사이즈	8.0 KB * 36001 = 2.7GB

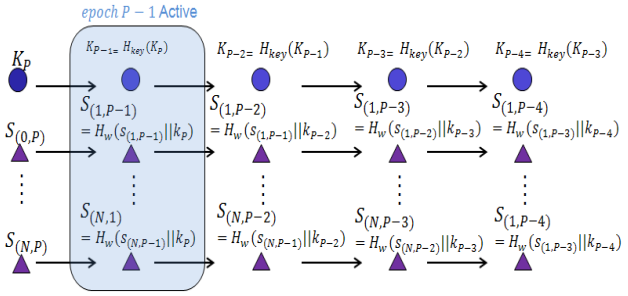
낼 수 있기 때문에 해쉬 체인의 마지막 해쉬 체인 (K_0, $S_{(-,0)}$)부터 사용하므로 저장비용이 높아 현실적이지 못했다. 본 논문에서는 해쉬 체인의 형성에 있어서 키입력 해쉬를 사용하여 전송 세션에서 사용할 모든 해쉬 체인을 미리 만들어 놓고 계속 유지할 필요 없이 epoch의 변화에 따라 계속 업데이트 하도록 제안한다. 키입력 해쉬에 사용되어지는 키는 송신자, 수신자 사이에서 미리 공유되어진 비밀키라고 가정한다.

(그림 2) 과 (그림 3)은 해쉬 체인을 5개 단위로 유지한다고 가정했을 때의 해쉬 체인 형성 과정이다. $P-1$번째 $epoch$에서는 $K_{P-1}, S_{(-,P-1)}$을 사용하여 서명한다. $P-1$번째 $epoch$이 만료되고 $P-2$번째 $epoch$이 활성화될 때는 (그림 3) 같이 만료된 $epoch$의 해쉬 체인은 삭제되고 다음에 사용되어질 $epoch$의 해쉬 체인들이 새로 생성된다.

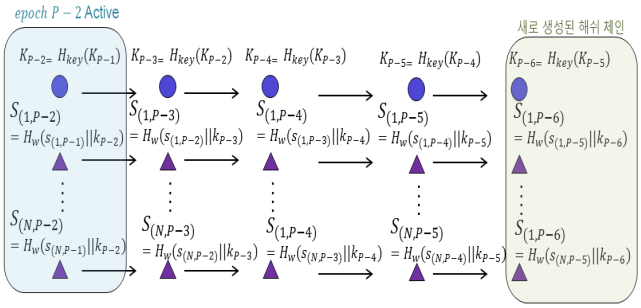
키입력 해쉬를 사용할 경우 기존 TV-HORS 멀티캐스트 인증 기법처럼 P개의 heavy 체인과 N*P개의 light 체인을 다 가지고 있지 않아도 되고, 이미 사용한 해쉬 체인 요소는 삭제하고 다음 epoch에 사용할 해쉬 체인 요소를 계속 만들어 가면서 사용할 수 있다.

기존 TV-HORS 멀티캐스트 인증 기법의 해쉬 체인 형성은 seed값을 알게 되면 누구나 서명에 사용할 해쉬 체인을 만들어 낼 수 있지만 제안 아이디어는 키입력 해쉬

를 사용하기 때문에 seed값을 알아내더라도 송신자와 수신자가 공유하고 있는 비밀키를 알지 못하면 해쉬 체인을 형성할 수 없다. TV-HORS 멀티캐스트 인증 기법의 해쉬 체인 키 사이즈와 비교하여 급격히 줄어드는 것을 <표3>에서 볼 수 있다.



(그림 2) 초기 해쉬 체인 형성



(그림 3) 만료된 epoch의 해쉬 체인 삭제 후 해쉬 체인 업데이트

<표 3> 제안 아이디어 적용 시 해쉬 체인의 키 사이즈

T(전송 세션)	1 hour (A발전소, B발전소 사이의 전송 세션 기간을 1 시간이라 가정)
E($epoch$)	10_{ms}
P	5 (해쉬 체인을 5개 단위로 계속 유지한다)
Heavy 체인 요소 하나당 사이즈	80 bit
Light 체인 요소 하나당 사이즈	40 bit
N (light 체인 요소 개수)	1358
전체 Heavy 체인 사이즈	10 byte * 5 = 50 byte
Heavy 체인 하나당 light 체인 사이즈	6 byte * 1358 = 8.0 KB
전체 Light 체인 사이즈	8.0 KB * 5 = 40 KB

5. 결론

본 논문에서는 TV-HORS 기법을 스마트그리드 송배전 환경에 적용했을 때 메시지의 무결성을 위해 서명과 검증 수행할 때 사용하는 해쉬 체인의 키 사이즈가 비현실적으로 크다는 문제점에 대해 지적하고 키입력 해쉬를 사용함으로써 키 사이즈를 줄임으로써 키 사이즈 문제를 해결하는 방법을 제시했다.

제안하는 아이디어는 타임-크리티컬한 특성과 메시지의 서명과 검증에 있어서 버퍼링이 없는 장점은 그대로 유지하면서 서명과 검증에 사용되는 키 사이즈는 줄어들기 때문에 대량의 키 사이즈를 유지하는 것이 비효율적인 스마트그리드 송·배전 환경에 적합할 것으로 기대된다

참고문헌

[1] Q.Wang, H. Khurana, Y. Huang, and K. Nahrstedt. 'Time Valid One-Time Signature for Time-Critical Multicast Data Authentication' INFOCOM''09. IEEE 2009 Conference on Computer Communications, 2009

[2] A. Perrig and R. Canetti and D. Song, and J. D. Tygar 'Efficient and secure source authentication for multicast' NDSS''01. 2001

[3] 문승일 '스마트그리드 개념' 한국통신학회지(정보와통신) 제27권 제4호, 2010.

[4] 이건희, 서정택, 이철원 '스마트그리드와 사이버 보안' 한국통신학회지 (정보와통신) 제27권 제4호, 2010.

[5] 박성찬, 최홍석, 최태섭 '스마트그리드 하에서의 보안 이슈 및 대응 방안' 2009 대한전기학회 전력기술부문회 추계학술대회 논문집, 2009.

[6] L. Lamport 'Constructing digital signatures from one-way function' Technical Report SRI-CSL-98, SRI International Computer Lab. 1979.

[7] A. Perrig 'The BiBa one-time signature and broadcast authentication protocol' CCS''01. Nov. 2001

[8] L. Reyzin and N. Reyzin, Better than BiBa: short one-time signatures with fast signing and verifying' ACISP''02. Information Security and Privacy

[9] W. D. Neumann 'HORSE: an extension of an r-time signature scheme with fast signing and verification' ITCC''04. 2004

[10] Y. Zhou and Y. Fang, Multicast authentication over lossy channels, MILCOM''07, 2007.

[11] 정유미, 박정민, 채기준 '효율적인 멀티캐스트 서비스를 위한 인증 기법' 한국정보처리학회논문지 Volume 11C. Issue 6, pp. 765 ~ 772 , 2004