소규모 DNP3 실험 환경에서 각종 공격과 대응방안

이동수* 김광조*

*한국과학기술원 전산학과

Simulated Attack on Small-scale DNP3 Protocol Testbed and its Countermeasure

Dongsoo Lee* Kwangjo Kim*

*Department of Computer Science, KAIST.

요 약

SCADA(Supervisory Control and Data Acquisition)는 주로 기간산업 시설을 관리하고 제어하는 시스템이다. 관리하는 대상의 특성 상 시스템이 공격 받을 경우 매우 심각한 사태가 야기될 수 있어, SCADA 시스템의 취약점 분석은 필수적이라 할 수 있다. DNP3는 북미지역에서 가장 많이 사용하는 공개 SCADA 프로토콜이지만 초기 단계의 DNP3는 외부부터 공격을 가정하지 않아 인증, 암호화 등의 과정이 없어 공격에 매우 취약하며, 이를 보완하기 위한 DNP3 SA(Secure Authentication) 또한 암호화 없이 인증만 제공하고 있는 상황이다. 이 논문에서는, 기본 DNP3 프로토콜을 사용하는 소규모 테스트베드에서 다양한 공격이 이뤄질 수 있음을 보이고, 이에 대한 보완책으로 암호화와 인증을 동시에 수행하는 DNP3 AE(DNP3 Authenticated Encryption)을 제안하며, PRINCE와 GCM을 이용하여 구현해 대응책을 마련한다.

I. 서론

SCADA는 ICS(Industrial Control System, 산업 제어 시스템)의 한 종류로써 발전소, 수도 공급, 철도 시스템 등과 같은 기간 시설을 관리하고 제어하는 시스템이다. 기간 시설에 대한 사이버 공격은 점점 더 많이 일어나고 있으며, 공격에 성공할 경우 사회에 돌이킬 수 없는 피해를 일으킬 수 있다. 과거에 ICS는 고립된 네트워크에서 운영되는 것으로 가정하고 외부망과 분리하는 것으로 보안 수준을 유지할 수 있었으나, 스마트 그리드 등과 같은 새로운 기술의 등장과 함께 폐쇄망을 유지할 수 없기 때문에 보안 문제가 발생할 소지가 있다.

DNP3 (Distributed Network Protocol)[1]은 북미에서 가장 널리 쓰이는 공개 SCADA 네트워크 프로토콜이다. DNP3는 SCADA 프로토콜 중 비교적 최근에 만들어졌으며, DNP3 Modbus과 같은 기존의 프로토콜에 비해 DNP3는 효율적이면서도 적은 네트워크 대역폭과 적은 프로세싱 자원으로도 운용을 가능케 하였는데, 이는 DNP3를 물리 레이어, 데이터 링크 레이어, 애플리케이션 레이어의 3가지 레이어로 나누고, 애플리케이션 레이어에서 트랜스포트 함수의 형태로 트랜스포트 레이어를 대신하여 처리하기 때문이다. 그러나 DNP3는 폐쇄망에서 운영되는 것을 가정하여 만들어졌기 때문에 별도의 보안체계를 갖추고 있지 않다. 논문[2]에서는 소규모 DNP3 테스트베드를 구성하였고, 논문[3]에서 어떻게 DNP3 프로토콜의 공격 가능성을 검사 하였으며, 본 논문에서는 이 공격 방식에 대한 대응방안으로 어떤 방법을 통해 DNP3 프로토콜을 보완할 수 있는지 보이고자 한다. 그리고 다른 DNP3 보안 프로토콜인 DNP3Sec과 DNP3 SA(Secured Authentication)과 비교하고자 한다.

* (letrhee, kkj)@kaist.ac.kr

* 본 연구는 미래부가 지원한 2014년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음

II. 관련 연구

2.1 DNP3 프로토콜의 취약점

East 등[4]은 이미 DNP3의 데이터 링크 레이어, 의사 트랜스포트 레이어, 애플리케이션 레이어에서 취약점이 존재함을 밝힌 바 있다. Jin 등[5]은 비동기 방식으로 동작하는 Unsolicited Message를 대량으로 보내어 이벤트 버퍼를 넘치게 만드는 형식의 공격을 시도한 바 있다.

2.2 DNP3 보안 강화 프로토콜

DNPSec[6]은 DNP3의 보안 프레임워크 용도로 제안되었다. DNPSec은 기밀성과 무결성을 제공하고, 추가로 인증을 지원한다. 암호화와 인증을 위해 DNPSec은 데이터 링크 레이어의 프레임 구조를 바꾸는 방식을 이용하며, 인증 후 암호화하는 방식을 사용한다. 암호화와 인증용으로 3-DES와 HMAC-SHA-1을 사용하고 있으나 3-DES와 SHA-1 모두 취약점이 드러난 알고리즘이라는 단점이 있다.

DNP3 Secure Authetication(DNP3 SA)[7]는 DNP3의 공식 보안 강화판이다. DNP3 SA는 애플리케이션 레이어의 객체 데이터를 확장하여 운영되며, HMAC을 이용한 Challenge-Response 구조뿐만 아니라 Asymmetric, Symmetric 키 관리 시스템을 지원한다. DNP3 SA는 한 기기에 접속한 여러 사용자에게 완벽한 전방 보안을 제공하며, 가로채기, 변조, 반복 공격을 방어할 수 있으나, 암호화는 제공하지 않는다.

2.3 Authenticated Encryption

Authenticated Encryption(AE)는 기밀성, 무결성 그리고 인증을 효율적으로 수행할 수 있는 암호화 모드이며, 그 유용성으로 NIST에서 표준 AE 알고리즘을 정하고자 2014년에 제출을 마쳐 2017년까지 표준화 결정을 목표로 하는 CAESAR Competition[8]을 진행 중이다.

GCM(Galois / Counter Mode)[9]은 암호화로 카운터 모드를 사용하며, 갈루아 필드 해시를 인증으로 이용하는 모드로, 하드웨어로도 적은 비용으로 구현 가능하다. 특히 GCM은 CAESAR Competition에서 다른 후보의 주요 비교 대상[10]이기도 하다.

III. DNP3 취약점 분석과 공격 시연

3.1 DNP3와 DNP3 SA의 취약점

DNP3는 앞서 설명한 바와 같이 보안 요소를 가지고 있지 않다. DNP3 SA가 DNP3에 무결성과 인증을 제공해주지만, 암호화를 하지 않으므로 비밀성을 보장하지 않는다. 이는 IEC와 DNP 유저 그룹에서 “위변조만 방지할 수 있다면 암호화가 필요없다”[11]는 의견에 따른 것이다. 그러나 Stuxnet과 그 후속 APT 공격들을 고려할 때, 위변조가 불가능하다 하더라도 시스템에서 중요한 요소를 엿볼 수 있는 것은 다른 공격의 실마리가 될 수 있다.

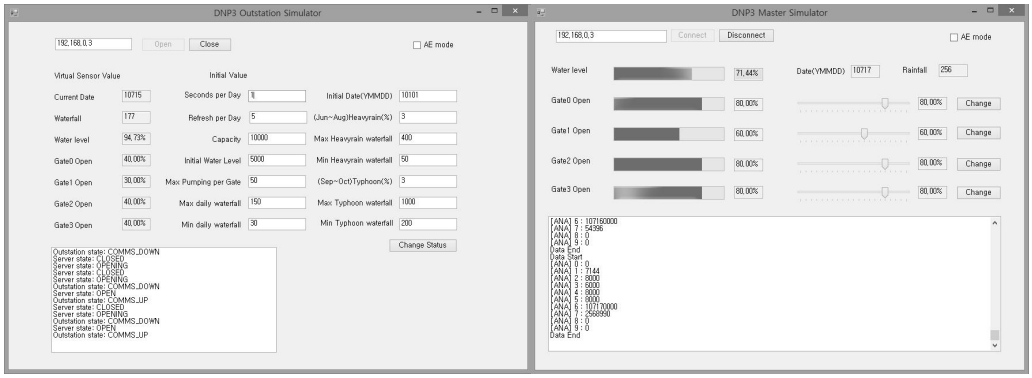
3.2 시연 모델

[그림 1] 소규모 SCADA 테스트베드

논문 [2]에서 OpenDNP3 Library[12]를 이용하여 수력 발전소를 모델로 하는 소규모 SCADA 테스트베드를 구축한 바 있다. [그림 1]에서 볼 수 있듯 테스트베드 요소로써 마스터, 아웃스테이션, 공격자의 세 기기가 있으며, 아웃스테이션은 마스터로 수위, 수문 정보 등을 보내며, 마스터는 아웃스테이션으로 액츄에이터에 명령을 내리도록 하는 간단한 구조이며, 공격자는 네트워크에 침입하여 각종 공격을 수행한다. 이 테스트베드에서는 센서 등을 물리적인 장비 대신 가상의 데이터로써 처리하며, 날짜에 따라 강우량이 무작위로 변하고, 이에 따라 수문의 정도를 적절히 조절하는 것을 목표로 한다.

3.3 공격 시나리오

DNP3 프로토콜 공격에 앞서, 공격자가 다양한 방법을 통하여 SCADA 네트워크 내부로 침



[그림 2] DNP3 시뮬레이터에서 데이터 변조 공격

투하는데 성공하였다고 가정하였고, 공격자는 패킷 스니핑과 패킷 변조를 통해 공격을 시도할 것이다.

패킷 스니핑으로써 공격자는 Ettercap[13]을 이용하여 ARP Poisoning을 시도하고, 가로챈 패킷을 Wireshark로 분석할 것이다.

패킷 변조를 위하여 직접 공격 프로그램을 작성하였다. Ettercap을 통하여 패킷을 가로채면, 프로그램은 TCP/IP 프로토콜 패킷과 DNP3 패킷 구조를 모두 분해하고, 원하는 DNP3 Object 값을 변경한 다음, 원래 구조에 맞도록 재 조립하여 원래 목적지로 보내는 구조이다. 또한 양 방향 모두 패킷을 변조하여, DNP3 마스터 측에서 값이 변조된 것을 확인할 수 없도록 하는 것 또한 특징이다.

3.4 공격 결과

패킷 스니핑의 경우 Wireshark를 통해 전송되는 DNP3 Object의 값이 무엇인지 쉽게 알아낼 수 있었다.

패킷 변조의 경우 공격 툴은 Master가 실제로 지시한 수문 개방 정도에 비해 절반만 열도록 값을 변조하였고, Slave의 응답은 반대로 두 배로 변조하여, [그림 2]와 같이 정상적인 값으로 보이게 하였다. 그 결과, 시뮬레이터 상에서는 장마철 기간 수위가 계속 차올라 결국 최대 수위를 초과하여 치명적인 피해를 입힐 수 있음을 알 수 있다.

DNP3 SA의 경우에는 변조가 불가능하도록 설계가 되어있으나, 패킷 스니핑 공격은 여전히 가능하다.

IV. 보안 개선

이상의 공격을 통하여, 인증 및 암호화가 이루어지지 않은 DNP3 프로토콜은 쉽게 공격 당할 수 있음을 알 수 있으며, 그에 따른 보완책으로 새롭게 DNP3 AE를 제시한다.

4.1 Authenticated Encryption

SCADA 시스템을 구성하는 RTU(Remote Terminal Units)는 매우 낮은 성능을 가지고 있기 때문에, 하드웨어로 구현이 가능한 암호 또한 사용할 수 있도록 고려하였다. 그 결과로 경량 암호화 알고리즘인 PRINCE[14]와 AE로써 GCM을 사용하여 구현하였다. GCM은 AE의 표준이 정해지지 않은 현 시점에서 가장 뛰어난 성능을 보여주고 있으며[15], PRINCE 역시 하드웨어에 구현할 경우 적은 칩 공간과 적은 전력 소모 둘 모두를 얻을 수 있는 장점이 있으나, 하드웨어 장비가 없어 소프트웨어 구현을 통해 테스트를 하였다.

GCM과 PRINCE는 Windows 7 64bit 버전에서 Visual Studio 2012를 통해 구현하였고, 라이브러리로써 GSL 1.16(GNU Scientific Library)를 이용하였다.

4.2 구현

실제 DNP3 AE 구현에 앞서 키 분배는 하드웨어 내장 등으로 사전에 이루어졌다고 가정하였다. DNP3 AE는 DNP3에서 Application Layer 전체를 암호화하며, 새로운 DNP3 Application Layer Header를 사용한다.

이 헤더는 Function Code로 0x30, 0x90을 사용하여 AE가 적용되었음을 알리며, 이번 구

현에 적용한 PRINCE 뿐만 아니라 다양한 암호화 알고리즘을 사용할 수 있도록 하는 등, 작동 환경을 쉽게 구성할 수 있도록 하였다. 새로운 헤더와 GCM에 필요한 인증 태그, 카운터 값으로 인해 기존 DNP3에 비해 24바이트를 추가로 사용한다.

4.3 평가

위 3.3과 3.4에서 언급했던 것과 같은 공격을 DNP3 AE에서 동일하게 시도해 보았다. Ettercap과 Wireshark를 통하여 패킷을 가로채고 패킷의 내용을 볼 수 있으나, 암호화되어 DNP3 Object의 값을 읽을 수는 없었다.

또한 패킷의 값을 가로챈 후 1bit만 변경하여 전송하였으나, 인증과 암호화를 동시에 하는 AE의 특성 상, 값이 변조되었음을 쉽게 확인하고, SCADA 시스템으로 문제가 발생함을 신속하게 알려 변조 또한 불가능하였다. 이를 통해 DNP3 AE가 DNP3의 공격을 성공적으로 막아낼 수 있음을 알 수 있다.

비교

DNP3 AE를 (가용성을 제외한) 비밀성, 무결성, 인증과 최적화의 관점에서 기존에 제시된 DNPSec, DNP3 SA와 비교하여 [표 1]에 정리해 보았다.

	DNPSec	DNP3 SA	**DNP3 AE**
비밀성	O	X	O
무결성	O	O	O
인증	O	O	O
동작 레이어	Data Link Layer	App. Layer	App. Layer
SW 최적화	O	O	O
HW 최적화	X	X	O
오버헤드	많음	보통	보통

[표 1] DNP3 보안 프로토콜의 비교

DNP3 SA는 암호화를 제공하지 않아 비밀성을 충족하지 못하며, 이는 DNP3 프로토콜 자체의 공격은 막을 수 있으나, SCADA 시스템의 다른 곳을 공격할 실마리가 될 수 있어 문제가 있다. DNPSec은 암호화와 인증을 모두 제공하지만, Data Link Layer에서 암호화를 수행하기 때문에, 별도의 최적화를 제공하지 않아 오버헤드가 많을 것으로 짐작된다. 또한 DNPSec은 암호화 알고리즘으로 3DES와 같은 오래된 알고리즘만 지원하는 것[6]도 단점이다. 우리가 제시한 DNP3 AE는 암호화와 인증을 동시에 제공할 뿐만 아니라, GCM, PRINCE 등으로 경량화를 노렸고, 이들은 모두 쉽게 하드웨어로 구현될 수 있는 장점이 있어, DNPSec, DNP3 SA에 비해 우위를 가지고 있다 볼 수 있다.

V. 결론

방화벽 등을 통해 프로토콜 외부에서 이미 공격에 대한 방어가 가능하나, APT와 같이 새로운 공격 방법에 대응하려면, DNP3 프로토콜 자체에서도 보안을 강화해야하는 것은 분명하다. DNP3는 인증과 암호화를 제공하지 않아, 우리가 시도한 간단한 가로채기 및 변조로도 쉽게 공격이 가능하였다.

보안 강화 수단으로써 본 논문에서는 Authenticated Encryption을 DNP3에 적용하는 것을 통해 인증과 암호화를 동시에 제공하는 것을 제안하였고, 한 구현 예로 PRINCE와 GCM을 적용하여 공격을 막을 수 있음을 보였다.

그러나, 이후에 해야할 작업 또한 많이 남아 있다. 현재 구현에서는 매 Application Layer 메시지마다 최소 24바이트의 오버헤드가 발생하고 있는데, 작은 데이터를 주로 주고 받는 DNP3에선 비교적 큰 부하가 될 수 있어 최적화가 필요하다.

또한 DNP3 AE를 실제 SCADA 시스템에 적용하기 위해서는, 더 실제 환경에 가까운 테스트베드에서 운용해 보아야만 한다. 이번에 사용한 테스트베드는 네트워크 내에 단지 세 대의 단말만 존재하여 명확한 한계를 보였으며, PRINCE 알고리즘 등이 소프트웨어로만 구현되어 실제 동작 속도를 확인하는데도 어려움이 있었고, SCADA 시스템의 특성상 폐쇄망을 운영하기 때문에 추후 본 방식의 효율성을 실제 환경에서 검증하는 과정이 필요하다.

[참고문헌]

[1] IEEE, “IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3),” IEEE Std. 1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

[2] 이동수, 김광조,"SCADA용 DNP3 프로토콜의 소규모 실험환경구축", 2013 정보보호학술발표회논문집 충청지부, pp.66-71, 순천향대학교, 천안.

[3] Dongsoo Lee, HakJu Kim, Kwangjo Kim, and Paul D. Yoo, "Simulated Attack on DNP3 Protocol in SCADA System", 2014 Symposium on Cryptography and Information Security (SCIS 2014), Jan. 21-24, 2014, Kagoshima, Japan.

[4] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi, “A Taxonomy of Attacks on the DNP3 Protocol,” Critical Infrastructure Protection III, Springer Berlin Heidelberg, 2009. 67-68.

[5] Dong Jin, David M. Nicol, and Guanhua Yan, “An event buffer flooding attack in DNP3 controlled SCADA systems,” Proceedings of the Winter Simulation Conference, Winter Simulation Conference, 2011.

[6] Munir Majdalawieh, Francesco Parisi-Presicce, and Duminda Wijesekera, “DNPSec: Distributed network protocol version 3 (DNP3) security framework,” Advances in Computer, Information, and Systems Sciences, and Engineering, Springer Netherlands, 2006, 227-234.

[7] DNP3 Users Group, “DNP3 Secure Authentication Version 5 Overview,” http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf

[8] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html

[9] David McGrew and John Viega, “The Galois/Counter mode of operation (GCM),” Submission to NIST, http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf, 2004.

[10] Encryption modes development - NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html

[11] “DNP Secure Authentication - Essential to Smart Grid Progress,” Smart Grid News, Nov 18, 2008, http://www.smartgridnews.com/artman/publish/industry/DNP_Secure_Authentication_Essential_to_Smart_Grid_Progress.html

[12] OpenDNP3 Project, https://github.com/automatak/dnp3/wiki/Introduction-to-OpenDNP3, Accessed: December 16th, 2013.

[13] Ettercap Project, http://ettercap.github.io/ettercap/

[14] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçın, “PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications,” Advances in Cryptology - ASIACRYPT 2012. Springer Berlin Heidelberg, 2012, 208-225.

[15] HakJu Kim and Kwangjo Kim, "Who can survive in CAESAR competition at round-zero? ",2014 Symposium on Cryptography and Information Security (SCIS 2014), Jan. 21-24, 2014, Kagoshima, Japan.