SCIS 2014 The 31th Symposium on Cryptography and Information Security
Kagoshima, Japan, Jan. 21-24, 2014
The Institute of Electronics, Information and Communication Engineers

# Simulated Attack on DNP3 Protocol in SCADA System

Dongsoo Lee* HakJu Kim* Kwangjo Kim* Paul D. Yoo†

**Abstract:** Supervisory Control and Data Acquisition (SCADA) system monitors and controls industrial process in physical critical Infrastructures. It is thus of vital importance that any vulnerabilities of SCADA system must be identified and mitigated. DNP3 is and open SCADA network protocol that is mainly used in electrical utilities. However, the security mechanisms of DNP3 were neglected at its design stage. For example, the coverage of DNP3 Secure Authentication is limited to itself only. In our experiments, we have successfully performed a number of attacks to DNP3 on a small-scale testbed. Hence, this paper will not only discuss our experimental results but also propose a novel hybrid method that can enhance the security of existing DNP3 protocol by combining both encryption and authentication techniques.

**Keywords:** SCADA, DNP3, Authenticated Encryption, Testbed.

## 1 Introduction

SCADA is a type of Industrial Control System (ICS) that controls and monitors all critical infrastructure such as power plants, water pipeline and railroad system, *etc.* Cyber-attacks on such systems are being launched more frequently and may cause unrecoverable damages to our societies. In the past, ICSs ran on proprietary networks and were isolated from cooperate networks (*i.e.*, business networks) and the Internet. However, their architectures have changed, and being externally inter-connected to the business network and the Internet. In other words, they now more resemble corporate LANs with Internet access. This change greatly increases the possibility of breaches.

DNP3 (Distributed Network Protocol)[1] is the most popular SCADA network protocol in North America, which is one of the modern SCADA network protocols and based on the open technologies. DNP3 is a bi-directional protocol between master and slave devices via various communication media. It is a relatively reliable and efficient, and allows low network bandwidth and processing power. To achieve better efficiency, DNP3 adopts a network layer model called Enhanced Performance Architecture (EPA). EPA has only three network layers; physical, data link, and application layers. As for better reliability, DNP3 includes transport function within its application layer. However, security mechanisms of DNP3 were not considered at its design stage since the network will be deployed in closed environment. Through our a few consecutive simulations performed on our testbed, we will show how DNP3 could be attacks, and how it could be improved. Finally, we will compare the performance of our novel protocols with DNPSec and DNP3 Secured Authentication as well.

## 2 Related Approach

### 2.1 Attacks on DNP3

East *et al.* [2] has successfully showed the vulnerability of all DNP3 layers in their work. DNP3 has a data link layer, a pseudo-transport layer and an application layer. They categorized existing attacks into interception, modification, and fabrication types.

Jin *et al.* [3] has also successfully attacked DNP3 event buffer for unsolicited message. Unsolicited

* Computer Science Dept., KAIST, 291 Gwahak-ro, Yuseong-gu, Daejeon, 305-701, Korea . {letrhee,ndemian, kkj}@kaist.ac.kr
† ECE Dept., Khalifa Univ., Abu Dhabi Campus, P.O.Box 127788, Abu Dhabi, UAE. paul.d.yoo@ieee.org

message in DNP3 is asynchronous, thus to make event buffer full, system is not able to receive normal message.

### 2.2 Enhancements to DNP3 Security

**DNPSec**

DNPSec[4] is a proposed security framework for DNP3. It effectively provides confidentiality, authenticity, and integrity. To encrypt and authenticate its frames, DNPSec changes its original frame structure of DNP3 data link layer. In the framework, the encryption and the authentication are executed separately. DNPSec encapsulates the original DNP3 frame with a new header, a new frame sequence number, and an authentication data. It uses the session key to encrypt and to authenticate the frame. The session key is updated when the session time is expired or the new frame sequence number reaches its limit. DNPSec utilizes several encryption and authentication algorithms, namely, 3-DES (Triple Data Encryption Standard), and HMAC-SHA-1(keyed-Hash Message Authentication Code using Secure Hash Algorithm). However, 3-DES and SHA-1 are found to be insecure, slow, and outdated algorithms [5] [6], and many devices in the SCADA systems do not have enough resources to execute both encryption and authentication separately.

**DNP3 Secure Authentication**

DNP3 Secure Authentication (DNP3 SA) [7] is the official security add-on to application layer of DNP3. With this add-on, DNP3 becomes compliant with IEC 62351-5 standard. DNP3 SA is based on open technologies. In addition, it not only uses challenge-response mechanism with HMAC to provide authenticity and integrity, but also supports both asymmetric and symmetric cryptography for key management. DNP3 SA provides perfect forward secrecy as it allows multiple users to be authenticated in one machine. It effectively protects the SCADA system from the spoofing, modification, and replay attacks.

### 2.3 Authenticated Encryption

Authenticated Encryption is an encryption mode of operation that provides confidentiality, integrity, and authenticity simultaneously and efficiently. GCM (Galois / Counter Mode) [8] is an Authenticated Encryption mode that uses counter mode in encryption and universal hashing under Galois field in authentication. GCM is very cost-efficient (less chip-area) when implemented in hardware. GCM is one of the submissions to NIST [9]; NIST is accepting Authenticated Encryption modes for public consideration.

## 3 Analyzing DNP3 Vulnerability and Simulating Attacks in DNP3

### 3.1 Vulnerability of DNP3 and DNP3 SA

DNP3 has no security features. DNP3 SA is a security add-on to DNP3, and DNP3 SA provides authentication for authenticity and integrity. However, DNP3 SA does not allow encryption for confidentiality. "IEC and DNP Users Group believe that encryption of the SCADA data is unnecessary if impersonation and modification are prevented"[10]. Stuxnet and its successors can collect the sensitive data from the SCADA system protected by DNP3 SA, because the data is not encrypted. The malicious master / slave or man-in-the-middle attack is also possible.

### 3.2 Simulated Models

Using OpenDNP3 Library [11], we build small-scale testbed which has a simulated simple water power plant. This testbed consists of one master station, one outstation, and one attacker. The outstation has sensors and actuators, which are not real device, just represents as values. The outstation repeats reporting current date, water level, opened state of water gate and rainfall to master station. Master station receives data from the outstation, and can change water gate only. Rainfall changes by day, especially rain is heavy from Jun. to Oct. in Korea. Thus, the master station should change water gate properly to prevent overflow.

### 3.3 Attack Scenario

We assume that the attacker have succeeded to break into out simulated SCADA network, and will try two kinds of attacks namely sniffing and modifying packets. In network, Master station, outstation and attacker have own IP; 192.68.0.2, 192.168.0.3, 192.168.0.4.

**Sniffing Packets**

We use Ettercap [12] as tool for man-in-the-middle attack, ARP poisoning and packet forwarding. After ARP poisoning we use Wireshark to

analyze sniffed DNP3 packets.

**Modifying Packets**

The attacker is aiming to modify DNP3 packets in the network. We made an attacking tool using libpcap. When attacking tool receives sniffed DNP3 packets, it divides the packets into all of the layers: Ethernet, IP Layer, TCP Layer, DNP3 Data Link Layer, DNP3 Transport Layer and DNP3 Application Layer, and parses DNP3 data objects. Then, tool updates them by modifying rules, and rebuilds its packets by reverse order, recalculate checksum values, and forwards them to original place.

Using this tool, the attacker can modify requested packets that water gates will open only half which master wants. It also changes the responded message from outstations. Modified packets always show safe water level and requested water gate status by master. It the time is over, water plants will face serious situation.

### 3.4 Result

**Sniffing Packets**

Wireshark display DNP3 Object Data which are same as DNP3 Testbed like Figure 1. If we try sniffing packets from DNP3 SA, We can successfully get object data with MAC, because DNP3 SA doesn't have encryption. It is quiet anxious.

**Modifying Packets**

In DNP3, Packet modification also works well. The master station and the outstation show totally different result, but there is no error like Figure 2. Master stations displays that all gates are opened as requested; 80%, 60%, 80%, 80%. But Outstation have falsified values; 40%, 30%, 40%, 40%. Also sensors detect that water level is over 90%, however it isn't sent correctly. Because of mimicking all of the values, thus the SCADA Administrators is hard to know entire system is attacked. When they figure out what happened on the system, the situation has already become worst.

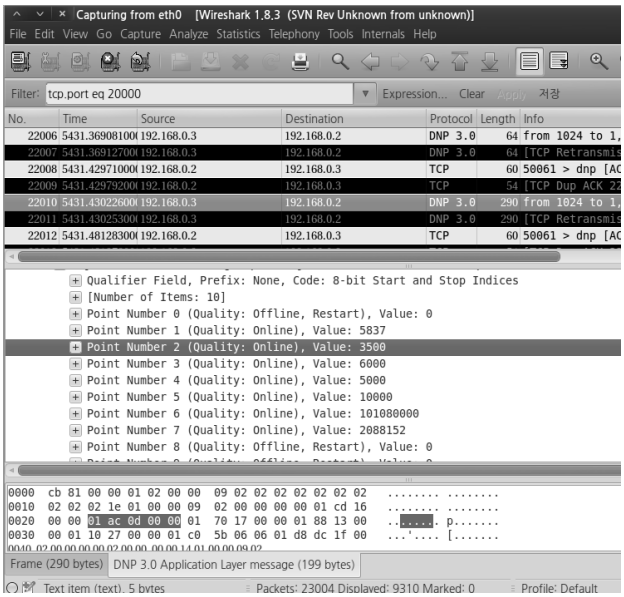
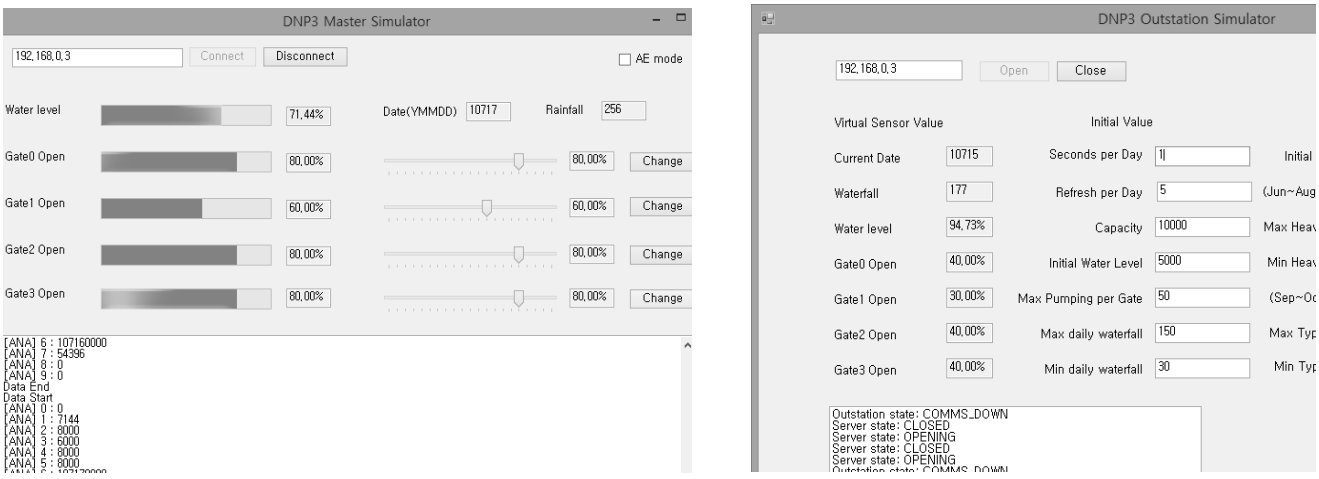



Figure 1: Analyzing DNP3 Object using Wireshark

## 4 Security improvement

### 4.1 Authenticated Encryption

SCADA system has many Remote Terminal Units (RTUs) which have very low resources. Thus, we must consider the hardware implementation of Authenticated Encryption mode. We have chosen GCM as the Authenticated Encryption mode and PRINCE [13] as the underlying block cipher of GCM. PRINCE requires very low chip-area and power consumption. Because we don't have resources to




(a) Master station part (b) Outstation part

Figure 2: Modified packets by MITM attack.

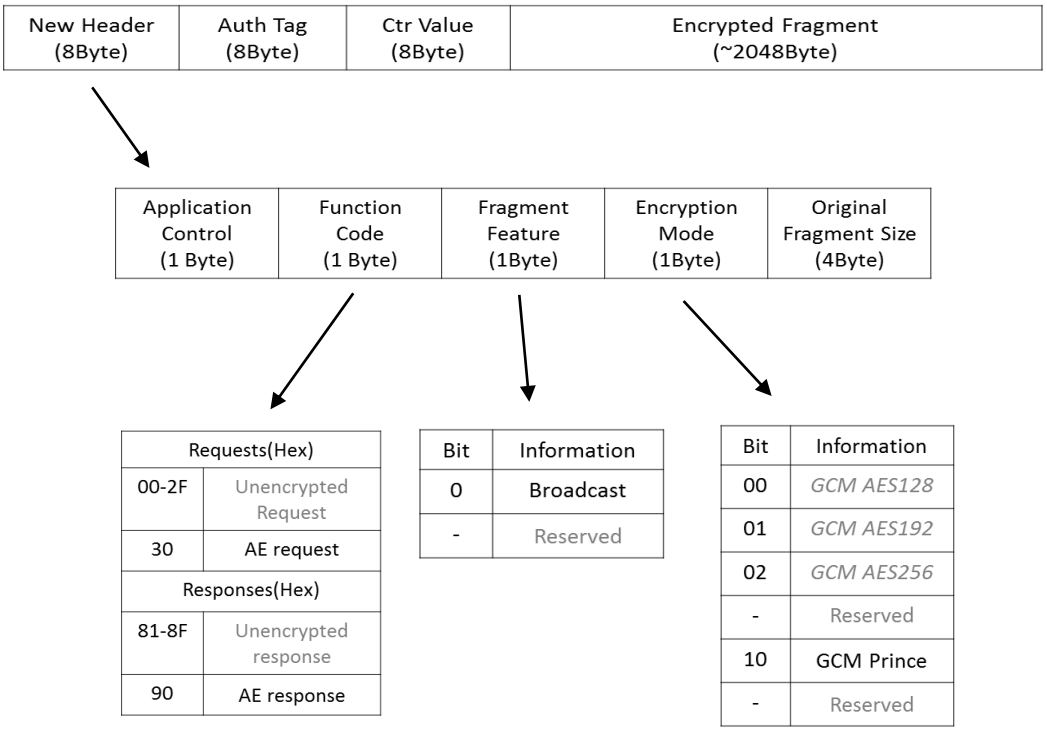



Figure 3: DNP3 AE's new application layer structure

implement the algorithms in hardware, we implemented them in software for out experiment.

GCM and PRINCE are implemented in C++ language using Microsoft Windows 7 64-bit version and Visual Studio 2012. The library used to implement GCM and PRINCE is GSL 1.16 (GNU Scientific Library).

### 4.2 Implementation

Let us assume all of the keys for the encryption are pre-shared. Supposed improvement may change DNP3 Application Layer. It encrypts all of the application layer message and makes own header to put it.

Our proposed scheme including new DNP3 AE Header was shown in Figure 3.

Application control is preserved for backward compatibility and function code is also preserved but it has another code 0x30, 0x90 for AE request and response.

Fragment feature is reserved for important flag in original application layer message whether it broadcasts or not. Encryption mode flag is for the selection of encryption algorithm and block size. In our implementation we implemented GCM Prince only.

Including new header, authentication tag and counter value, about 24byte are increased compare to DNP3.

### 4.3 Evaluation

To see if our approach works successfully, we try to attack same methods which sniffing packets and modifying packets mentioned above.

Although we sniff DNP3 AE Packets, we are still not able see the message in it as Figure 4. We also try to change just 1 bit of the message to check falsification, counterpart does not receive message because of authentication failure.

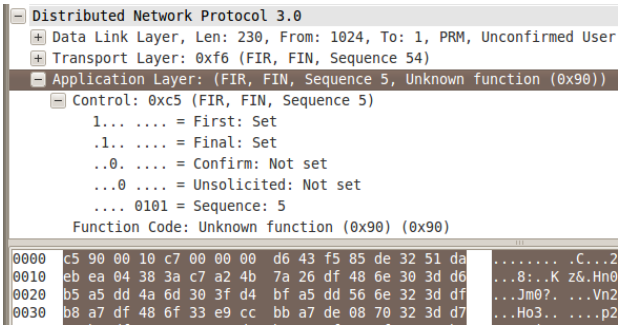



Figure 4: Result at Sniffing DNP3 AE packets

## 5 Comparison

We compare DNPSec, DNP3 SA, Bump-in-the-wire and our scheme in view of CIA principle, changed layer and overhead in Table 1.

With critical infrastructures, confidentiality is very important as any marginal expose of critical

infrastructure's information can cause cyber-attacks. Many SCADA devices also has low performance, thus method should have low overhead is import as soon as possible. However DNPSec should encrypt in data link layer, thus there is no way to reduce overhead.

Table 1: Comparison of DNP3 secure schemes

| | DNPSec | DNP3 SA | Bump-in-the-wire | Ours |
|---|---|---|---|---|
| Confidentiality | O | X | O | O |
| Integrity | O | O | O | O |
| Authenticity | O | O | O | O |
| Embedded Layer | Data Link Layer | App. Layer | Physical Layer | App. Layer |
| S/W | O | O | X | O |
| H/W | X | X | O | O |
| Overhead | High | Mid | Low | Mid |

Bump-in-the-Wire is easy method to enhance security without legacy device upgrade, however if we want to secure entire system, it is not proper solution.

## 6 Conclusion

Although there are a few external security options available such as firewalls, it is of critical importance to protect DNP3 protocol. The security aspect of DNP3 is still weak due to the lack of authentication and encryption. In this paper, we have shown that we can sniff and modify DNP3 messages, and finally attack DNP3-based SCADA system.

DNP3 Secure Authentication guarantees integrity and authenticity. However, there is still no guarantee on confidentiality. Therefore, we proposed a novel DNP3 Authenticated Encryption method, which has capability for both authentication and encryption. The consecutive simulations showed that our approach could enhance the security of DNP3 better than DNPSec and DNP3 AE as one of simple practices.

However, we still have many tasks remain. First, we need to reduce the overhead of encryption and decryption. We have at least 24byte overhead for every application layer message. If our approach needs less overhead, it would be better to adapt previous DNP3 systems.

Second, we need to implement a more real-scale SCADA testbed. Our experiments considered three devices only in our simulated SCADA network. In addition, PRINCE algorithm was not implemented in hardware. With such improved experimental setting, our experimental results would be more precise and bring helpful results.

## Acknowledgement

This research was supported by the KUSTAR-KAIST Institute, Korea, under the R&D program supervised by the KAIST and funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program.

## References

[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] 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.

[3] 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.

[4] 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.

[5] Tomoiaga Radu and Stratulat Mircea, "Evaluation of DES, 3 DES and AES on Windows and UNIX platforms," Computational Cybernetics and Technical Informatics (ICCC-CONTI), 2010 International Joint Conference on, IEEE, 2010.

[6] Stéphane Manuel, "Classification and generation of disturbance vectors for collision attacks against SHA-1," Designs, Codes and Cryptography 59.1-3 2011, 247-263.

[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, Accessed: December 16th, 2013.

[8] 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.

[9] Encryption modes development - NIST, http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html, Accessed: November 21th, 2013.
[10] "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, Accessed: December 16th, 2013.
[11] OpenDNP3 Project, https://github.com/automatak/dnp3/wiki/Introduction-to-OpenDNP3, Accessed: December 16th, 2013.
[12] Ettercap Project, http://ettercap.github.io/ettercap/, Accessed: December 16th, 2013.
[13] 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.