

배전자동화 시스템에서 사이버 공격에 대비한 보안 알고리즘 적용방안

論 文

Cyber Security Algorithms in the Distribution Automation System

Abstract – As communication is becoming increasingly prevalent and especially communication architecture is more relying on the open standard communication protocols, the security issues become major concerns. In this paper we consider possible cyber attacks in the applications based on the current distribution communication architecture, and then derive the security goals. Next we propose how the security algorithms can be adapted to achieve these security goals. We intend to adapt the most efficient ways of secure message exchange, taking the resource-constrained FRTUs into account. Finally we show some experiments to validate the protocols.

Key Words : 배전자동화, 배전통신망 보안, 사이버 공격, 보안 알고리즘, 메시지 인증, 메시지 인증 코드, 키 분배, Message Authentication Code

1. 서 론

배전자동화 시스템의 목적은 원거리에 산재하는 배전선로용 개폐기들이 전압과 전류 등의 계통 운전 정보를 통신망을 통하여 중앙 서버로 전송하고, 전송된 데이터를 기반으로 계통의 상태감시와 제어를 통해 배전계통을 운영하는 것이다[1].

배전자동화 시스템은 최근의 발달된 데이터 통신기술을 적용함으로써 중앙제어장치와 단말장치간의 통신을 통하여 운영되고 있다. 이러한 통신기술 덕분에 각 기기들로부터 신속하고 정확한 정보를 취득하여 배전계통의 효율적 운영을 할 수 있게 되었지만, 통신의 중요성에 비해 통신망 보안에 대한 문제는 아직까지 전력 분야에서 심각하게 고려되고 있지 않다.

대부분의 통신망을 사용하는 전력계통 운영 시스템들은 로컬 망(local network)을 구성하여 외부 출입을 차단하고 구역 내에 있는 사용자의 접근만 허용하는 물리적 보호에 의해 보안이 유지되고 있다. 하지만 이러한 보안방식은 전력 분야의 통신 인프라가 이전의 폐쇄된 사설 통신방식에서 벗어나 국제표준 통신방식을 사용하는 방향으로 발전하게 되면서 점차 한계를 드러내고 있다.

이러한 개방형 표준 프로토콜의 사용은 전체적인 시스템의 성능 향상과 효율을 증대시키지만 자연적으로 폐쇄된 통

신 방식에 의존했을 때에 비해서 사이버 공격에 대해 취약한 부분을 갖고 있다. 따라서 전력 시스템이 점점 통신 인프라에 의존하고 개방형 표준 통신 프로토콜에 의존함에 따라 사이버 공격에 대한 보안의 중요성이 증대되고 있다.

사이버 공격과 관련하여 미국에서는 2000년부터 통신을 사용하는 사회 각 분야의 시스템에 사이버 공격의 위협을 인식하고 이에 대한 대안을 마련하도록 법으로 제정하였다. 지금까지의 대부분은 LAN 기반의 근거리 통신망으로 연결되어 있는 SCADA 시스템 서버에 대한 보안이 주요한 대상으로 고려되어왔다[2-5]. 그리고 최근에는 통신망을 사용하여 원격으로 정보취득 및 제어를 할 수 있는 계전기나 자동화 개폐기들을 대상으로도 보안을 적용하려는 업체들의 움직임과 학계의 연구가 증가하고 있다[6-7].

이와 비슷한 시기에 유럽에서도 사이버 공격에 대해 본격적인 연구들이 시작되었으며, 특히 전력분야의 통신 보안의 경우에는 IEC에서 IEC TC 57을 통해 표준화 작업을 진행하고 있다. IEC TC 57에서는 현재까지 전력 시스템에서의 전반적인 보안 체계와 변전소 자동화 통합 프로토콜인 IEC 61850과 관련된 보안 요구사항과 보안 기술에 대해서 중점적으로 작업을 진행하여 IEC 62351이라는 표준화 작업을 진행 중에 있다[8-14]. 그 중 배전용 통신 프로토콜과 관련된 보안 표준은 IEC 62351-5로 배전용 프로토콜로 사용되고 있는 IEC 60870-5와 DNP 3.0 환경에서의 사이버 공격에 대한 위협과 보안 방안에 대해서 다루고 있다.

이러한 해외 연구들은 IEC 61850과 같은 이더넷 기반의 통합 프로토콜을 사용하는 디지털 변전소와 DNP 3.0 over TCP/IP over Ethernet과 같이 개방형 통신 프로토콜 기반의 통신 인프라로 진행되고 있는 움직임에 맞추어 진행되고 있다.

특히 배전계통 운영을 위한 통신망 보안에 대해서는 IEC

나 NERC의 보안 표준화 연구 동향과 본 논문에서 제안한 배전자동화 시스템의 통신망 특성에 따른 적합한 보안 알고리즘 적용방안의 기본적인 관점은 비슷하다. 배전계통 운영 특성에 따라 보다 빠르고 정확한 정보를 전송하기 위하여 인증의 기법을 사용하고 있고, 배전계통 운영에 대한 사이버 공격의 유형도 본 논문에서 다루는 패킷의 위변조 및 재생성과 시간차 공격에 대하여 주요 위협요소로 정하고 있다.

하지만 본 논문은 직접적으로 우리나라의 배전자동화 시스템 구조를 대상으로 적용이 가능한 방안을 제안하기 위하여 보다 세밀한 문제점과 그에 따른 방안에 대해 다루었다.

본 논문에서는 국내 배전자동화 시스템의 통신망의 특성에 따른 모든 보안 위협사항에 대하여 다루고 있다. 사이버 공격 가능성과 가장 파급효과가 클 것으로 예상되는 계통 단말장치에 대한 직접적인 공격에 대해 시스템 특성을 고려한 보안 알고리즘을 채택하고, 배전자동화 시스템에 대한 적용 방안을 제안한다.

본 논문에서는 시스템 특성을 고려하여 암호화 방식이 아닌 인증 방식을 채택하고 있다. 배전계통 운영 효율을 위해서는 다른 보안 알고리즘 보다는 연산양이 적은 메시지의 인증 방식이 더 효율적이기 때문에 인증의 방식을 채택하였다. 또한 인증방식의 보안능력 향상을 위해 비밀 키를 포함하는 인증 방식을 사용하려고 한다. 그러기 위해서는 키분배에 대한 문제가 새롭게 생기는데 이 문제에 대해서는 DES 알고리즘을 사용한 키 분배 방식을 채택하였다. 그리고 채택한 보안 알고리즘을 그대로 적용하면 패킷의 생성 및 위변조를 막을 수 있지만 시간차 공격에 대해서는 방어하지 못한다. 따라서 시간차 공격에도 대비할 수 있도록 본 논문에서 패킷을 설계하였고, 이러한 것들을 고려하여 본 논문의 사례연구를 하였다.

본 논문 구성은 다음과 같다. 2장에서는 배전자동화 시스템 통신망의 구조와 배전망의 특성에 따른 보안 위협의 유형을 분석하여 배전자동화 시스템이 목표로 하는 보안 요구사항에 대해 다루고 있다. 3장에서는 이러한 보안 요구사항을 만족시킬 수 있는 보안 알고리즘들을 소개하고, 4장에서는 그 중에서 배전자동화 시스템에 가장 적합한 보안 알고리즘을 선택하여 적용 방안을 제안한다. 5장에서는 본 논문에서 제안한 알고리즘의 타당성을 검증하기 위한 사례연구 결과를 보였다.

2. 배전자동화 시스템 통신망 특성에 따른 보안 위협

이 장에서는 보안 위협에 대해 1절에서는 우선 배전자동화 시스템의 통신망 구조를 살펴보고, 2절에서는 배전자동화 시스템 특성과 통신구조 때문에 생길 수 있는 사이버 공격 유형을 분석하였다. 그리고 3절에서는 사이버 공격 유형에 따라 배전자동화 시스템 통신망에서 요구되는 보안사항들에 대해 언급하였다.

2.1 보안 관점에서의 배전자동화 시스템의 통신 구조

배전자동화 시스템은 DAS 서버와 단말간에 DNP 3.0을 이용한 1:1 통신구조로 되어있다. 그림 1과 같이 DAS 서버는 FEP(front-end-processor)라는 통신 처리장치를 통해 계통의 단말장치로부터 정보를 취득하여 계통을 감시한다. 단

말장치는 연계통신망으로써 주로 광 전송망을 사용하고 있고, 보통 9600bps 속도의 직렬 통신 포트(serial port)를 통해 통신을 하고 있다.

배전자동화 시스템의 통신망은 로컬 망으로 독립적인 구성을 가지고 있기 때문에 외부에서의 침입이 쉽지 않다. 하지만 운영 설비나 통신망이 현장 지역에 널리 분포되어 있기 때문에 광 네트워크 내부나 광모뎀과 단말장치 사이에 접근하여 로컬 망에 침입이 용이할 것이다. 특히 단말장치마다에서의 침투는 단말장치가 현장에 널리 분포되어 있기 때문에 로컬 망 내부로의 침입과 경로에 대해 파악하기 어려운 특징을 가지고 있다. 따라서 DAS 서버와 단말장치 간의 메시지를 조작하여 임의로 계통에 전원을 공급하거나 정전을 유발시키는 사이버 공격에 대해 매우 취약한 구조를 가지고 있다.

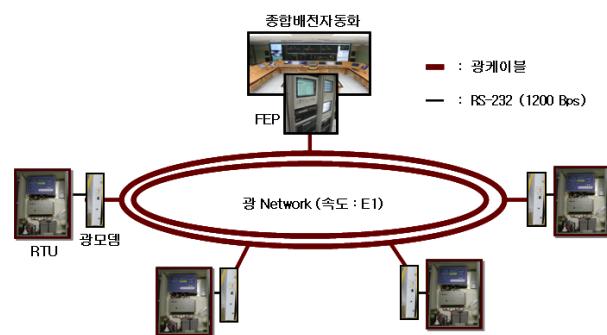


그림 1. 국내 배전자동화 시스템의 통신구조

Fig 1. Communication structure of DAS

배전자동화 시스템의 연계통신망 중에서 유선 광 전송망과 달리 무선 PCS 모뎀을 사용하는 지역도 있다. 이 경우에는 외부에서 쉽게 접근이 가능한 개방형 통신망 구조를 가지게 된다. 따라서 메시지의 조작에 의한 사이버 공격의 가능성이 더 높아진다.

이러한 사이버 공격 가능성에 대하여 한전에서는 무선의 경우 대칭키 방식(DES)의 보안 알고리즘을 사용하고 있다. 하지만 DES를 이용한 일반적인 메시지 은닉을 통한 암호화 알고리즘도 시간차 공격이라는 사이버 공격에 대해서는 취약한 부분이 있다.

예를 들면 휴대전화 복사 방식과 같이 모뎀의 정보를 복사하여 일정기간 패킷을 모았다가 제어 정보만 추출한 뒤, 특정시점에 한꺼번에 계통으로 전송을 하여 자동화 개폐기가 임의동작을 하도록 만드는 사이버 공격에 대해서 취약한 구조를 가지고 있다.

현재의 배전자동화 시스템은 정보의 전달이 DAS 서버와 단말장치 간의 통신에 집중되어 있다. 하지만 앞으로 배전 통신망은 이더넷과 TCP/IP 프로토콜을 기반으로 하는 통신 구조로 발전해 나갈 것이며, 이에 따라 정보의 전달도 서버와 단말 간의 통신에서 단말 간의 정보 전달이 주를 이루는 구조로 발전할 것이다.

따라서 본 논문에서는 현재의 배전자동화 시스템의 통신 환경 뿐 아니라 앞으로의 발전된 형태의 통신 구조에서도 배전계통 운영 단말 장치 간의 통신을 고려하여 사이버 공격 위협을 분석하고, 이를 기반으로 배전자동화 시스템 통신

망의 보안 요구사항에 대해 알아보도록 한다.

2.2 배전자동화 통신망에서의 사이버 공격 유형

가장 일반적인 보안 위협이 바로 정보 엿보기를 통한 공격이다. 공격자가 서버와 배전계통 운영 단말장치들 간에 통신 내용을 엿듣는 공격이다. 이것은 네트워크상에서 도청을 하거나 모니터링을 통해서 전송되는 메시지의 정보를 훔쳐보는 것으로서 엿듣기(eavesdropping)와 트래픽 분석, 두 가지 유형의 공격이 존재한다. 엿듣기는 직접적으로 메시지의 내용을 훔쳐보는데 비해서 트래픽 분석은 간접적으로 트래픽의 패턴을 분석하여 전달되는 내용을 파악하는 방법이다.

하지만 배전계통 상태정보 및 서버에서 단말로 전달되는 명령의 내용이 공개된다고 해서 배전계통 운영에 있어서 정전 등의 문제를 가져오지는 않는다. 따라서 배전자동화 시스템에서 이 공격의 위험도는 상대적으로 낮다고 볼 수 있다.

서버의 공격에 대해 서비스 거부(denial of service)를 목표로 하는 능동적인 형태의 공격으로는 메시지의 집중 전송으로 인해서 컴퓨터 자원을 고갈(resource exhaustion)시키는 공격이 있을 수 있다. 이러한 공격은 DAS와 FRTU 간에 세션을 하이재킹(hijacking)함으로써 이루어질 수 있다. 서버에 대한 수동적인 형태의 공격으로 바이러스, 웜과 같은 악성 코드에 의해 오동작을 유도하거나 부분적으로 기능을 정지시키는 공격이 있을 수 있다.

또한 서버에 대한 또 다른 형태의 공격으로서 서버에 존재하는 관리 정보 혹은 로그 기록에 대한 접근을 시도하여 훔쳐보거나 정보 내용을 변경하는 공격이다. 이러한 공격은 공격자에 따라서 두 가지로 구분할 수 있다. 먼저 내부 사용자가 고의적이건 비고의적이건 자신이 접근할 수 없는 정보에 대해서 권한을 위반하고 접근하는 경우이다. 두 번째로 외부 공격자가 마치 권한이 있는 사용자처럼 위장하고 서버의 정보에 접근하는 경우이다.

이러한 공격을 통해 서버가 정상적으로 동작하지 못할 경우는 신속한 조치를 통해서 해결이 가능하며, 서버의 재부팅 혹은 정상 동작으로 복구하는 동안에도 배전계통 운영 설비들은 정상동작을 하기 때문에 계통에 혼란이 생기거나 정전이 발생하여 문제가 생길 가능성은 적다.

하지만 배전계통 운영설비들은 넓은 지역에 퍼져있고 계속해서 설비들을 감시할 수 없기 때문에 오히려 서버에 대한 공격보다는 배전계통 운영설비들에 대한 직접적인 사이버 공격이 보다 용이할 것이다. 또한 수용가에 직접적으로 연결되어 있기 때문에 사이버 공격에 대한 피해가 보다 더 클 것이다.

따라서 본 논문에서는 배전계통에서 사이버 공격에 대한 가장 위험도가 높은 운영설비들에 대한 직접적인 사이버 공격을 대상으로 공격 유형과 이에 대한 대책을 제안한다. 본 논문에서는 배전자동화 시스템에 대한 사이버 공격유형을 크게 두 가지로 분석하였다.

- 메시지의 변조 또는 생성을 통한 공격
- 메시지 재사용에 대한 공격

첫 번째는 메시지의 변조 또는 생성을 통한 공격이다. 서버와 배전계통 운영 단말장치들에 전달되는 메시지를 이용해서 자동화 스위치의 상태를 임의로 조작하여 수용가에 정전을 유발시키는 공격이 있을 수 있다. 공격자는 배전계통 운영 단말장치로 전송되는 메시지를 가로채서 변조된 메시지를 전송하거나 자신이 인증된 송신자처럼 위장하여 위조된 제어 메시지를 전송할 수 있다.

두 번째는 이전에 전달된 메시지를 나중에 다시 최근의 메시지로 가장하여 전송하는 메시지 재사용(reply) 공격이 가능하다. 이러한 유형의 공격은 주로 배전계통 운영 단말장치들을 대상으로 오동작을 유발해서 계통에 혼란을 일으킬 수 있는 공격이라고 볼 수 있다.

이 두 가지 공격의 특징은 서버도 정상이고 배전계통 운영 설비들도 정상이지만 공격자는 계통의 스위치 상태를 임의로 조작하여 정전을 유발시킨다. 따라서 여러 사이버 공격 형태 중에 가장 위험도가 높은 공격 형태라 할 수 있다.

2.3 배전자동화 통신망에서의 보안 요구사항

모든 보안 위협을 해결하는 하나의 해결책은 존재하지 않으며, 또한 모든 위협에 대처하기 위해서 여러 가지 보안 기술을 동시에 적용하는 것은 현실적인 접근 방법이 될 수 없다. 보안 기술의 적용은 서비스의 종류와 시스템의 환경을 고려하여 보안 목표를 수립하고 이에 따라 보안 요구사항의 중요도를 고려하여 보안 목표를 수립해야 한다.

일반적인 통신망의 기본 보안 요구사항은 <표 1>과 같이 5가지로 구분할 수 있다. 하지만 배전자동화 시스템의 특성에 따라 이 통신망에서는 모든 보안 요구사항이 요구되는 것은 아니다.

표 1 통신망의 보안 요구사항

Table 1. Security demand of communication network

요구사항	내용
기밀성 (confidentiality)	전송되는 메시지를 공격자가 볼 수 없도록 하는 것으로 흔히 메시지를 암호화하여 전송
메시지 무결성 (message integrity)	송신자가 전송한 원래의 메시지의 내용이 변경되지 않는 것
가용성 (availability)	네트워크 노드의 정상적인 동작을 보장하도록 하는 것 (서버의 정상적인 동작을 방해)
접근 제어 (access control)	비권한 사용자가 특정 자원에 접근하는 것을 방지하는 것 (사용자의 인증)
부인 방지 (repudiation)	이전에 발생한 동작에 대해서 나중에 부인을 하거나 발생하지 않은 동작을 후에 주장하는 것

배전 통신망에서는 서버와 FRTU 혹은 FRTU 간에 정보의 전달을 통해서 각종 제어 동작을 수행한다. 따라서 배전 통신망에서 메시지를 전송할 때 공격자가 메시지의 내용을 판독하는 것 보다 더 위험한 공격은 메시지의 내용을 변경해서 전송하는 것이다. 따라서 메시지가 권한이 있는 사용자가 전송한 것인지를 확인할 수 있는 메시지 소유자 인증

과 메시지의 내용이 변조되지 않았다는 것을 보장할 수 있는 메시지 무결성은 가장 중요한 보안 요구사항이라고 할 수 있다.

가용성은 장비의 사용을 보장할 수 있도록 하는 것이다. 현재 연구되고 있는 차세대 배전통신망 서비스는 서버를 중심으로 이루어지기 보다는 오히려 피어간(peer-to-peer) 통신에 의한 FRTU 간에 메시지 전달이 주를 이룰 것으로 예상된다. 이러한 점에서 배전자동화 시스템에서는 LAN으로 연결된 서버를 중심으로 서비스가 제공되는 SCADA 시스템과는 달리 서버에 대한 집중 공격을 방어하기 위한 가용성은 상대적으로 중요성이 높지 않다.

또한 접근 제어의 경우 역시 서버에 의존하는 서비스가 아니기 때문에 중요도는 낮다고 할 수 있다. 특히 서버의 권한이 다른 여러 종류의 데이터베이스 정보를 접근하는 서비스의 필요성은 배전망 서비스에서는 크지 않다고 할 수 있다. 끝으로 부인 방지도 본 논문에서 고려하는 대상에 대해서 중요도는 아주 낮다고 할 수 있다.

배전자동화 시스템 통신망의 노드, 즉 배전계통 운영 단말장치는 장거리에 산재되어 위치하고 있고, 또한 배전자동화 시스템 통신망 노드의 컴퓨팅 파워(연산처리 능력)는 매우 제한적이며, 메시지의 전송과 응답은 가능한 빠르게 이루어져야 한다는 특징을 가지고 있다.

따라서 이와 같은 특징들을 고려하여 배전자동화 통신망에서의 사이버 위협 요소들과 보안 요구사항의 상관관계와 배전통신망의 특성을 고려한 보안 요구사항의 중요도를 <표 2>과 같이 정리할 수 있다. 따라서 본 논문에서는 <표 2>와 같은 보안 요구사항에 초점을 맞춰서 이를 만족시킬 수 있는 보안 방식에 대해 알아보도록 한다.

표 2. 배전자동화 시스템에서 보안 요구사항 상관관계
Table 2. A correlation of security demand in DAS

위협 유형	보안 요구사항	중요도
데이터 엿보기(eavesdropping)	기밀성 (confidentiality)	●
트래픽 분석		●
메시지 변경	메시지 무결성 (message integrity)	●●●
위장(악의적) 메시지 전송		●●●
메시지 재사용(replay)		●●●
하이 재킹(hijacking)		●
서비스 거부(denial-of-service)	가용성 (availability)	●●
자원고갈(resource exhaustion)		●●
악성 코드		●
위장(masquerade)	접근 제어 (access control)	●●
비권한 사용자의 접근		●●
부인(repudiation)	부인 방지	

3. 배전계통 통신망 보안 요구사항에 따른 보안 알고리즘

이 장에서는 2장에서 설명한 배전자동화 시스템 특성에 따른 보안 요구사항들을 만족시킬 수 있는 보안 알고리즘들의 특징들을 간략하게 살펴본다. 1절에서는 메시지의 기밀성을 보장하는 암호화 알고리즘을, 2절에서는 메시지의 유효성을 확인하는 인증의 방식에 대해 다루고 있다.

3.1 암호화 알고리즘

메시지의 기밀성을 보장하기 위해서 암호화 알고리즘이 사용된다. 또한 암호화 알고리즘은 메시지의 무결성과 인증을 위해서 사용되기도 한다. 암호화와 복호화에는 비밀 정보, 즉 키(key)가 필요하다. 암호화와 복호화를 하는데 같은 키를 사용하는 것을 대칭키(symmetric key) 암호화 방식이라고 하고, 다른 키를 사용하는 것을 비대칭키(asymmetric key) 암호화 방식이라고 한다.

대칭키 암호화 방식은 안전한 통신을 하고자 하는 두 사용자가 서로 똑 같은 비밀 키를 소유하여 암호화와 복호화를 하는 방식이다. 대표적인 대칭키 암호 기법에는 DES 알고리즘이 있다.

비대칭키 방식은 누구에게나 알려진 공개키와 각 개인만이 알고 있는 개인키의 결합으로 이루어진다. 송신자 A가 수신자 B의 공개키를 사용하여 암호화하여 메시지를 전송하면 수신자 B는 자신의 개인키를 사용하여 암호화된 메시지를 복호화 한다. 비대칭키 방식의 대표적인 방법으로는 RSA 알고리즘이 있다[15].

이 방법은 대칭키 방식과는 달리 두 개의 키를 가지고 암호화 및 복호화를 하기 때문에 연산 복잡도가 높다. 따라서 암호화 된 데이터의 크기와 연산양이 대칭키 알고리즘보다 훨씬 크기 때문에 컴퓨팅 능력이 한정되어 있는 시스템에서 비대칭키 알고리즘을 적용하는 것은 바람직하지 않다.

3.2 메시지 인증 코드

송신자의 공개키를 사용하여 전체 메시지를 암호화하여 보낼 경우 메시지의 무결성을 보장할 수 있다. 하지만 긴 메시지 전체를 공개키로 암호화하는 것은 많은 계산을 요구한다. 다른 방법으로는 원래의 메시지로부터 만들어지는 짧은 길이의 메시지 인증 코드(Message Authentication Code: MAC)를 메시지의 뒤에 붙여 전달하여 수신자는 MAC를 조사함으로써 원래의 메시지에 변경이 발생하였는지를 확인할 수 있다.

메시지 인증 코드(MAC)는 원래의 메시지로부터 해쉬 함수를 사용하여 얻은 짧은 길이의 메시지 디아제스트(message digest)를 구한다. 따라서 수신 노드는 MAC를 통하여 메시지의 무결성 뿐 아니라 송신 노드의 인증을 증명할 수 있다[16-17].

MAC을 구할 때 주로 해쉬 함수(hash function)를 사용한다. 해쉬 함수 H는 가변 크기의 메시지 값(x)을 고정된 크기의 스트링(h)으로 변화시켜 주는 것이다($h=H(x)$). 출력되는 스트링의 길이는 입력되는 메시지의 길이에 비해서 훨씬 짧은 길이이다. 흔히 고정 길이의 스트링을 메시지 디아제스트라는 용어로 부르기도 한다.

해쉬 함수 알고리즘으로는 다양한 메시지 디아제스트 알고리즘이 있는데 보통 MDn으로 표현한다. 이중 MD5와 함

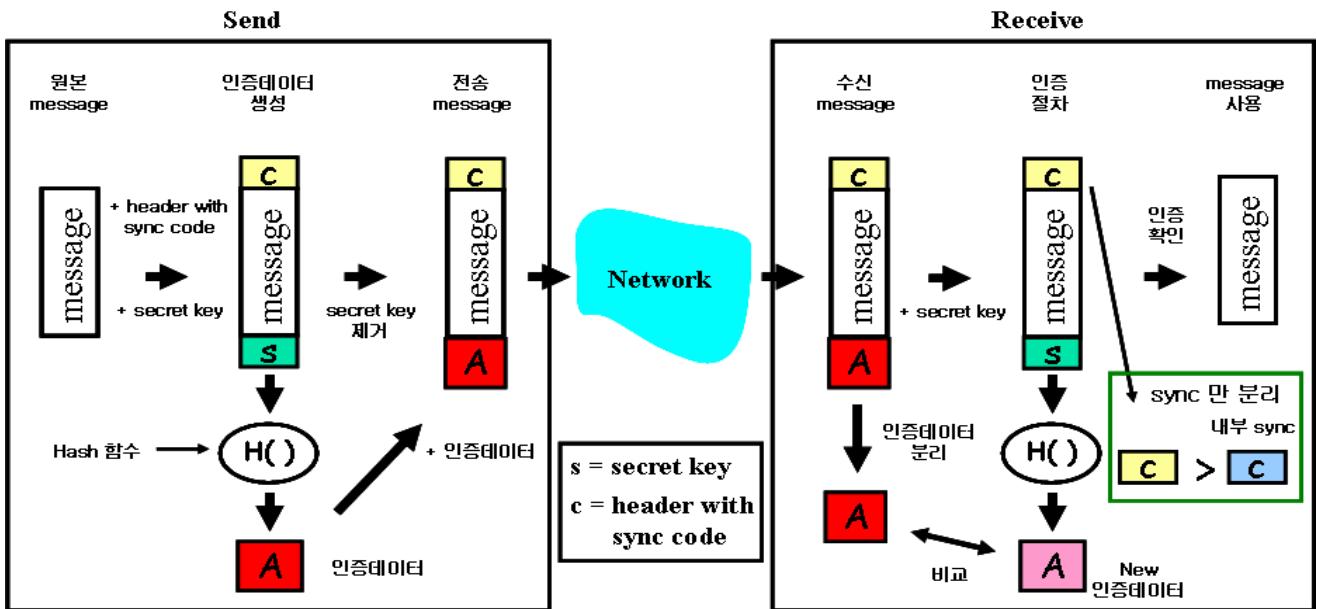


그림 2. 배전자동화 시스템에 적합한 보안 알고리즘의 적용방안

Fig 2. Applying Security Algorithms to suit to the Distribution Automation System

계 널리 알려진 해쉬 함수 secure hash algorithm-1(SHA-1)이 있다. 하지만 SHA-1은 입력 메시지의 길이에 제한이 있고 신뢰성에 문제가 있기 때문에 본 논문의 사례 연구에서는 해쉬 함수 알고리즘으로 MD5 방식을 선택하였다[18-20].

4. 배전자동화 시스템 통신망에 적합한 보안 알고리즘의 적용

본 논문에서는 2장에서 언급한 보안 요구사항과 3장에서 언급한 보안 알고리즘 방식에 따라 배전자동화 시스템에 인증의 방식을 적용하여 보안을 유지하는 방식을 제안한다. 이 장에서는 1절에서는 본 논문에서 제안한 방식을 어떻게 적용하는지에 대해 다루고 있다. 2절에서는 키를 사용하는 보안 방식에 꼭 필요한 키 분배 방식에 대해서 다루고 있다.

4.1 배전계통 운영 특성에 따른 인증방식의 보안 알고리즘 적용방안

3장에서 언급한 바와 같이 암호화 알고리즘, 특히 비대칭 키 알고리즘은 많은 계산 시간을 필요로 한다. 따라서 배전 통신망의 노드가 컴퓨팅 능력이 높지 않은 점을 고려한다면 암호화 연산 없이 메시지를 인증하는 방법이 배전계통 운영 효율에 있어서 바람직한 방법이라고 할 수 있다. 메시지의 무결성과 송신자의 인증은 메시지 인증 코드를 통해서 실현될 수 있다. 따라서 본 논문에서 제안하는 방식은 메시지 인증 코드는 원래의 메시지로부터 구한 메시지 디제스트에 sync code를 추가하는 방식이다.

그림 2는 본 논문에서 제안하는 배전자동화 시스템에 적합한 메시지의 인증 절차를 보여주고 있다. 먼저 송신 노드는 전송하고자 하는 메시지에 각 노드들이 공유하고 있는

비밀 키(secret key)를 첨부하고, 메시지 재사용 공격을 방지하는 동기화 코드(sync code)를 합쳐 해쉬 함수를 적용하여 인증 데이터(MAC)를 만들어 낸다. 그리고 송신 노드는 비밀 키를 제거한 원래의 메시지에 동기화 코드를 붙이고, 끝에 MAC이 첨부된 메시지를 최종적으로 전송한다.

수신 노드에서는 전송된 메시지에서 먼저 MAC을 제거하고, 원본 메시지에 송신 노드가 사용한 동일한 비밀 키를 첨부하여 해쉬 함수를 적용한다. 해쉬 함수를 통해 구한 MAC을 전송받은 MAC과 비교하여 두 값이 동일하면 수신한 메시지의 내용이 전송 중에 변경되지 않았다는 것을 증명할 수 있다. 또한 MAC의 값이 동일할 경우 이 메시지를 전송한 노드는 비밀 키를 소유한 신뢰할 수 있는 노드인 것을 인증하게 된다. 이와 같이 메시지 내용의 인증 뿐 아니라 메시지 소유주의 인증도 같이 할 수 있다.

동기화 코드의 역할은 메시지 재사용 공격을 방지하기 위해서 사용되는데 이 값은 항상 증가하는 값으로 나중에 전송되는 메시지는 이전에 전송된 메시지의 동기화 코드의 값 보다 항상 더 큰 값을 갖는다.

만약 현재 메시지의 동기화 코드의 값이 이전의 값 보다 작으면 이 메시지는 이전에 사용되었던 것으로 재사용된 메시지로 판단하여 폐기한다. 동기화 코드는 해쉬 함수가 적용될 때 메시지에 포함되므로 이 값을 변경하면 인증 데이터 값이 변경되기 때문에 수신 노드는 메시지가 변경된 것을 알 수 있다.

이와 같은 알고리즘을 통해서 2장에서 다른 배전자동화 시스템 특성에 따른 사이버 공격에 대한 보안 요구사항들을 모두 충족시킬 수 있다. 이 알고리즘에서 사용하는 메시지의 구성은 그림 3과 같다.

맨 앞의 *Auth Type* 필드는 사용하고자 하는 인증 유형을 표시한다. 이 절에서 설명한 알고리즘 이외에도 다른 형태의 인증 방식을 정의했다면 이 필드를 통해서 지정할 수 있

다. Key ID 필드는 각 노드가 상호 약속된 비밀 키가 여러 개 있을 경우 어떤 비밀 키에 대한 타입을 알려준다. Node ID 필드는 각 노드간의 통신을 위해 전송 노드의 정보를 가 들어간다. 그 뒤에는 원본 메시지의 길이, 인증데이터의 길이, 동기화 코드가 들어간다. 그리고 다음에 원본 메시지가 오고 마지막으로 MAC이 붙게 된다.

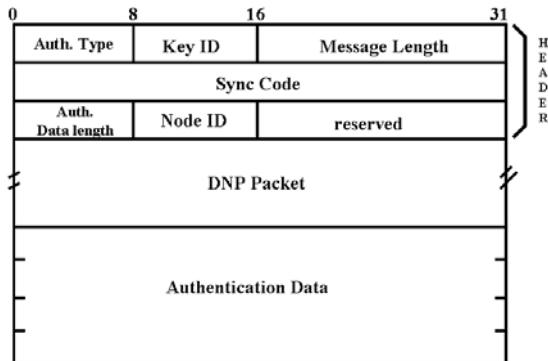


그림 3 패킷의 구성

Fig. 3. Packet format

4.2 키 분배 방안

이와 같은 보안 알고리즘을 적용하기 위해서는 배전자동화 시스템의 모든 노드들은 통신을 하는 상대방 노드와 공유하는 비밀 키를 갖고 있어야 한다. 각 노드에게 비밀 키를 부여하는 방법으로는 관리자가 각 노드에 비밀 키를 설치하는 수동적인 방법과 키 분배 알고리즘에 의해서 자동적으로 비밀 키를 부여하는 방법이 있다. 두 가지 방법은 병행해서 사용될 수 있는데 주기적으로 키를 갱신해야 하는 경우 수동적인 키 분배는 적합지 않기 때문에 이 경우에는 자동적인 키 분배 방식을 사용해야 한다.

자동적인 키 분배 방식은 신뢰할 수 있는 제3자를 통해서 키를 분배하는 것이다. 배전자동화 시스템에서는 DAS 서버가 이 역할을 담당한다. 제 3자를 통해서 키 분배하는 방법으로 가장 간단한 방식은 공개키(public key) 암호화를 사용하는 것이다. 하지만 배전시스템 노드의 컴퓨팅 능력이 일정할 때 동일한 데이터 전송 속도를 만들어 내려면 비대칭 키를 이용한 암호화의 키 분배 방식 보다는 대칭키에 의한 키 분배 방식을 사용하는 것이 보다 효율적일 것이다. 따라서 본 논문에서는 대칭키 방식에 의한 키 분배 알고리즘을 제안한다.

초기 설정 시 각 노드는 서버와 공유하여 사용하는 대칭 키를 메모리에 보관한다. 서버는 각 노드에게 비밀 키를 부여할 때 비밀 키를 이 대칭키로 암호화하여 전송한다. 따라서 비밀 키를 분배할 때 기밀성을 보장할 수 있으며 각 노드는 안전하게 비밀 키를 부여받을 수 있다.

각 노드는 비밀 키를 부여받을 때 서버에 랜덤 값(nonce)과 메시지를 전송한다. 그러면 서버는 이 노드와 공유하고 있는 대칭키(SK_{SA})를 사용하여 비밀키(AK_{SA})를 암호화하여 전송한다. 다음은 노드A가 서버 S로부터 비밀 키를 부여 받는다.

$$A \rightarrow S: N_A, M_A \\ S \rightarrow A: \{AK_{SA}\}_{SK_{SA}}, MAC(N_A|M_A|\{AK_{SA}\}_{SK_{SA}})$$

여기서

N_A	: A의 nonce
M_A	: A의 전송 메시지
AK_{SA}	: A의 비밀키
SK_{SA}	: A와 공유하고 있는 대칭키
$\{M\}_S$: 키 S로 암호화한 메시지 M
$MAC(x y z)$: x, y, z로 연결된 메시지의 MAC

노드 A는 비밀 키를 부여받을 때마다 새로운 nonce (N_A) 값을 사용한다. 만약 공격자가 A로 위장하고 서버로부터 비밀 키를 받고자 할 때 nonce 값이 다르기 때문에 nonce 값을 포함하여 계산된 MAC 값이 달라진다. 또한 서버는 각 노드에게 비밀 키를 전송할 때 MAC을 첨부하여 전송하기 때문에 각 노드는 비밀 키가 서버로부터 배분된 것임을 확인할 수 있다. 따라서 이와 같은 키 분배 알고리즘을 통해서 서버가 각 노드에게 비밀 키를 전송할 때 비밀 키의 기밀성뿐 아니라 서버 자신의 인증과 메시지 무결성을 보장하고 메시지 재사용 공격을 막을 수 있다.

5. 사례 연구

본 논문의 4장에서 제안한 보안 알고리즘을 검증하기 위하여 그림 5와 같이 세 대의 PC를 이용하여 시스템을 구성하였다. 그리고 제안한 보안알고리즘에 대한 검증은 다음의 6 단계의 절차를 걸쳐 진행하였다.

1단계의 의미는 보안이 적용되지 않은 상태에서 해커가 DAS와 FRTU간의 패킷을 바이패스 시킨다면 DAS에서 해커의 침입여부를 파악할 수 없다는 것을 보여준다. 2단계의 의미는 보안이 적용되지 않는 상태에서 해커의 단말장치가 DAS의 DNP Master address를 가지고 FRTU에 직접적으로 제어명령을 내렸을 때 DAS로 인식하고 동작하는 것을 보여준다. 이는 해커의 침투로 인하여 계통의 스위치 상태가 해커의 의도에 따라 계통이 변경될 수 있다는 위험을 보여준다.

3단계의 의미는 보안이 적용된 상태에서 해커가 DAS와 FRTU간의 패킷을 바이패스 시켰을 때 1단계와 동일하게 시스템에 이상여부를 파악할 수 없다는 것을 보여준다. 하지만 4, 5단계에서 DAS가 FRTU로 보내는 패킷을 해커가 중간에서 가로채어 패킷을 위변조 하였을 때 FRTU가 동작하지 않음을 보여준다. 이는 보안을 적용하였을 때 해커의 의도대로 계통의 스위치 상태가 변하지 않음을 알 수 있다.

6단계의 의미는 시간차 공격에 대한 사례연구이다. 보안이 적용된 상태에서 DAS가 FRTU에 3번의 각기 다른 스위치 변경 명령을 전송하여 FRTU가 동작함을 보여주고 있고, 해커가 중간에서 해당 패킷을 가로채어 이 명령을 그대로 다시 전송했을 때 FRTU가 동작하지 않음을 보여주고 있다.

사례연구 환경은 일반 windows 환경의 PC 3대를 사용하였으며 DAS PC는 DNP 3.0 master를 탑재하였고 FRTU PC는 DNP 3.0 slave를 탑재하였다. Hacker PC는 serial port 두 개가 사용 가능하도록 꾸며 DNP 3.0 Master를 탑

재하여 다음과 같은 6단계의 절차를 진행하였다.

- 1) 우선 보안이 적용되지 않은 그림 5와 같은 구조에서 DAS PC가 FRTU PC에 명령을 내려 정상동작 하는지를 확인
- 2) 공격자 PC에서도 FRTU PC로 같은 명령을 내려 동작하는지를 확인하여 보안 위협에 대한 가능성을 보임
- 3) 보안을 적용하여 DAS PC에서 FRTU PC로 명령을 전송할 때 정상적인 인증 절차를 통해 시스템에 문제가 생기지 않는 것을 보임
- 4) DAS PC에서 전송한 명령 메시지를 공격자 PC에서 중간에서 빼돌려 저장시켰다가 원본 메시지 부분을 변경하여 FRTU PC로 전송하여 인증 여부를 파악
- 5) 공격자 PC는 DAS PC에서 사용하는 비밀키를 알지 못하는 상태에서 대신 같은 해쉬 함수를 가져다가 1번에서 내린 명령을 정해진 패킷대로 설계하여 전송을 시도
- 6) DAS PC에서 3개의 제어명령을 전송하여 FRTU PC의 정상 동작 여부를 확인하고, 공격자 PC에 그 패킷을 저장한 뒤 공격자 PC에서 저장한 3개의 패킷을 FRTU PC로 재전송하여 시간차 공격을 시도

이와 같은 6번의 절차를 거친 결과는 표 2의 사례연구 결과에 잘 나타나 있다. 각각의 의미를 살펴보면 순서 1, 2는 현재 배전자동화 시스템에서 그림 5와 같은 공격자의 침입이 있을 경우에 자동화 스위치 동작에 따른 정전 및 계통 혼란이 가능하다는 위험성을 보여준다.

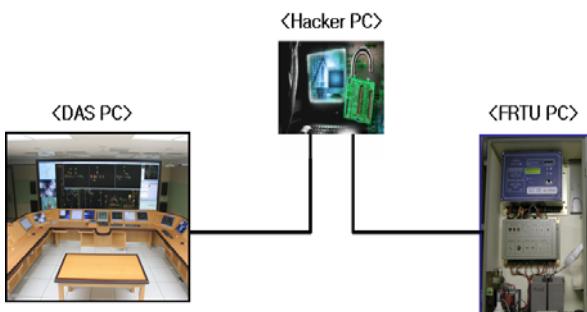


그림 5 배전자동화 시스템의 사이버 공격 시스템

Fig 5. A structure of cyber attack in DAS

순서 3에서는 보안을 적용하였을 때 상호간의 인증 시스템을 통해 정상적으로 시스템이 운영되는 것을 확인하였다. 이것을 바탕으로 순서 4에서는 공격자 PC에서 패킷을 취득하여 원본 메시지를 변경한 후에 FRTU PC로 같은 명령을 전송하였을 때 인증실패를 통해 오동작 하는 것을 확인할 수 있었다.

순서 5에서는 DAS PC에서 사용하는 해쉬 함수를 공격자 PC에서 패턴을 통해 알아냈다고 하더라도 비밀키를 모르기 때문에 신규 패킷 생성에 대해 명령 실패가 이루어 진 것을 보여주고 있다.

끝으로 순서 6에서는 재사용 공격에 대한 검증으로 DAS PC에서 명령 메시지 3개를 FRTU로 전송하여 패킷의 유효

성을 확인하고, 공격자 PC에서 이 3개의 메시지를 저장하였다가 FRTU로 한꺼번에 전송했을 때 동기화 코드 비교를 통해 인증 실패가 되는 것을 확인할 수 있다.

4.2에서 제안한 키 분배 방식을 적용하여 앞서 진행한 6 단계를 통해 같은 결과를 얻음으로써 본 논문에서 제안한 방법의 타당성을 검증하였다. 그 결과는 표 3에서 알 수 있듯이 해커의 패킷 위변조, 생성, 시간차 공격을 통해 단말장치에 직접적인 사이버 공격에 대해서는 인증을 통하여 완벽하게 방어하는 것을 확인할 수 있다.

표 3. 사례연구 결과

Table 3. The result of case study

순서	보안	DAS	Hacker	FRTU
1	X	제어명령 전송	바이패스	동작
2	-	제어명령 전송	제어명령 전송	동작
3	O	제어명령 전송	바이패스	인증성공 동작
4		제어명령 전송	패킷 취득 및 변경 후 전송	인증실패 부동작
5		-	보안 적용	인증실패 부동작
6		3번의 제어명령 전송	제어명령 전송 저장	인증성공 동작
		-	저장된 명령 한꺼번에 전송	인증실패 부동작

또한 본 논문에서 제안한 hash 알고리즘을 이용한 인증의 기법이 대칭키 알고리즘이나 비대칭키 알고리즘보다 얼마나 빠른가에 대하여 시간을 측정한 결과를 <표 4>에 정리하여 나타내었다.

시간측정을 하기위한 사례연구는 AMD Opteron(tm) Processor 150(2.4GHz) CPU에 O/S는 LINUX Fedora core 5를 사용하는 환경에서 표 4와 같은 결과를 얻었다. 이렇듯 배전계통 운영에 있어서 보안 알고리즘들 중에 암호화 기법보다는 인증의 기법을 이용하는 것이 데이터 전송이나 명령 전송에 있어서 보안성도 확보하고 빠르게 처리를 할 수 있다는 것을 입증하였다. 표 4의 시간 단위는 ms이며, 30회 연산의 평균값이다.

표 4. 보안 알고리즘별 연산시간 비교

Fig 4. Processing time comparison of each security algorithm

길이 (byte)	RSA		DES	Hash	
	Encoding	Decoding		MD5	SHA
32	129.4	830.5	3.4	2.8	3.1
128	253.2	1666.1	11.3	6.7	8.1
512	377.8	2499.7	42.9	16.6	24.2
2048	503.4	3332.5	170.2	57.5	87.1
8192	627.5	4171.5	673.8	219.1	350.7

6. 결론

본 논문에서는 전력계통 운영을 하는데 있어 꼭 필요하게

된 통신기술의 적용에 따라 계통보호의 입장에서 생길 수 있는 문제점인 사이버 공격에 대한 대응 방안을 다루었다. 먼저 배전계통을 대상으로 배전자동화 시스템의 보안 위협에 대해 분석하고 보안 요구사항에 대해 알아보았다. 그리고 배전자동화 시스템 특성에 따른 적합한 보안 알고리즘의 적용방안을 제안하였다.

본 논문에서는 배전계통 운영 특성에 따라 배전계통 운영 단말장치들의 컴퓨팅 파워를 고려하여 많은 연산양을 요구하는 암호화 알고리즘이 아닌 인증의 방식을 제안하였다. 그리고 중앙 서버를 통한 효율적인 키 분배 방식을 제안하였다.

제안한 방안들의 성능을 검증하기 위하여 6번의 절차를 거쳐 본 논문에서 제안한 사이버 공격의 위협에 대하여 모두 안전하게 방어하는 모습을 통해 제안한 방안의 타당성을 검증하였다. 또한 암호화 방식 보다 인증의 방식이 더 빠르다는 것을 입증하기 위하여 대표적인 보안 방식들의 시간비교를 하였다.

본 논문에서 제안한 적용방안이 배전자동화 시스템 또는 배전지능화 시스템에 적용된다면 시설물에 대한 물리적 공격을 제외한 사이버 공격에 대해서 우리의 배전계통안전을 지킬 수 있을 것이다.

또한 향후 배전자동화 시스템이 더 발전하여 이더넷 기반의 통신망을 사용하더라도 본 논문에서 제안한 적용방안을 통해 2.2절에서 언급한 보안 위협에 대해서는 방어가 가능할 것이다. 하지만 이더넷 기반의 통신망을 사용한다면 통신 구조도 변할 것이고, 본 논문에서 고려하지 못한 새로운 보안 위협들이 생길 수 있다. 현재로써는 배전자동화 시스템이 직렬통신기반의 시스템이기 때문에 본 논문에서는 직렬통신을 중심으로 사이버 공격에 대한 위협을 찾고 그 대안에 대해 연구를 진행하였다. 하지만 이더넷에 대한 보다 자세한 연구는 앞으로 배전자동화 시스템의 발달에 발맞추어 계속해서 연구가 진행되어야 할 것이다.

이제 더 이상 전력IT 산업에서 통신관련 기술을 통신만의 문제로 보는 시각이 아닌 전력 계통의 시각에서 함께 바라보고 연구를 진행해야 한다. 그 중 특히 보안 문제는 국내의 전력IT 산업에서 앞으로 본격적으로 연구가 시작되어야 할 분야라고 생각된다.

참 고 문 현

- [1] 임일형, 홍석원, 최면송, 이승재, 하복남, “배전지능화 시스템의 서비스 향상을 위한 P2P 기반의 분산형 통신망 구조”, 대한전기학회 논문집, 56권 3호 pp. 443-450, 2007.
- [2] Sanghun Jeon, “Critical Alert for Cyber Terror - Security for Nation’s Infrastructure(SCADA & DCS)”, 2002.
- [3] National SCADA Test Bed, “A Summary of Control System Security Standards Activities in the Energy Section”, 2005.
- [4] P. Oman, E. O. Schweitzer, III, and J. Roberts, “Safeguarding IEDs, substations, and SCADA systems against electronic intrusions”, 2005.
- [5] A. Creery and E. J. Byres, “Industrial Cybersecurity for Power System and SCADA Network”, Industry Application Magazine, IEEE, Vol 13:4, July-Aug. 2007.
- [6] Arturo Herrera, “NERC/CIP Security Standards : What you need to know to comply”, WPRC, Oct, 2007.
- [7] Rhett Smith, “Tutorial : Security in Electric Utility Control Systems”, WPRC, Oct, 2007
- [8] F. Cleveland, “IEC TC57 Secuirty Standards for the Power System’s Information Infrastructure – Beyond Simple Encryption”, 2005.
- [9] IEC technical committee 57, “Part 1: Communication network and system security - Introduction ti security issues”, IEC 52351-1, May 2007.
- [10] IEC technical committee 57, “Part 3: Communication network and system security - Communication network and system security - Profiles including TCP/IP”, IEC 62351-3, June 2007.
- [11] IEC technical committee 57, “Part 4: Communication network and system security - Profiles including MMS”, IEC 62351-4, June 2007.
- [12] IEC technical committee 57, “Part 6: Data and communication security - Security for IEC 61850”, June 2007.
- [13] IEC technical committee 57, “Part 5: Communication network and system security - Security for IEC 60870-5 and derivatives”, IEC 62351-5, February 2008.
- [14] T. Mander, F. Nabhani, L. Wang, and R. Cheung, “Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security”, Power Engineering Society General Meeting IEEE, June 2007.
- [15] R. Rivest and A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems”, Communications of the ACM, February 1978.
- [16] Krawczyk, H., Bellare, M., and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, February 1997.
- [17] R. Rivest, “The MD5 Message-Digest Algorithms”, RFC 1321, April 1992..
- [18] Eastlake, D. and T. Hansen, “US Secure Hash Algorithms(SHA)”, RFC 4634, July 2006.
- [19] “Secure Hash Standard”, (SHA-1/224/256/384/512) US Federal Information Processing Standard, with Change Notice 1, February 2004.
- [20] D. Harkins and D. Carrel, “The Internet Key Exchange(IKE)”, RFC 2409, November 1998.