한국정보전자통신기술학회논문지(jkiiect)'15-12, Vol.8 No.6
논문 15-08-06-534 http://dx.doi.org/10.17661/jkiiect.2015.8.6.534

스마트 그리드 환경에서 에너지 도둑 추적 프로토콜

정은희, 이병관, 안희학*

A Energy Theft Traceback Protocol in a Smart Grid Environment

Eun-Hee Jeong, Byung-Kwan Lee, Hui-Hak Ahn*

요 약 본 논문에서는 스마트 그리드 환경에서 에너지 도둑을 역추적 할 수 있는 로깅과 마킹 기반 에너지 도둑 역추적(Energy Theft Traceback Protocol) 프로토콜을 제안한다. 제안하는 ETTP는 첫째, 에너지 도둑 트리를 생성하여 측정 거부와 데이터위조로 구분하였고, 둘째, 에너지 도둑 트리를 이용하여 에너지 도둑을 탐지하고, 셋째 라우터의 Logging Table과 패킷의 Marking 정보를 이용하여 에너지 도둑을 역추적한다. ETTP의 모의 실험결과, 에너지 도둑 탐지율은 92%이고, 에너지도둑 역추적 성공률은 93%로 평가되었다. 따라서 ETTP는 스마트 그리드에 활용하여 과금 정보의 위변조 등의 위험요소를 줄일 수 있을 뿐만 아니라 안전하고 신뢰성이 높은 스마트 그리드 환경을 제공할 수 있다.

Abstract This paper proposes an Energy Theft Traceback Protocol(ETTP) based on Logging and Marking that can trace Energy Theft back in Smart Grid Environment. The ETTP consists of the following three phases. First, it classifies Energy Theft Type into Measurement Rejection and Data Fabrication by generating an Energy Theft Tree. Second, it detects an Energy Theft by using the Energy Theft Tree. Finally, it trace an Energy Theft back by using the Logging Table of a Router and the Marking Information of a Packet. The result of its simulation shows that the Detection Ratio of Energy Theft is estimated at 92% and the Success Ratio of Energy Theft Traceback at 93%. Therefore, the ETTP not only reduces such risk factors as Forgery and Tampering about Billing information but also provides safe and reliable Smart Grid environment.

Key Words : Energy Theft Traceback Protocol, Energy Theft Tree, Logging, Marking, Detection Ratio, Smart Grid

1. 서론

스마트 그리드(Smart Grid)는 현재의 중앙 집중형, 일반형인 전력 계통의 비효율성을 극복하기 위해 기존 전력망에 IT기술을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하고자 하는 차세대 전력망이다[1]. 특히, 소비자와 전력회사 간의 양방향 통신을 통해 원격검침과 같은 다양한 융·복합 서비스를 제공하는 AMI(Advanced Metering Infrastructure)가 기존의 네트워크 환경을 사용하기 때문에 DDoS 공격, 개인정보노출, 과금 정보 위/변조 등의 공격발생이 가능하다. 또한, 통신 취약점을 이용한 과금 정보 폭탄, 과금 전가에 따른 피해, 잘못된 수요반응 정보로 인해서 전력 계통이 불안정하게 되어 대규모 정전까지 발생할 수 있다[2][3][4].

본 논문에서는 AMI에 침입한 에너지 도둑을 분류하고, 에너지 도둑을 역추적하는 ETTP(Energy Theft Traceback Protocol)를 제안한다. 제안하는 ETTP는 에너지 도둑을 탐지하기 위해 에너지 도둑을 에너지 도둑 트리로 분류하고, 분류된 에너지

*Corresponding Author : Department of Computer Engineering, Catholic Kwandong University
Received November 24, 2015 Revised December 01, 2015 Accepted December 10, 2015

도둑의 위치를 Logging과 Marking 기법으로 역추적하는 프로토콜을 설계한다. 그리하여 ETTP는 에너지 도둑을 탐지할 뿐만 아니라 에너지 도둑을 역추적함으로써 안전하고 신뢰성이 높은 스마트 그리드 환경을 제공하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트 그리드와 역추적에 대한 관련연구를 살펴보고, 3장에서는 본 논문에서 제안하는 ETTP를 설계한다. 그리고 4장에서는 ETTP의 성능분석 결과를 설명하고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 AMI

스마트 그리드(smart grid)는 전기의 생산, 운반, 소비 과정에 정보통신기술을 접목하여 공급자와 소비자가 서로 상호작용함으로써 효율성을 높인 지능형 전력망시스템으로 AMI, 스마트 미터, 스마트 변전/배전/송전/시스템으로 구성된다. 특히 AMI는 전력의 공급자와 사용자 사이의 양방향 통신, 측정 및 자료수집을 가능하게 하는 시스템으로 정의되며, AMI의 범위는 스마트미터, 쌍방향 통신 인프라, 데이터관리 시스템(MDMS; Metering Data Management System)등으로 이루어진다. 데이터관리 시스템까지 데이터를 수집 및 전송하는 구간에서의 구성요소는 스마트미터, 집중기 또는 중계기, 데이터관리 시스템으로 구성된다. 통신기술은 범위에 따라 가정 및 건물 내외의 근거리 통신과 MSMD까지의 원거리 통신으로 구분될 수 있다. 근거리 통신방식은 RS-485, Ethernet, PLC(Power Line Communication)과 같은 유선방식과 Zgbee, RF, Wi-Fi 등이 사용되고 있으며, 원거리 통신으로는 3G, Wibro, LTE와 같은 무선방식과 Ethernet을 통한 유선 인터넷 방식을 활용하고 있다[2][3][4].

본 논문에서는 스마트 미터가 전력회사에 전송하는 패킷이 경유하는 라우터에 패킷 정보를 저장하는 Logging 기법과 패킷에 패킷 전송 경로를 저장하는 Marking 기법을 제안하여 에너지 도둑의 위치를 역추적 하고자 한다.

2.2 확률적 패킷 마킹 기법

확률적 패킷 마킹 기법(Probability Packet Marking)[5]은 네트워크를 구성하는 라우터에서 자신을 지나는 패킷에 라우터 정보를 삽입하여 스푸핑된 패킷의 실제 경로를 찾는 방법으로 라우터에서는 패킷 IP헤더에 자신의 IP주소를 마킹하여 다음 라우터에 전송한다. 그러나 라우터는 엄청난 양의 패킷을 전달하므로 역추적 정보를 모든 패킷에 대해 마킹하게 되면 라우터에 많은 오버헤드가 발생하게 되므로 통신에 지연 및 장애가 발생할 수 있다. 그리하여 PPM은 일정한 확률로 패킷을 샘플링하는 Node sampling, Edge sampling, Advanced marking 등이 있다[6][7].

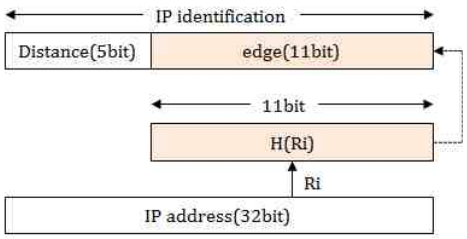

그림 1. IP 인식 필드 구조
Fig. 1. IP identification field structure

Advanced Marking Scheme기법은 그림 1과 같이 IP 식별자 필드 16비트를 마킹 필드로 사용하며 라우터까지의 거리를 나타내는 5비트의 거리 필드와 11비트의 edge 필드로 구분한다. 5비트의 거리필드는 32홉을 표시할 수 있으므로 인터넷 경로들을 충분히 나타낼 수 있다. 패킷의 IP 식별자 필드에 32비트의 라우터 주소를 hash함수를 이용하여 11비트로 암호화한 후 마킹하게 된다. 그 후 각 라우터를 경유할 때마다 XOR 연산을 통해 라우터의 정보를 암호화하여 마킹하게 되고, 공격경로를 재설정하게 된다[8][9].

본 논문에서는 향상된 패킷 마킹의 기법의 IP 인식필드를 Marking, Logging한 카운트 값, 이전 라우터 주소, 그리고 에지 값으로 구조 변경하여

패킷 정보를 기록하고, 에너지 도둑을 탐지되면 패킷의 이 헤더 정보를 이용하여 공격 경로를 재구성하여 공격자의 위치를 역추적 하고자 한다.

3. ETTP 설계

본 논문에서 제안하는 ETTP는 AMI가 전력회사, 스마트 미터, 스마트 미터를 관리하는 유틸리티, 라우터로 구성된다고 가정한다. 그리고 ETTP는 그림 2에서 설명하고 있듯이 스마트 미터를 전력회사에 등록하고 스마트 미터와 전력회사간의 암호화키를 생성하는 SMM(Smart meter Management Module), AMI에서 발생할 수 있는 에너지 도둑에 대한 에너지 도둑 트리(Energy Theft Tree)를 생성하고, 이 에너지 도둑 트리(ETT)를 이용하여 에너지 도둑을 탐지하는 ETDM(Energy Theft Detection Module), 그리고 Logging과 Marking기법으로 에너지 도둑을 역추적하는 TSM(Traceback Server Module)와 TRM(Traceback Router Module)로 구성된다.

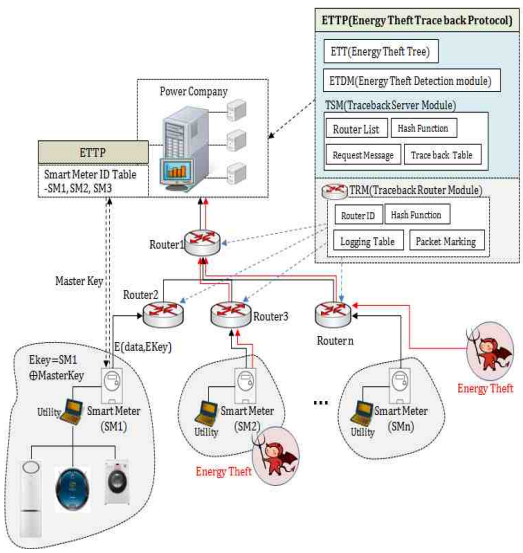

그림 2. ETTP 구성요소
Fig. 2. ETTP component

3.1 스마트 미터 관리 모듈(SMM) 설계

Smart meter에는 고유 ID가 등록되어 있고, 그림 3과 같이 Smart meter를 설치할 때 Smart meter의 ID, 설정된 장소, 고객 등의 정보를 전력회사에 등록시킨다.

① Smart meter가 자신의 ID(SM1)를 해시하여 전력회사에 전달한다.

② 전력회사는 Smart meter의 ID가 전력회사 DB에 저장되어 있는지 확인한다.

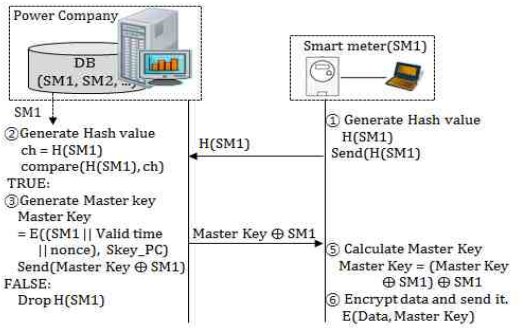

그림 3. Smart meter 확인 및 마스터 키 생성
Fig. 3. Smart meter verification and Mater Key generation

③ 전력회사는 Smart meter의 ID가 DB에 존재하면, 전력회사에 등록된 Smart meter로 판단하고, 전력회사는 SM1, 유효기간, nonce를 전력회사의 비밀키로 암호화하여 Master Key를 생성한다.

이때, 전력회사는 nonce를 주기적으로 변경함으로써 Master Key를 주기적으로 새로 생성한다. 그리하여 전력회사는 Master key의 노출로 인한 프라이버시 침해, 데이터 위조와 변조 등의 보안 문제들을 예방한다.

$$\text{Master Key} = E(\text{SM1} \,||\, \text{valid time} \,||\, \text{nonce}, \text{비밀키})$$

④ 전력회사는 Master Key를 SM1로 XOR연산을 한 후에 AMI에 전달한다.

$$(\text{Master Key} \oplus \text{SM1})$$

⑤ Smart meter는 SM1를 한번 더 XOR 연산을 하여 전달받은 Master key를 추출한다. 그리고 에너지 정보를 Master Key로 암호화하여 전력회사에 전달한다.

Master Key = (Master Key ⊕ SM1)
⊕ SM1
E(Data, Master Key)

⑥ 전력회사는 암호화된 데이터를 Master Key로 복호화하여 Smart meter가 전달한 데이터를 확인한다.

3.2 에너지 도둑 트리(ETT) 설계

에너지를 훔치는 가장 간단한 방법은 사용된 에너지의 수요량을 위조하는 것이다. 에너지 수요량을 위조하는 방법으로는 Smart Meter에 수요량을 기록할 때, Smart Meter의 데이터를 네트워크를 이용해 수요 데이터를 전송할 때, 서버에 저장되어 있는 데이터를 위조하는 등의 여러 가지 방법이 있다.

본 논문에서는 [9]의 attack tree를 이용하여 수요 데이터를 조작하는 방법에 따라 고객의 에너지 수요 및 공급에 대한 정보를 위조하여 에너지를 훔쳐가는 방법을 OR 연산자를 이용하여 효율적으로 찾을 수 있는 에너지 도둑 트리(Energy Theft Tree)를 설계하였다.

제안하는 ETT는 그림 4와 같이 에너지 도둑을 크게 측정거부와 사용량 위조로 분류한다[7].

첫째, 측정거부는 Smart meter 차단과 통신차단으로 분류하고, Smart meter 차단은 Smart meter의 전원 차단 또는 Smart meter를 관리하는 유틸리티 종료로 분류한다.

둘째, 사용량 위조는 log 기록 삭제/수정과 트래픽 주입으로 분류한다. 그리고 log 기록 삭제/수정은 Smart meter와 전력회사에서 각각 발생할 수 있으므로 Smart meter와 전력회사로 분류한다.

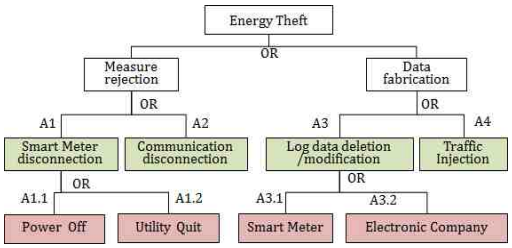

그림 4. 에너지 도둑 트리
Fig. 4. Energy Theft Tree(ETT)

3.2 에너지 도둑 탐지 모듈(ETDM) 설계

ETTP의 에너지 도둑 탐지 모듈(Energy Theft Detection Module)은 에너지 도둑 트리에서 분류한 에너지 도둑의 유형별로 에너지 도둑을 탐지한다. 그림 5는 ETDM의 흐름도를 설명한 것이다[7].

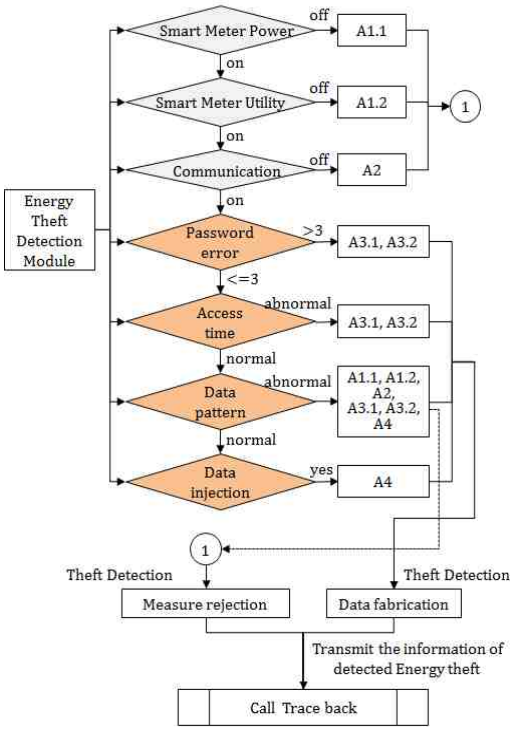

그림 5. 에너지 도둑 탐지 모듈 절차
Fig. 5. The flowchart of energy theft detection module

1) 측정 거부 도둑 탐지

ETDM은 고객이 직접 Smart Meter 전원을 차단(A1.1)하거나 Smart Meter Utility 프로그램을 종료(A1.2)시킴으로써 전력사용량에 대한 정보를 전달하지 않을 경우 측정거부로 판단한다. 또한, ETDM은 공격자에 의해 Smart Meter와 전력회사 사이와의 통신을 차단(A2)되는 경우에도 측정거부로 판단한다. ETDM은 Smart Meter의 연결상태를 주기적으로 확인하고, Smart Meter의 수요량의 패턴을 분석하여 Smart Meter 상태를 파악함으로써 측정 거부를 탐지한다[7].

2) 데이터 위조 도둑 탐지

Smart Meter의 유틸리티는 패스워드 오류 횟수가 3회 이상, 근무시간 외의 접속 시도, 에너지 사용량의 패턴의 변화 등과 같은 비정상적인 동작이 감지가 되었을 경우에 Smart Meter log 파일을 전력회사에 전달한다. ETDM은 Smart Meter로부터 전달받은 Smart Meter log 파일(A3.1)을 분석하여 데이터 위조공격을 탐지 할뿐만 아니라 Smart Meter가 전송한 데이터의 패턴을 분석하여 해커의 트래픽 주입(injection) 공격을 탐지한다. 또한, ETDM은 전력회사의 비정상적인 동작이 감지되었을 때에도 전력회사의 log 파일(A3.2)을 분석하여 데이터 위조 도둑을 탐지한다[7].

3.3 TSM과 TRM 설계

본 논문에서 제안하는 ETTP는 에너지 도둑을 역추적하기위해 전력회사에 설치되는 TSM(Traceback Server Module)와 각 라우터에 설치되는 TRM(Traceback Router Module)를 포함하고 있다. 에너지 도둑을 탐지한 ETTP는 전력회사의 TSM을 실행하여 역추적 메시지를 생성하여 라우터에 전달하면, 라우터는 라우터 TRM을 실행하여 에너지 도둑이 라우터를 경유했는지를 확인한다. 그리고 라우터는 그 결과를 전력회사에 전달함으로써 에너지 도둑의 공격 경로와 위치를 역추적한다.

3.3.1 TRM 설계

본 논문에서 제안하는 라우터는 그림 6에서 설명하고 있듯이 라우터 ID, 해시함수, Logging table, Marking, 응답메시지, 라우터를 관리하는 TRM으로 구성된다. TRM은 라우터를 경유하는 패킷에 marking을 하고 라우터의 logging table에 패킷 정보를 저장한다. 그리고 TRM은 공격패킷의 경로를 역추적할 때, TRM은 logging table을 분석하여 공격패킷이 라우터를 경유했는지 확인한 후 응답메시지를 생성하여 TSM에 전달한다.

1) Marking

라우터의 TRM은 자신을 경유하는 패킷의 ML_count가 3의 배수가 아니면 Marking 작업만을 수행한다. TRM이 Marking 작업을 수행하는 경우, TRM은 패킷의 Last_RID 필드에는 현재 라우터 ID를 기록하고, 패킷의 edge 필드에는 edge 필드의 값과 Last_RID 필드의 Router ID를 XOR 연산한 결과 값을 기록한다. 그리고 TRM은 ML_count 필드의 값에 1을 더하여 ML_count 필드에 저장한 후에 이 패킷을 다음 Router에 전달한다.

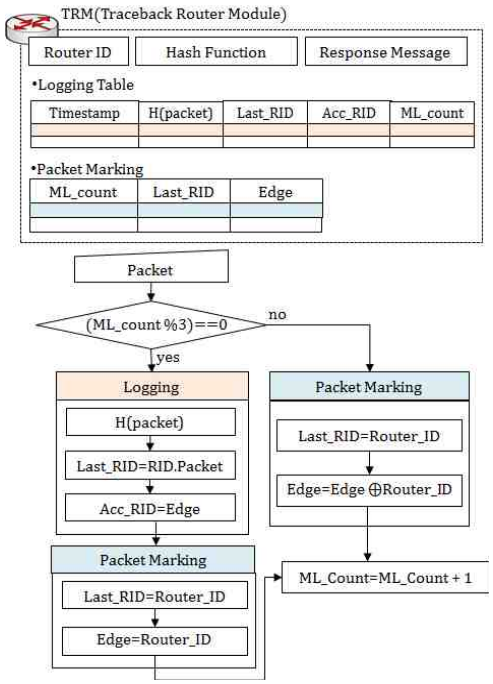

그림 6. TRM 구성 요소와 로깅과 마킹의 흐름도

Fig. 6. TRM component and flowchart of Logging and Marking

그림 7은 packet marking의 구조를 설명한 것이다.

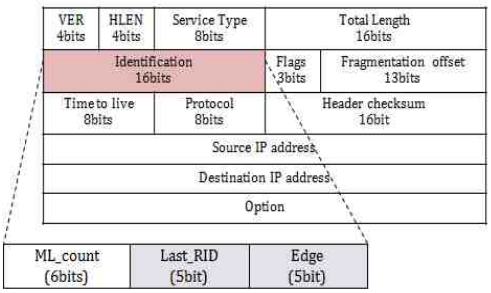

그림 7. 패킷 마킹의 구조
Fig. 7. Structure of packet marking

2) Logging

라우터의 TRM은 자신을 경유하는 패킷의 ML_count가 3의 배수이면 Logging 작업과 Marking 작업을 순서대로 수행한다. 이때, TRM은 Logging Table의 Timestamp 필드에는 패킷 정보 기록시간을 기록하고, Last_RID 필드에는 패킷을 전달한 라우터 ID를 기록하고, Acc_RID 필드에는 패킷의 edge 필드 값과 현재 라우터 ID와 XOR 연산한 결과 값을 기록하고, 패킷을 해시한 값을 value 필드에 기록한다. TRM은 패킷의 Last_RID 필드와 Edge 필드에는 현재 라우터 ID를 각각 기록한다. 그리고 난 후에 TRM은 ML_counter를 1을 증가한 후에 패킷의 ML_count 필드와 Logging Tabled의 ML_count필드에 각각 저장하고, 이 패킷을 다음 라우터에 전달한다.

그림 8은 TRM이 Marking과 Logging 작업을 판단하여 수행하는 과정을 예를 들어 설명한 것이고, 표 1은 그림 8에 대한 Marking과 Logging 작업 결과를 설명한 것이다.

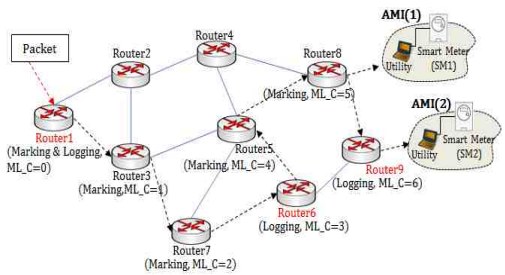

그림 8. 마킹과 로깅의 예
Fig. 8. The example of marking and logging

패킷이 Router1의 시작으로 하여 전력회사로 전송된다고 할 때, Router1은 패킷이 처음 경유하는 라우터이기 때문에 TRM은 Logging과 Marking 작업을 순서대로 진행한다. TRM은 Logging Table의 Last_RID 필드와 Acc_RID 필드에 현재 라우터 ID인 “1”을 각각 기록하고, 패킷의 Last_RID 필드와 edge필드에도 현재 라우터 ID인 “1”을 각각 기록한다. TRM은 ML_count를 1 증가시켜(ML_count=1) Logging Table과 Packet의 ML_count 필드에 각각 기록한다. 그리고 난 후에 TRM은 이 패킷을 다음 라우터인 Router3에 전달한다.

패킷을 전달받은 Router3의 TRM은 패킷의 Last_RID 필드에 라우터3의 ID인 “3”을 기록하고, edge 필드에는 패킷의 edge 필드 값인 “1”과 Router3의 ID인 “3”을 XOR 연산한 결과 값을 기록하고, 패킷의 ML_count 필드 값에 1을 더한 결과 값(ML_count=2)을 ML_count 필드에 기록한다. 그리고 TRM은 이 패킷을 다음 라우터인 Router7에 전달한다.

표 1. Marking과 logging의 결과
Table 1. The result of marking and logging

	Marking/ Logging	Last _RID	Edge	Acc _RID	ML_ Count
Router 1	Logging	1	-	1	1
	Marking	1	1		
Router 3	Marking	3	1 XOR 3		2
Router 7	Marking	7	1 XOR 3 XOR 7		3
Router 6	Logging	7	-	1 XOR 3 XOR 7	4
	Marking	6	6		
Router 5	Marking	5	6 XOR 5		5
Router 8	Marking	8	6 XOR 5 XOR 8		6
Router 9	Logging	8	-	6 XOR 5 XOR 8	7
	Marking	9	9		

패킷을 전달받은 Router7의 TRM은 라우터 3과 같은 방법으로 패킷을 마킹 작업을 한 후에 다음 라우터인 Router6에 전달한다.

패킷을 전달받은 Router6의 TRM은 ML_count가 3의 배수이므로 Logging 작업과 Marking 작업을 차례대로 수행한다. 즉, TRM은 Logging Table의 Last_RID필드에는 패킷의 Last_RID 필드 값인 “7”을 기록하고, Logging Table의 Acc_RID 필드에는 전달받은 패킷의 Edge 필드 값을 기록한다. 그리고 TRM은 패킷의 Last_RID 필드와 Edge 필드에는 각각 “6”과 “6”을 기록하고, ML_count 필드 값을 1 증가(ML_count=4)시켜 Logging Table과 패킷의 ML_count 필드에 기록한다. 그리고 난후에 TRM은 다음 라우터인 Router5에 이 패킷을 전달한다.

패킷을 전달받은 Router5의 TRM은 ML_count가 3의 배수가 아니므로 Logging 작업을 수행하지 않고, Marking 작업만을 수행한다. 즉, 패킷의 Last_RID필드에는 현재 라우터의 ID인 “5”를 기록하고, Edge 필드에는 Edge 필드 값인 “6”과 현재 라우터 ID인 “5”을 XOR 연산한 결과 값을 기록하고, ML_count 필드 값을 1만큼 증가시켜 (ML_count=5) ML_count 필드에 기록한다. 그리고 난 후 TRM은 이 패킷을 다음 라우터인 Router8에 전달한다.

패킷을 전달받은 Router8의 TRM은 ML_count가 3의 배수가 아니므로 Logging 작업을 수행하지 않고, Marking 작업만을 수행한다. 즉, TRM은 패킷의 Last_RID필드에는 현재 라우터의 ID인 “8”를 기록하고, Acc_RID 필드에는 Acc_RID 필드 값인 “6 XOR 5”와 현재 라우터 ID인 “8”을 XOR 연산한 결과 값을 기록한다. 그리고 TRM은 ML_count 필드 값을 1만큼 증가한 후에 (ML_count=6) ML_count 필드에 기록하고, 다음 라우터인 Router9에 이 패킷을 전달한다.

패킷을 전달받은 Router9의 TRM은 ML_count가 3의 배수이므로 Logging 작업과 Marking 작업을 차례대로 수행한다. 즉, Logging Table의 Last_RID필드에는 패킷의 Last_RID 필드 값인 “8”을 기록하고, Logging Table의 Acc_RID 필드에는 전달받은 패킷의 Edge 필드 값인 ″6 XOR 5 XOR 8″을 기록한다. 그리고 TRM은 패킷의 Last_RID 필드와 Edge 필드에는 각각 “9”과 “9”을 기록하고, ML_count 필드 값을 1 증가(ML_count=7)시키고, Logging Table과 패킷의 ML_count 필드에 각각 기록한 후에 목적지에 이 패킷을 전달한다.

3.3.2 TSM 설계

본 논문에서는 전력회사가 에너지 도둑 탐지 모듈을 이용하여 에너지 도둑을 탐지한 경우, 전력회사가 TSM을 실행하여 에너지 도둑을 역추적 한다.

TSM은 전력회사가 수신한 공격 패킷을 Hash 함수로 해시하고, 이 해시값을 이용해 역추적 요청 메시지를 생성한다. 그리고 TSM은 이 메시지를 전력회사가 관리하고 있는 Router에게 배포한다.

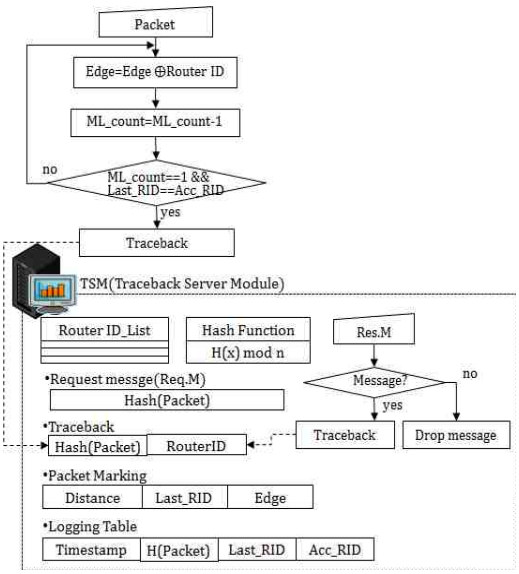

그림 9. TSM 구성 요소와 역추적 절차
Fig. 9. TSM component and traceback procedure

역추적 요청 메시지를 전달받은 라우터는 TRM을 실행하여 이 패킷은 라우터를 경유하였는지를 확인하고, 이 패킷이 라우터를 경유하였다면, 역추적 응답메시지(Res.M)를 전력회사에게 전달한다. 전력회사는 전달받은 역추적 응답 메시지

를 재구성하여 에너지 도둑의 위치를 추적한다. 즉, TSM은 Marking된 패킷과 Logging Table의 정보를 이용하여 공격패킷의 경로를 역추적함으로써 에너지 도둑의 위치를 추적한다.

1) Marking된 패킷과 Logging Table을 이용한 역경로 생성

①전력회사의 ETDM(Energy Theft Dection Module)로부터 에너지 도둑이 탐지되었음을 전달받으면, TSM을 실행하여 에너지 도둑을 역추적한다. 즉, TSM은 에너지 도둑이 전달한 패킷이 경유한 라우터를 다음과 같이 역추적함으로써 에너지 도둑의 위치를 찾는다.

전력회사의 ETDM은 Router9로부터 전달받은 패킷을 에너지 도둑이 전달한 패킷으로 판단한다. 그리고 난 후에, 전력회사는 에너지 도둑의 위치를 역추적하기 위해 TSM을 실행한다. TSM은 TSM의 Traceback Table에 해시함수로 패킷을 해시한 결과값과 라우터 ID인 Router9를 기록하고, 요청메시지를 Router에 배포한다.

Request.Message(H(packet))

②요청메시지를 전달받은 Router9의 TRM은 H(packet)이 Logging Table에 있는지 확인한다. 이때 Logging Table에 H(packet)이 존재하면, Router9의 TRM은 해당 정보를 TSM에 전달한다. 즉, Router9의 TRM은 Logging Table의 {timestamp, H(packet), Last_RID, Acc_RID, ML_count}로 구성된 응답메시지를 TSM에 전달한다.

Response.Message(timestamp, H(packet), Last_RID, Acc_RID, ML_count) = Response.Message(timestamp, H(packet), 8, 6 XOR 5 XOR 8, 7)

③ TSM은 Router8을 Traceback Table에 저장하고, 전달받은 “8, 6 XOR 5 XOR 8”를 XOR 연산하여 “6 XOR 5″ 결과 값을 산출한다. 그리고 난 후, TSM은 이 산출 결과 값과 자신이 관리하는 Router ID를 XOR 연산하여 Router5와 Router6을 찾는다.

④ TSM은 Router5와 Router6에게 요청메시지를 전달하여 Router5와 Router6의 Logging Table에 기록되어 있는지를 확인을 요청한다.

⑤ Router5와 Router6은 Logging Table을 확인한 후에, 그 결과를 TSM에 전달한다.

Router5의 응답메시지: Response.Message(no)

Router6의 응답메시지: Response.Message(timestamp, H(packet),7,1 XOR 3 XOR 7)

⑥ TSM은 Router5, Router6, Router7을 차례대로 Traceback Table에 저장하고, 전달받은 ″7, 1 XOR 3 XOR 7″를 XOR 연산하여 “1 XOR 3 ″ 결과 값을 산출한다. 그리고 난 후, TSM은 이 산출 결과 값과 자신이 관리하는 Router ID를 XOR 연산하여 Router1와 Router3을 찾는다.

⑦ TSM은 Router1와 Router3에게 요청메시지를 전달하여 Router1와 Router3의 Logging Table에 기록되어 있는지를 확인을 요청한다.

⑧ Router1과 Router3은 Logging Table을 확인한 후에, 그 결과를 TSM에 전달한다.

Router3의 응답메시지: Response.Message(no)

Router1의 응답메시지: Response.Message(timestamp, H(packet),1,1)

⑨ TSM은 Router3, Router1을 차례대로 Traceback Table에 저장하고, 공격 패킷의 경로를 Router9 → Router8 → Router5 → Router6 → Router7 → Router3 → Router1로 역추적한다.

4. 분석

본 논문에서는 ETT로 에너지 도둑을 탐지하고, Logging과 Marking 기법을 이용하여 에너지 도둑을 추적하는 ETTP를 제안하였다.

ETTP의 역추적의 실험은 ns-2 시뮬레이터를 이용하였으며, 실험을 위한 그림 10과 같이 라우터의 위치를 설정하였으며, 파라미터 설정은 표 2와 같다.

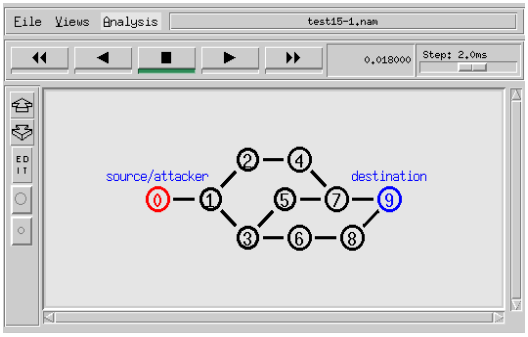

그림 10. 노드의 위치
Fig. 10. The position of nodes

표 2. 시뮬레이션 파라미터
Table 2. The parametrs of simulation

Parameters	Values
traffic type	CBR
the number of nodes	11
Simulation times	60 seconds
packet size	500 bytes
packet interval time	0.5 sec
근원지 노드(공격 노드)	0
목적지 노드	9
패킷 전송 경로(경로1)	0-1-2-4-7-9
패킷 전송 경로(경로2)	0-1-3-6-8-9
패킷 전송 경로(경로3)	0-1-3-5-7-9

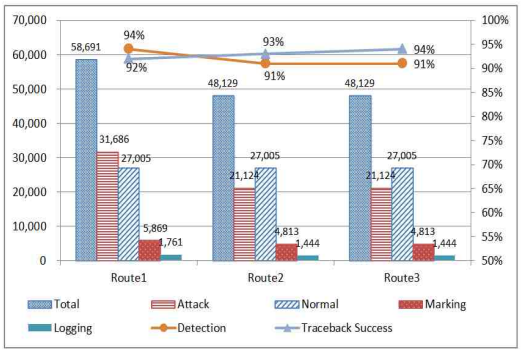

그림 11. 에너지 도둑 추적의 모의실험 결과
Fig. 11. The simulation result of Energy Theft Traceback

실험은 근원지 라우터와 에너지 도둑을 0, 목적지 노드는 9로 설정하였고, 패킷들은 표 3의 패킷 전송 경로를 통해 목적지에 도착하도록 진행하였다. 그리고 에너지 도둑 역추적 모듈은 공격패킷의 전송 경로를 역추적하고, 역추적한 공격 패킷 경로의 정확도를 평가하였다. 실험 결과 그림 11과 같이 공격 탐지율의 94%, 91%, 91%으로 평균 92%이고, Logging과 Marking한 패킷을 이용한 역추적 성공률을 92%, 93%, 94%로 평균 93%로 나타났다.

5. 결론

본 논문에서는 AMI에서 발생하는 에너지 도둑을 탐지하고 역추적 할 수 있는 ETTP를 제안하였다. 제안한 ETTP의 특징은 첫째, 에너지 도둑을 트리 형태로 분류하고, 이 에너지 도둑 트리를 이용하여 에너지 도둑을 탐지하는 에너지 도둑 탐지(Energy Theft Detection) 모듈을 설계하였다.

둘째, ETTP는 탐지된 에너지 도둑과 공격자의 위치를 역추적하는 에너지 도둑 역추적(Energy Theft Traceback) 모듈을 설계하였다.

셋째, 에너지 도둑 역추적 모듈은 패킷에 패킷의 전송 경로를 Marking하거나 라우터의 Logging 테이블에 저장하도록 설계하였다.

그리하여 Logging과 Marking 정보를 이용하는 ETTP는 에너지 도둑의 탐지율이 평균 92%이고, 에너지 도둑의 역추적율은 평균 93%로 평가되었다.

따라서 ETTP는 스마트 그리드에 활용하여 에너지 도둑을 탐지할 뿐만 아니라 에너지 도둑을 역추적함으로써 안전하고 신뢰성이 높은 스마트 그리드 환경을 제공할 수 있다.

REFERENCES

[1] D. G. Kim, “The concept of a Smart Grid”, Journal of the society of naval architects of Korea, vol.50, no.1, pp.45-49, 2013.

[2] Y. J. Jang and J. Kwak, “Group Key Management Mechanism for Secure Device in AMI Environment”, Journal of Korea Navigation Institute, vol.16, no.4, pp.679-686, 2012

[3] J. J. Lee, “AMI Technology Trends”, Proceedings of the Korean Institute of Illuminating and Electrical Installation Engineers, vol.23, no.6, pp.27-31, 2009.

[4] http://news.koita.or.kr/rb/?c=1/8&uid=1112
[5] S. Savage, D. Wtherall, A. Karlin and T. Anderson, “Practical Network Support for IP Traceback”, Proceedings of ACM SIGCOMM2000, August 28-September 1, 2000, Stockholm, Sweden.
[6] D. X. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback”, Processing of INFOCOM2001, April 22-26, 2001, Anchorage, AK.
[7] E. H. Jeong and B. K. Lee, “A Design of ETDTP(Energy Theft Detection and Traceback Protocol) for AMI(Advanced Metering Infrastructure) of Smart Grid”, Journal of Security Engineering, Vol.11, No.6, pp.535-550, 2014.
[8] S. Y. Won, S. W. Han, D. I. Seo, S. Y. Kim, C. S. Oh, “Hacking Path Retracing Algorithm using Packet Marking,” Journal of the Korea Contents Association, vol.3 no.1, pp.21-30, 2003.
[9] J. Heo, C. S. Hong and H. J. Lee, “Lightweight IP traceback mechanism”, The KIPS transactions: Part C, vol.14-C, no.1, pp.17-26, 2007.
[10] Bruce Schneier, “Attack trees”, Dr Dobb’s Journal, vol. 24, no.12, pp.21-29, 1999.

저자약력

정 은 희(Eun-Hee Jeong) [종신회원]

- 1998년 2월 : 관동대학교 컴퓨터공학과 (공학석사)
- 2003년 2월 : 관동대학교 컴퓨터공학과 (공학박사)
- 2003년 9월 ~ 현재 : 강원대학교 지역경제학과 교수

<관심분야> 전자상거래 보안, 빅데이터, 헬스케어, IoT

이 병 관(Byung-Kwan Lee) [종신회원]

- 1986년 2월 : 중앙대학교 전자계산공학과 (공학석사)
- 1990년 2월 : 중앙대학교 전자계산공학과 (공학박사)
- 1988년 3월 ~ 현재 : 가톨릭관동대학교 컴퓨터공학과 교수

<관심분야> 네트워크 보안, 빅데이터, 데이터 마이닝, IoT

안 희 학(Hui-Hak Ahn) [정회원]

- 1983년 2월 : 숭실대학교 전자계산공학과 (공학석사)
- 1994년 2월 : 숭실대학교 전자계산공학과 (공학박사)
- 1984년 3월 ~ 현재 : 가톨릭관동대학교 컴퓨터공학과 교수

<관심분야> 시스템소프트웨어, 정보보안, 오토마타