情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

스마트그리드 네트워크에서 가용성 보장 메커니즘에 관한 연구: 신호정보를 이용한 공격 및 공격노드 검출*

김 미 희† ‡
한경대학교 컴퓨터웹정보공학과

Study on Availability Guarantee Mechanism on Smart Grid Networks: Detection of Attack and Anomaly Node Using Signal Information*

Mihui Kim† ‡
Hankyong National University, Department of Computer&Web Information Engineering

요 약

최근 전력 수요의 급증으로 인한 전력난은 효율적 전력 사용을 위한 스마트그리드 기술의 중요성을 부각시키고 있다. 스마트그리드 네트워크의 필수구성요소인 스마트미터기의 가용성 취약점에 대한 실험적 내용이 보고되고 있다. 따라서 안전한 스마트그리드의 실현가능성을 위한 가용성 보호 메커니즘 고안이 필수불가결하다. 본 논문에서는 스마트그리드 구조 및 트래픽패턴의 특징 분석을 통해 스마트미터기에 대한 가용성 침해 공격을 탐지하고, 이상 트래픽을 발생하는 공격노드를 검출할 수 있는 메커니즘을 제안한다. 제안하는 탐지 메커니즘은 공격 탐지를 수행하는 시스템의 탐지 부하를 줄이고 적은 샘플 수에도 높은 탐지율을 제공하기 위해 근사엔트로피 기법을 사용한다. 또한 공격노드가 공격트래픽에서 변경할 수 없는 물리정보(CIR 또는 RSSI 등)를 이용하여 공격 탐지 및 공격노드 검출을 수행한다. 마지막으로 본 논문 제안 기법에 대한 시뮬레이션 결과, 탐지 성능과 실현가능성을 보인다.

ABSTRACT

The recent power shortages due to surge in demand for electricity highlights the importance of smart grid technologies for efficient use of power. The experimental content for vulnerability against availability of smart meter, an essential component in smart grid networks, has been reported. Designing availability protection mechanism to boost the realization possibilities of the secure smart grid is essential. In this paper, we propose a mechanism to detect the availability infringement attack for smart meter and also to find anomaly nodes through analyzing smart grid structure and traffic patterns. The proposed detection mechanism uses approximate entropy technique to decrease the detection load and increase the detection rate with few samples and utilizes the signal information(CIR or RSSI, etc.) that the anomaly node can not be changed to find the anomaly nodes. Finally simulation results of proposed method show that the detection performance and the feasibility.

Keywords: Availability Guarantee, Smart Grid, Smart Meter, Attack Detection, Anomaly Node Detection, Signal Information

접수일(2013년 2월 15일), 수정일(2013년 4월 8일), 게재확정일(2013년 4월 9일)
* 본 연구는 한경대학교 2011년도 학술연구조성비의 지원에 의한 것임

† 주저자, mhkim@hknu.ac.kr
‡ 교신저자, mhkim@hknu.ac.kr

I. 서 론

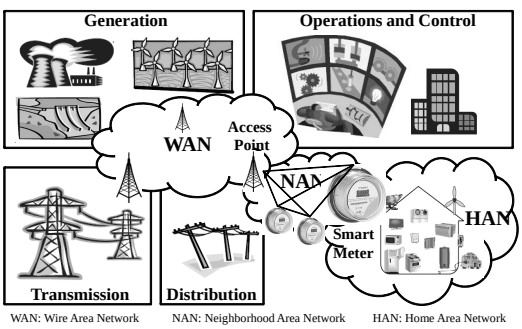
최근 전세계적인 관심이 집중되고 있는 차세대 성장동력인 스마트그리드 기술은 기존의 전력망과 IT의 융합을 통해 전력시스템의 효율적인 생산과 소비를 유도할 것으로 기대되고 있다. 그림 1과 같이 계층적으로 구성된 스마트그리드 네트워크는 송전/배전용 변전소뿐 아니라 말단 홈네트워크의 스마트미터기까지 양방향 네트워크로 연결되어 있다. 스마트미터기는 댁내 또는 기업의 효율적 에너지 사용과 재생산에 허브역할을 수행할 중요 기기로서 실시간 전력 소비량의 주기적 보고(report) 및 관리를 수행한다. 따라서 해당 기기의 정보 오류 및 이상행동을 야기하는 가용성 침해는 홈네트워크 뿐만 아니라 전체 에너지공급시스템에 커다란 영향을 끼칠 수 있다. 특히 이 기기에 대한 용이한 보안 침해 및 파급효과에 대한 실험적 결과는 가용성 보장에 대한 메커니즘 고안의 필요성을 뒷받침하고 있다[2].

그림 1과 같이 스마트미터기는 HAN(Home Area Network)에서 다양한 스마트기기 및 가정용 에너지 생성/축적 장치의 정보 수집의 중심 역할을 수행하고, NAN(Neighbor Area Network)에서 다수의 스마트미터기가 트리 또는 메쉬 형태로 연결되어 WAN(Wide Area Network)에 접속되는 구조를 갖는다. 이러한 NAN은 메쉬네트워크와 유사 구조를 보이고 있으나, 주기적 상향 미터링 트래픽과 간헐적 하향 관리/제어 트래픽이 주를 이루고 있어 트래픽 패턴이 다르다. 이에 네트워크 구조와 트래픽 패턴에 적합한 탐지 메커니즘 고안이 필수적이다.

본 논문에서는 스마트미터기에 대한 가용성 침해 공격을 탐지하고 그 공격노드를 탐지할 수 있는 가용성 보장 연구를 수행한다. 해당 공격노드는 합법적인 노드가 위협당해(compromised) 공격 트래픽을 발생하는 내부공격과 외부에서 합법적인 노드를 가장하여 공격트래픽을 발생하는 외부공격을 모두 탐지할 수 있다. 본 논문에서 제안한 탐지 메커니즘의 목표는 다음과 같다: **낮은 처리비용, 높은 탐지율, 공격노드 검출.**

- 낮은 처리비용: 스마트그리드 HAN에서 저전력이 요구되고, 제약된 리소스를 가지고 있는 센서노드, 스마트기기, 스마트미터기 등에서도 수행될 수 있고, 제어 관리하는 스마트미터기의 수가 많은 경우에도 낮은 처리비용이 요구되는 탐지 모델을 사용한다.
- 높은 탐지율: 변조하기 힘든 정보를 사용하고, 적은 양의 샘플링 데이터로도 높은 탐지율을 제공한다.
- 공격노드 검출

본 논문의 구성은 다음과 같다. 2장에서는 기반 연구내용을 소개하고, 3장에서는 본 논문에서 제안하는 신호정보를 이용한 공격 및 공격노드 검출 방법을 설명한다. 4장에서는 제안한 기법의 성능을 시뮬레이션을 통해 입증하며, 5장에서 결론을 맺는다.



〔그림 1〕 스마트그리드 네트워크 구조[1]

II. 기반 연구

2.1 스마트그리드 네트워크 구조, 기능, 트래픽 특징

스마트그리드 네트워크는 그림 1과 같이 HAN/NAN/WAN의 3 멀티티어 구조로 구성되어 있다. 각 네트워크의 특징은 다음과 같다.

HAN은 다양한 센서를 장착한 가전기기와 스마트 장치들, 가정용 에너지 생성 장치 및 축적장치 등이 외부와의 통신 창구인 스마트미터기를 중심으로 하나의 네트워크를 구성하고 있다.

- 스마트 장치: 전기요금이 싼 시간대만 작동하는 스마트 가전도구, 전기 사용량이 과도할 경우 스스로 온도를 조절 하는 스마트 온도계, 자기 집의 에너지 정보를 얻고, 통제할 수 있는 온라인 에너지 관리 시스템
- 가정용 에너지 생성 및 축적장치: 태양광, 풍력 등 신 재생에너지를 생성하고, 플러그인 하이브리드 전기차 등을 에너지 저장 도구로 이용
- 스마트미터기: 스마트 장치의 실시간 전기 사용량, 에너지 생성 장치/축정장치의 전기량 측정 및 보고, 양방향 통신이 가능하도록 설계된 핵심 기기

NAN은 스마트미터기를 중심으로 구성된 HAN들이 WAN에 접속되기 전에 메쉬 또는 트리 구조로 구성된 네트워크이다. WAN은 HAN과 NAN을 에너지 생성/분배 시스템, 스마트그리드 데이터/제어 센터, 에너지공급업자 및 시스템운영업자의 관리 시스템과 연결하기 위해 제공되는 광역 네트워크이다.

그림 1에 기반 한 스마트그리드 네트워크에서 제공되는 기능은 다음과 같다[3]: **원격 감시 및 보고, 양방향 통신, 원격 공급 제어, 기기 간 통신**. 스마트미터는 주기적으로 소비 전력을 읽어 관리 서버에 제공한다(원격 감시 및 보고). 또한 스마트미터는 전력 품질(quality), 공급, 수요 정보를 서버에게 전달하고, 서버는 이에 맞는 제어정보 및 시간 동기화 정보 등을 제공한다(양방향 통신). 관리 서버는 미터기를 통해 전력 공급을 제한할 수 있다(원격 공급 제어). 스마트기기, 축적장치, 스마트미터기 등은 에너지 관리 정보를 공유하기 위해 서로 통신 가능하다(기기 간 통신).

설명된 스마트그리드 네트워크의 제공 기능을 고려해 보면 해당 네트워크의 트래픽 패턴은 다음 표 1과 같이 두 가지로 나뉘어 특징지어 진다.

[표 1] 스마트그리드 네트워크의 트래픽 특징

종류	특징
미터링 트래픽	전송특징: 주기성을 갖거나 스케줄 된 전송 (이벤트 기반 전송도 가능), 작은 크기 데이터의 집중적인 (busty) 전송, 효율적 전송을 위해 미터기간 그룹핑 되어 전송 가능
	전송방향: 단말기기로부터 관리서버로 전송
	중요요소: 높은 전송률
관리/제어 트래픽	전송특징: 이벤트 기반 전송, 멀티캐스트/브로드캐스트/유니캐스트 가능
	전송방향: 관리서버로부터 단말기기로 전송
	중요요소: 낮은 지연

2.2 스마트미터기의 가용성에 대한 취약점 및 대응에 관한 연구

앞서 소개한 스마트그리드 네트워크의 중요 역할을 수행할 스마트미터기는 댁외에 설치되기 때문에 권한을 가지지 않은 공격자에게 쉽게 노출된다. 또한 공격자는 유무선으로 연결된 스마트미터기를 기존 해킹기술을 이용하여 공격할 수 있다. 이렇게 공격 당한 스마트미터기를 조작하여 에너지공급업자의 유동적인 전력 가격 책정 및 에너지 관리를 정상적으로 수행할 수 없게 할 수 있다. 더 나아가 다수의 스마트미터기에 대한 서비스 거부 공격(연산능력, 데이터 송·수신 능력 그리고 데이터 저장 능력 등을 의도적으로 초과하도록 하여, 제품 자체의 기능을 마비시킴)을 통해 전체 에너지공급시스템에 커다란 영향(예, 전력망 불안정, 대규모 정전 사태)을 끼칠 수 있다. 이러한 가능성은 모의 해킹 실험을 통해서 보였고 그 위험성을 시사하였다[2,4,5].

그러므로 스마트미터기에 대한 가용성 보호는 필수적이며 스마트미터기 또는 관리 기기에 이러한 공격을 탐지할 수 있는 모듈 및 프로그램을 갖추어야 한다[5]. 그러나 해당 네트워크에 대한 공격대응 연구로 false data injection attack에 대한 연구가 주를 이루어 왔고[6], 스마트미터기에 대한 보안 연구로는 인증에 대한 연구가 진행되어 왔다[7,8]. 스마트그리드 네트워크와 유사한 센서 네트워크나 메쉬네트워크에서의 가용성 보호 메커니즘들의 적용을 고려해 볼 수 있으나, 스마트미터기는 센서보다는 처리용량이 크고 일반적인 인터넷 트래픽을 전달해 주는 메쉬라우터와 다른 트래픽 패턴을 보이므로 기존 연구들의 직접적 적용은 효율성이 떨어질 수 있다. 그러므로 스마트그리드 네트워크 구조와 트래픽 특성을 고려한 가용성 보호 메커니즘 연구가 필수적이다.

2.3 엔트로피와 근사엔트로피

본 절에서는 값의 분산 정도를 추정하는 통계학적 개념인 엔트로피(entropy)와 본 논문에서 공격 탐지에 기본 메소드로 사용할 근사엔트로피(approximate entropy)를 소개한다.

엔트로피 값은 값들의 분산 정도를 나타내어 정상과 이상을 구분하는 이상징후 탐지 시스템으로 사용이 되어 왔다[9]. 예를 들어 정상 트래픽들의 근원지 IP 주소에 대한 엔트로피 값과 비교하여 서비스거부(DoS, Denial of Service) 공격 시 특정 공격노드의 트래픽양이 증가하면 해당 엔트로피 값이 변하게 된다. 즉 분산 정도가 달라져 이 차이로 인해 공격을 탐지할 수 있다[9-11]. 수식(1)은 엔트로피 값을 추정하는 가장 일반적인 식으로 M개의 그룹의 엔트로피를 계산할 때 p_i는 i 그룹의 발생 확률이고 maximal likelihood 추정법에 의해 $\hat{p_i} = n_i/N$ (n_i는 i 그룹의 샘플 수, N은 추정에 사용된 총 샘플 수)가 사용된다.

$$E = -\sum_{i=1}^{M} p_i \log p_i \quad (1)$$

그러나 이 엔트로피 추정법은 least square error 측면에서 최적이 아님이 알려져 있고, 특히 M 값이 커지는 경우 많은 계산 비용을 요구한다. 이러한 단점을 개선하기 위해 truncated Taylor series를 적용한 근사엔트로피 추정법이 제안되었다[12]. 근사엔트로피는 로그계산의 부하를 줄이고, 엔트로피 계산에 사용되는 적은 샘플 수에도 비교적 정확한 엔트로피 값에 근사할 수 있게 유도된 수식이다. 수식의 대부분의 값은 고정 값으로 미리 저장하여 사용할 수 있다. 특히, 논문 [12]에서는 S_i 값을 중앙값 0.5 (i=1,…,M), K=20이 근사치 정확성 측면에서 충분함을 보이고 있어서, 수식 (2)에 의해 근사엔트로피 계산 시 n_i만 변수로 사용된다.

2.4 신호정보를 이용한 인증, 로컬라이제이션

물리적 무선 신호정보는 대기의 지문(fingerprint in the ether)이라 할 정도로 의도된 변조 및 예측이 어려운 고유 정보이다. 이러한 이유로 최근 신호정보를 이용한 보안 메커니즘들이 소개되고 있는데, CIR(Channel Impulse Response)를 이용한 인증메커니즘이 대표적인 예이다[13,14]. Transmitter에서 송신한 신호는 서로 다른 곳에 위치한 Receiver들에서 다른 CIR 값을 나타내고, 특히 근처에 있는 경우에도 변동 패턴의 차이가 보임을 실험결과로 증명하였다. 이를 이용해 다른 지역에 있는 공격자의 신호를 합법적인 노드의 신호와 구별하여 인증한다[13].

신호정보를 이용한 또 다른 대표적 기법으로 로컬라이제이션 메커니즘이 있다[15,16]. 신호의 세기인 RSSI(Received Signal Strength Indication)는 거리에 연관성이 있어 이를 위치 측정의 기본 정보로 사용하는 기법들이다. 본 논문에서도 고정 노드들(스마트미터기)의 무선 시그널은 특정 신호정보(CIR, RSSI)를 가지고 있고 공격노드가 이를 변조하기 어렵다는 특성을 이용한다. 즉, 트래픽의 정보를 변조(예, ID 변조)하여도 신호정보는 합법적인 노드의 신호로 변조하기 어렵다는 점을 이용하여 공격노드 검출 시 사용한다.

$$\hat{E}=\sum_{i=1}^{M}s_i-\frac{1}{N+M}\sum_{i=1}^{M}(1+\log s_i)(n_i+1)-\sum_{k=2}^{K}\frac{1}{k(k-1)}\sum_{j=0}^{k}\binom{k}{j}\frac{(N+M-1)!}{(N+M+j-1)!}(-1)^j\sum_{i=1}^{M}s_i^{-j+1}\frac{(n_i+j)!}{n_i!} \quad (2)$$

III. 신호정보를 이용한 공격 및 공격노드 검출

3.1 네트워크 모델 및 공격 모델

본 논문에서 가정한 네트워크 모델은 스마트그리드 네트워크의 NAN과 HAN이다. 그림 1과 같이 가정의 가전과 스마트 기기들이 스마트미터기를 중심으로 HAN을 구성하고 있고, 이러한 스마트미터기들은 메시 또는 트리 구조를 구성하며 WAN에 연결된다. 각 스마트미터기들은 주기적으로 WAN에 위치한 서버(예, SCADA서버)에 미터링정보를 전송한다. 또한 서버에서는 스마트미터기에 대한 제어 정보 및 전력에 대한 가격 정보, 사용한 에너지에 대한 요금 청구서 등을 비주기적으로 전송할 수 있다. 안전한 정보 전송을 위해 인증 수행이나 암호화된 정보 전송이 가능하다.

본 논문에서 가정하는 공격 모델은 HAN과 NAN의 중요 장비인 스마트미터기의 가용성 측면을 저해하는 공격, 즉 서비스거부 공격이다. 공격 당한 내부 기기(스마트미터기, 스마트 장치) 또는 합법적이지 않은 기기가 많은 센싱정보 또는 미터링 정보를 전달(injecting 공격)하여 스마트미터기가 정상적인 통신 및 처리를 할 수 없는 상태를 만든다. 해당 공격 트래픽은 공격 사실의 은폐를 위해 노드 정보(예, ID)를 스푸핑(spoofing)할 수 있다. 이러한 공격 트래픽은 NAN 내의 주변 스마트미터기뿐만 아니라 WAN의 Access Pointer, 미터링 정보의 관리 서버까지 마비시킬 수 있다. 공격당한 내부 노드에 의해 공격이 이루어 질 수 있으므로 기본적인 인증이나 암호화된 정보 전송은 해당 공격을 탐지 또는 방어할 수 없다. 본 논문에서는 해당 공격을 탐지하고, 이상 트래픽을 발생하는 노드를 검출하고자 한다.

3.2 제안하는 탐지 모델

본 절에서는 2 장에서 소개한 근사엔트로피를 이용한 가용성 공격 탐지 메커니즘을 제안한다. 이러한 탐지 메커니즘은 정해진 주기마다 다음 프로세스를 수행한다.

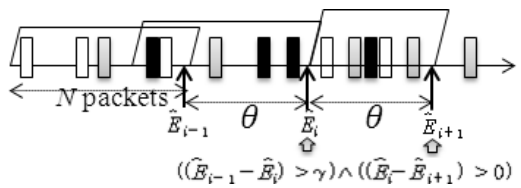
1. 윈도우 내의 수신 패킷에 대해 근사엔트로피 $\hat{E}_i$를 구한다.

$$\hat{E}=0.5M-\frac{0.7}{(A+1)}\sum_{i=1}^{M}(n_i+1)-\sum_{k=2}^{K}\frac{1}{k(k-1)}\sum_{j=0}^{k}\binom{k}{j}\frac{(A)!}{(A+j)!}((-2)^j/2)\sum_{i=1}^{M}\frac{(n_i+j)!}{n_i!} \quad (3)$$

2. $\hat{E}_i$와 지난 윈도우 내의 근사엔트로피 값 $\hat{E}_{i-1}$ 차이가 임계치 이상으로 감소하였는지 조사한다. 임계치 이상이면 다음 근사엔트로피 값 $\hat{E}_{i+1}$을 조사하여 계속 감소 추세인지 조사하고 그렇다면 공격 탐지를 알린다.
3. 공격이 탐지되면, 해당 패킷들의 신호정보와 각 노드의 신호정보로 저장된 정보를 비교하여 빈도수가 높은 신호정보를 방출하는 노드를 공격노드로 검출한다.

3.2.1 윈도우 내의 근사엔트로피 계산

탐지 메커니즘은 2장에서 소개한 근사엔트로피(수식 (2))를 이용한다. 해당 수식은 수식 (3)과 같이 전개할 수 있다(단, $A=N+M-1$, N은 윈도우내 수신 패킷 수, M은 그룹 수). 탐지 메커니즘에서 정한 윈도우 내에 N개의 수신 패킷의 ID를 가지고 그룹핑하여 각 그룹에 해당하는 패킷의 수를 가지고 수식 (3)을 이용해 근사엔트로피를 계산한다. 그룹핑 방법은 각 그룹에 포함된 노드의 RSSI 값 편차가 크도록 배정한다. 이는 공격 탐지 후 가장 많은 패킷이 포함된 그룹 내에서 공격 노드를 용이하게 검출하기 위함이다. 공격 탐지를 위한 이 계산은 주기 θ, 즉 슬라이딩 간격마다 이루어진다(그림 2 참고).



〔그림 2〕 윈도우 내 수신 패킷으로 근사엔트로피 계산 및 임계치 비교

3.2.2 공격 여부 검사

새로이 근사엔트로피 $\hat{E}_i$가 계산되면 이전에 계산된 근사엔트로피 값 $\hat{E}_{i-1}$과의 차를 임계치 γ와 비교한다. 임계치는 시스템 파라미터로서 정상트래픽에서의 근사엔트로피 값들 차이를 측정하여 정할 수 있다. 비교 시, 임계치 이상이면 공격 가능성이 있으므로 다음 근사엔트로피 값 $\hat{E}_{i+1}$의 차를 0과 비교하여 0보다 크다면 (줄어드는 추세, 즉 트래픽 분포가 특정 그룹에 치우치면) 공격으로 탐지한다.

3.2.3 공격노드 검출

공격 여부 검사에서 공격이 탐지되면, 마지막으로 계산된 근사엔트로피에 사용된 패킷들의 신호정보(RSSI 또는 CIR)를 조사하고, 높은 빈도의 신호정보를 가지고 기 저장된 각 노드의 신호정보와 유사도 체크를 통해 공격노드를 검출한다. 유사도 체크를 위해 CIR 정보를 활용하여 검출하는 경우 〔13〕의 가설검정테스트 기법을 활용할 수 있고, RSSI 정보를 이용하는 경우 〔15〕의 위치 측정법 등을 이용하여 노드의 위치 정보로서 공격노드를 검출할 수 있다.

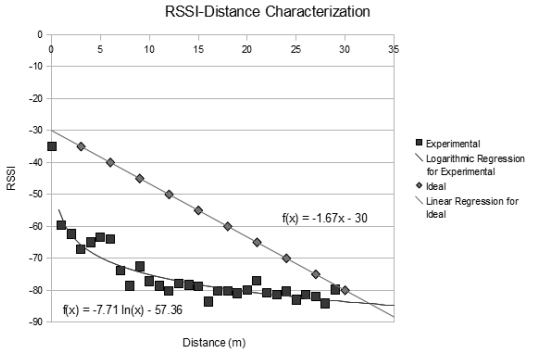
IV. 성능 평가

본 장에서는 제안된 메커니즘의 탐지 성능 및 가능성을 입증하기 위해 시뮬레이션 환경을 구축하여 결과를 도출 및 분석한다.

4.1 시뮬레이션 환경

시뮬레이션을 위한 스마트그리드 네트워크는 다음과 같이 구성되어 있다. 100m x 100m 영역에 좌측 하단에 WAN의 연결을 위한 AP가 있고, 20개의 스마트미터기(SM)가 랜덤으로 배치되어 있다(단, HAN을 가정하므로 10m 반경에 하나 이상의 SM 배치 배제). 모든 SM은 직접 AP와 통신한다. 각 SM들은 주기 1분, 5분 또는 10분 주기로 AP에 전력량(사용 또는 저장량)을 보고하고(각 주기와 시작 시간은 랜덤으로 선택됨), SM에서 AP로 간헐적(랜덤) 제어 트래픽을 발생한다.

공격모델은 20개의 SM 중 SM5가 공격노드가 되고 짧은 주기로(1초, 5초, 10초) AP에 전력량을 보고한다(1700초 공격 개시). 공격노드 탐지에 사용되는 신호정보는 RSSI를 사용하였다. 거리에 따른 RSSI 모델은 그림 3에서처럼 실측 정보에 의해 추정된 함수 f(x)=-7.71ln(x)-57.36 (x는 거리(m))를 사용하되 거리에 따라 해당 수식 RSSI 값이 평균값이 되고, 분산값이 0.5가 되는 가우시안 분포를 사용하여 각 패킷의 RSSI 값을 생성하였다. 본 논문에서 제안한 근사엔트로피 측정 주기는 50초, 측정 패킷의 수 N은 100, 그룹 수 M은 5로 하고, 공격여부 검사 및 공격노드 탐지는 SM의 패킷을 수집 전달하는 AP에서 수행하는 것으로 가정하였다. 공격여부에 사용된 임계치 γ은 공격이 없는 Normal 상태일 때의 엔트로



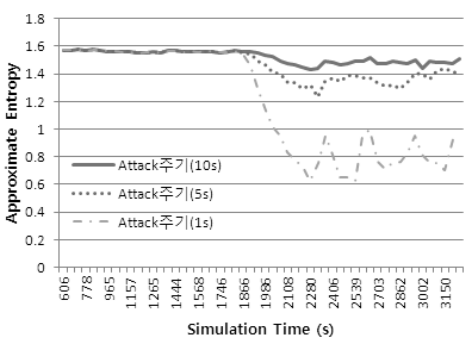
〔그림 3〕 거리와 RSSI 관계(실험적/이론적 결과)〔13〕

피 값의 변화량 평균(0.006591)을 참고하여 0.015로 하였다.

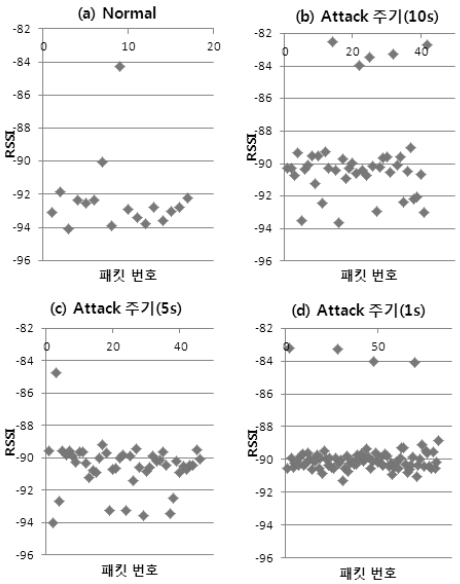
4.2 시뮬레이션 결과

우선 근사엔트로피를 이용한 공격 탐지 성능을 분석하였다. 그림 4와 같이 공격 패킷이 SM5에서 생성되기 전까지는 Normal 상태, 즉 안정된 근사엔트로피 값을 갖는다. 그러나 공격 패킷 발생 후 누적되면서 각 그룹의 패킷 분포도 값이 변하고 약 1800초에 공격을 탐지하게 된다. 공격 주기에 따라 근사엔트로피의 변화량의 정도가 보이며, 가장 심한 공격인 경우(공격주기 1초) 가장 큰 감소와 변동을 나타내고 있다. 이로써 공격 탐지 가능성과 성능을 입증할 수 있다.

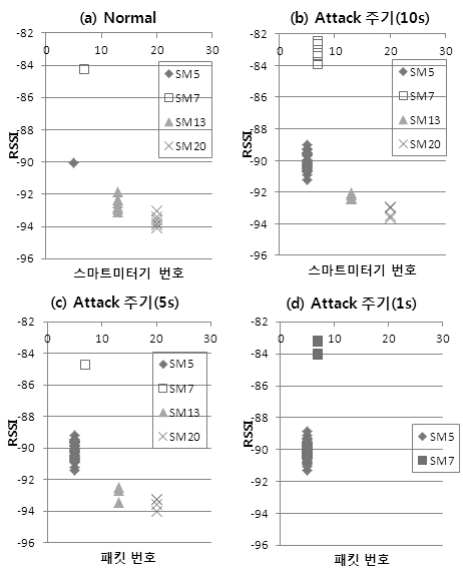
다음으로 신호정보 RSSI를 이용한 공격노드 검출 가능성을 분석하였다. 그림 5는 SM5가 포함된 그룹의 특정 근사엔트로피 계산에 포함된 패킷의 RSSI 값을 나타내고, Normal 상태와 Attack(공격주기 10,5,1초) 경우를 나누어 도시하였다. 우선 근사엔트



〔그림 4〕 공격에 따른 근사엔트로피 값 변화



〔그림 5〕 공격 노드 SM5가 포함된 그룹의 패킷 RSSI



〔그림 6〕 공격 노드 SM5가 포함된 그룹의 노드 당 패킷 RSSI

로피 계산에 사용된 100개의 패킷 중 Normal 상태인 경우 17개로 고른 분포를 보이고 있고(총 그룹 수 M은 5), Attack(주기 10,5,1초)인 경우 각 42,46,83 순으로 증가하고 있음을 보이고 있다. 또한 공격이 강해질수록(1초 경우) 유사도가 큰 값들이 분포되어 공격노드 검출에 용이함을 보여주고 있다. 그림 6은 그림 5와 동일 한 값을 노드 당 패킷 RSSI 값

으로 도시하고 있다. Normal인 경우 SM5의 패킷 수는 한 개였으나 공격이 심해질수록 SM5 패킷의 수가 증가하고, 다른 노드의 패킷 수가 감소함을 보이고 있다. RSSI의 유사도 측정(예, 저장된 각 노드의 RSSI값과 수신 패킷 RSSI의 차이에 대한 절대값 이용)을 이용해 정확한 공격 노드를 검출할 수 있다.

V. 결 론

본 논문에서는 스마트그리드 네트워크의 핵심 기기인 스마트미터기에 대한 가용성 보장에 대한 연구를 수행하였다. 스마트그리드 구조 및 트래픽패턴의 특징 분석을 통해 탐지 메커니즘을 고안하였고, 특히 공격 노드에서 변조하기 어려운 신호정보를 이용해 공격 탐지 및 공격노드를 검출하는 기법을 제안하였다. 이는 일반적인 패킷 정보로 엔트로피 계산에 의한 기존 공격 탐지 기법에 비해 탐지율을 향상 시킬 수 있다. 마지막으로 시뮬레이션을 통해 검출 가능성과 성능을 보였다.

참고문헌

〔1〕 M. Kim, "A Survey on Guaranteeing Availability in Smart Grid Communications," Proceedings of IEEE ICACT, pp. 314-317, Feb. 2012.

〔2〕 정교일 , 박한나 , 정부금 , 장종수 , 정명애, "스마트그리드의 안전성과 보안 이슈," 정보보호학회지, 22(5), pp. 54-61, 2012년 8월.

〔3〕 Y.M. Kwon, J.S. Kim, M.Y. Chung, H. Choo, T.J. Lee, and M. Kim, "State of the Art 3GPP M2M Communications toward Smart Grid," KSII Transactions on Internet and Information Systems, vol. 6, no. 2, pp. 468-479, Feb. 2012.

〔4〕 남궁완, 조효진, 조관태, 이동훈, "스마트미터 보안 연구," 정보보호학회지, 20(5), pp. 20-30, 2010년 10월.

〔5〕 정철조, 은선기, 최진호, 오수현, 김환구, "스마트미터의 취약성/보안요구사항 분석 및 CC v3.1 기반 보호프로파일 개발," 정보보호학회논문지, 20(6), pp. 111-125, 2010년 12월.

〔6〕 Y. Liu, P. Ning, and M.K. Reiter, "False data injection attacks against state estimation in electric power grids," Proceedings of the 16th ACM conference on Computer and communications security (CCS '09), pp. 21-32, Nov. 2009.

〔7〕 김홍기, 이임영, "스마트그리드 AMI환경에서의 ID기반 인증기법에 관한 연구," 정보처리학회지c, 18(6), pp. 397-404, 2011년 12월.

〔8〕 최재덕, 서정택, "스마트그리드 보호를 위한 AMI 망 분리 및 인증 프레임워크," 정보보호학회논문지, 22(3), pp. 525-536, 2012년 6월.

〔9〕 L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical Approaches to DDoS AttackDetection and Response," Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 303-314, Apr. 2003.

〔10〕 전재현, "엔트로피를 이용한 DDoS 공격 탐지 방법," 석사학위논문, 경북대학교, 2011년 2월.

〔11〕 김민택, 최영우, 권기훈, 김세헌, "다중 엔트로피를 이용한 네트워크 공격 탐지 기법," 정보보호학회논문지, 16(1), pp. 71-77, 2006년 2월.

〔12〕 Y. Yokota, "An Approximate Method for Bayesian Entropy Estimation for a Discrete Random Variable," Proceedings of the 26th IEEE EMBS, pp. 99-102, Sep. 2004.

〔13〕 L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," Proceedings of the IEEE Int. Conf. on Comm.(ICC), pp. 4646-4651, Jun. 2007.

〔14〕 Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," Proceedings of IEEE Symp. Security and Privacy, pp. 286-301, May 2010.

〔15〕 M. Quan, E. Navarro, and B. Peuker, "Wi-Fi Localization Using RSSI Fingerprinting," Bachelor's thesis, California Polytechnic State University, 2010.

[16] A.S. Paul and E.A. Wan, "Wi-Fi based indoor localization and tracking using sigma-point Kalman filtering methods," Proceedings of IEEE/ION Position, Location and Navigation Symposium, pp. 646-659, May 2008.

〈著者紹介〉

김 미 희 (Mihui Kim) 종신회원
1997년: 이화여자대학교 전자계산학과 졸업
1999년: 이화여자대학교 전자계산학과 석사
1999년~2003년: 한국전자통신연구원 연구원
2007년: 이화여자대학교 컴퓨터공학과 박사
2007년~2009년: 이화여자대학교 컴퓨터공학과 전임강사
2009년~2010년: 미국 노스캐롤라이나주립대학 컴퓨터학과 포스닥연구원
2011년~현재: 국립한경대학교 컴퓨터웹정보공학과 조교수
〈관심분야〉 센서/스마트그리드 네트워크 보안, 네트워크 프로토콜 설계 및 성능평가