정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

산업 제어 시스템 네트워크 분석 저지를 위한 트래픽 난분석화 기법

이 양 재*, 정 혜 림*, 안 성 규*, 박 기 웅**

요 약

산업 제어 시스템 대상 원격 관제 기술은 관리자의 즉각적 대응을 통해 산업 재해 발생 확률 저하를 위한 핵심기술로 주목받고 있다. 그러나 산업 제어 시스템 원격 관제 기술은 원격의 관리자와 통신하기 위해 외부 네트워크 연결이 필수적이며, 따라서 공격자들에게 기존 산업 제어 시스템에 존재하지 않던 새로운 네트워크 취약점을 노출하게 된다. 산업 제어 시스템은 네트워크 취약점을 해결하기 위해 터널링 프로토콜 또는 패킷 암호화 솔루션을 사용하고 있지만, 이러한 솔루션은 패킷 메타데이터를 분석하는 네트워크 트래픽 분석 공격을 방어하지 못한다. 공격자는 네트워크 트래픽 분석을 통해 패킷의 송수신 대상, 통신 빈도, 활성화 상태 등을 알 수 있으며 획득한 정보를 다음 공격을 위한 초석으로 사용할 수 있다. 따라서 기존의 솔루션들이 해결하지 못하는 산업 제어 시스템 네트워크 환경에서 발생하는 잠재적인 문제들을 해결하기 위해 네트워크 트래픽 분석 난이도를 향상시켜 분석을 방어하는 솔루션이 필요하다. 본 논문에서는 패킷 메타데이터를 분석하는 네트워크 트래픽 분석 공격을 어렵게 하고자 패킷 분할 및 병합 기반 네트워크 트래픽 난분석화 기법을 제안한다. 본 논문에서 제안하는 기법의 참여자인 관리자와 산업 기기는 각각 일정한 크기의 그룹으로 묶인다. 그리고 원격 관제를 위해 관리자와 산업 기기 간 송수신되는 모든 패킷을 대상으로 분할 노드를 경유하도록 한다. 분할노드는 패킷의 난분석화를 위한 핵심 요소로써, 관리자와 산업 기기 사이에 송수신되는 모든 패킷을 상호 목적 대상 그룹의 개수로 분할한다. 그리고 분할한 패킷 조각에 패킷 식별자와 번호를 부여하여 패킷 조각을 모두 수신한 목적대상이 올바르게 패킷을 병합할 수 있도록 하였다. 그리고 분할노드는 목적 대상이 속한 그룹의 모든 참여자에게 서로 다른 패킷 조각들을 전달함으로써 공격자가 패킷의 흐름을 알 수 없도록 하여 산업 제어 시스템 정보를 수집하는 것을 방어한다. 본 논문에서 제안하는 패킷 분할 및 병합 기반 트래픽 난분석화 기법을 통해 산업 제어 시스템을 대상으로 한 트래픽 분석 공격을 방어함으로써 네트워크 공격의 피해를 줄이고 추가적인 네트워크 공격을 차단할 수 있을 것으로 기대된다.

Ⅰ. 서 론

산업 제어 시스템 대상의 원격 관제 기술[1,2,3]은 위험을 빠르게 감지하고 즉각적으로 대응하여 산업 재해 발생 확률을 낮출 수 있는 핵심기술로서 각광받고 있다. 원격 보안 관제를 위한 핵심 기반기술 중 하나는 산업용 사물 인터넷(IIoT)과 클라우드를 산업 제어 시스템에 통합한 4세대 IoT-Cloud 기반 산업 제어 시스템이다. 그러나 산업 제어 시스템 원격 관제 기술은 원격의 관리자와 통신하기 위해 외부 네트워크 연결이 필수적이며, 따라서 공격자들에게 기존 폐쇄형 산업 제어 시스템에는 존재하지 않던 새로운 네트워크 취약점을 노출하게 되었다. 원격 관제로 인한 네트워크 취약점은 병원, 발전소, 지하철과 같은 사회 기반 시설의 사고가 사회 혼란과 직접적으로 이어지는 산업 제어 시스템의 특성과 결합되어 사회 혼란을 목표로 하는 테러리스트 또는 적국의 공격자들이 네트워크라는 새로운 통로를 통해 산업 제어 시스템을 공격할 수 있게 하였다. 실제로 산업 제어 시스템이 외부 네트워크와 연결된 이래로 산업 제어 시스템 대상 공격이 증가하였으며, 많은 수가 네트워크 공격과 연관이 되어있다[5].

대표적으로 2013년 뉴욕 RyeBrook 인근의 작은 댐이 유지보수를 위해 인터넷에 연결된 사이 해커에게 공격당했다[6]. 2014년, German steel mill을 대상으로 한

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 지원(Project No. 2018-0-00420)을 받아 수행된 연구임.
* 세종대학교 정보보호학과 시스템보안연구실 (대학원생, {leelambjae, hyello13, yiimfn}@gmail.com)
** 세종대학교 정보보호학과 (교수, woongbak@sejong.ac.kr)

공격자는 비즈니스 네트워크 접속을 통해 생산 네트워크까지 침입함으로써 German steel mill에 막대한 피해를 입혔다[7]. 산업 제어 시스템 공격에 관한 문헌 조사 결과, 이 외에도 많은 산업 제어 시스템을 대상으로 한 공격이 네트워크를 통해 이루어졌다[8,9].

기존 산업 제어 시스템이 4세대 IoT-Cloud 기반 산업 제어 시스템으로 전환됨에 따라 산업 기기가 외부 네트워크에 연결되어 네트워크 취약점에 노출되었고, 많은 공격자들에게 공격의 대상이 되었다. 기존 네트워크 취약점을 해결하기 위해 기존에 사용되는 터널링 프로토콜 또는 패킷 암호화 같은 솔루션은 패킷의 메타데이터를 분석하는 네트워크 트래픽 분석 공격들을 방어하기에는 한계가 존재한다[4,11]

산업 제어 시스템 네트워크를 대상으로 한 공격은 공격자가 산업 제어 시스템의 정보를 얼마나 수집할 수 있느냐에 따라 공격의 위험성이 달라질 수 있다. 예를 들어, 공격자가 산업 제어 시스템이 통신량이 많은 시간대에 DDoS 공격을 수행한다면 공격의 위험성과 피해는 증가한다. 또한 산업 제어 시스템이 통신 중인 IP를 대상으로 공격을 수행하여 효율적으로 특정 사용자의 통신만을 차단할 수도 있다. 이와 같이, 공격자가 산업 제어 시스템 네트워크 트래픽 분석을 통해 네트워크 패킷의 송수신 대상, 통신 빈도, 활성화 상태 등을 알 수 있다면 공격자는 네트워크 공격의 피해를 증폭시킬 수 있다. 따라서 산업 제어 시스템의 산업 기기가 외부의 관리자와 통신할 때, 공격자의 네트워크 트래픽 분석 공격을 막기 위해서는 보안채널을 사용함과 더불어 공격자가 패킷 메타데이터를 분석하여 산업 제어 시스템의 정보를 수집하는 것을 방지하는 트래픽 난분석화 솔루션이 요구된다.

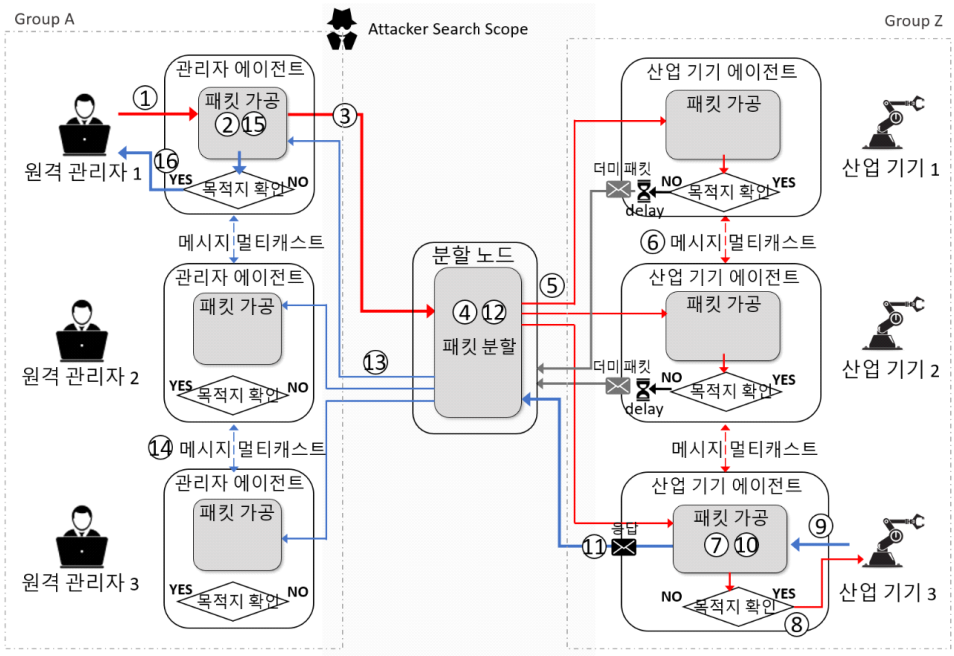
트래픽 난분석화 기법은 공격자의 네트워크 트래픽 분석 대상이 되는 패킷의 크기, 송수신 타이밍, 헤더 등의 메타데이터 분석을 저지하기 위한 연구로, 1981년 Chaum에 의해 최초로 제안되었다[13]. 그러나 산업 제어 시스템이 아닌 일반 시스템을 대상으로 설계되었기 때문에 산업 제어 시스템에 트래픽 난분석화 기법을 적용하기 위해서는 몇 가지 추가로 고려해야할 요구사항이 존재한다.

첫 번째로 산업 제어 시스템은 저지연성이 중요한 시스템이다. 일부 시스템은 시스템이 처한 현재 상황에 대한 즉각적인 대응이 필요하다. 그러나 일부 난분석화 기법은 트래픽 분석 방지를 위해 반드시 일정량의 메시지가 수신되어야 메시지를 송신하기 때문에 저지연성 요구사항을 만족시키기에는 적합하지 않다[16].

두 번째로 산업 제어 시스템은 가용성이 매우 중요한 시스템이다. 일시적인 중단에도 수만 파운드의 비용이 소모되며[15], 다른 산업 제어 시스템들과도 상호 연결되어 있기 때문에 연결된 모든 산업 제어 시스템이 영향을 받는다. 따라서 새로운 트래픽 난분석화 기법의 적용 및 업데이트로 인한 시스템 중단 시간은 최소한으로 유지되어야 한다.

따라서 본 논문에서는 그림 1과 같이 메시지 분할 및 병합을 기반으로 산업 제어 시스템을 위한 트래픽 난분석화 기법을 제안한다. 트래픽 난분석화 기법에 참여하는 요소는 원격 관리자와 원격 관리자 에이전트, 분할노드, 산업 기기와 산업 기기 에이전트로 이루어진다. 추가적인 원격 관리자와 산업 기기를 효율적으로 관리하기 위해 원격 관리자 에이전트와 산업 기기 에이전트는 n개씩 동일한 그룹으로 묶인다. 본 논문에서 원격의 관리자가 패킷을 보낼 대상인 산업 기기를 목적대상 산업 기기라 명칭 한다. 반대의 상황 또한 동일하다. 원격 관리자가 산업 기기에 데이터를 전송할 때의 흐름은 그림 1의 붉은 선, 산업 기기가 원격 관리자에게 데이터를 전송할 때의 흐름은 그림 1의 푸른 선과 같으며 그 절차는 다음과 같다.

1) 관리자는 데이터와 데이터를 보낼 목적대상 산업 기기의 IP를 관리자 에이전트에 전달한다.
2) 관리자 에이전트는 수신한 데이터와 목적대상 산업 기기 IP를 목적대상 산업 기기 에이전트의 공개키로 암호화한다.
3) 관리자 에이전트는 암호화한 패킷을 분할노드에 송신한다.
4) 분할노드는 수신한 패킷을 목적대상 산업 기기 에이전트 그룹의 산업 기기의 개수 n으로 분할한 후, 재조합을 위해 분할한 패킷 조각에 패킷 식별자와 번호를 부여하여 n개의 새로운 패킷을 생성한다.
5) 분할 노드는 목적대상 산업 기기 그룹의 산업 기기 에이전트들에게 분할한 패킷 조각을 하나씩 전달한다.
6) 산업 기기 에이전트는 멀티캐스팅을 통해 수신한 분할된 패킷 조각들을 그룹 내의 모든 산업 기기들에게 전달한다.



〔그림 1〕 3개의 관리자 및 3개의 산업기기로 구성된 패킷 분할 기반 트래픽 난분석화 기법 전체 아키텍처

7) 분할된 모든 패킷 조각들을 수신한 산업 기기 에이전트는 패킷 조각의 패킷 식별자와 번호를 바탕으로 온전한 데이터를 생성 후, 자신의 개인키로 패킷을 복호화하여 데이터와 산업 기기 IP를 확인한다.
8) 산업 기기 에이전트는 목적지 산업 기기 IP를 확인 후, 자신에게 온 메시지일 경우 산업 기기로 전달한다.
9) 산업 기기는 수신한 데이터에 따른 응답을 생성하여 산업 기기 에이전트에 보낸다.
10) 산업 기기 에이전트는 산업 기기로부터 수신한 데이터와 목적 대상 관리자 에이전트 IP를 해당관리자 공개키로 암호화한다.
11) 목적대상 산업 기기 에이전트는 분할 노드로 패킷을 전달한다. 산업 기기 에이전트 그룹 내에서 패킷의 목적지 산업 기기 에이전트가 아닌 산업 기기 에이전트들은 일정시간 지연 후 더미 패킷을 분할 노드에 전달한다. 이 때, 더미 패킷의 지연은 공격자가 실제 패킷을 식별하는 것을 기만하기 위한 용도로 실제 패킷 전송에 영향을 끼치지 않는다.
12)~14)번은 4)~6)번과 목적 대상만 반대일 뿐, 동일하게 수행된다.
15) 분할된 모든 패킷을 수신한 관리자 에이전트는 패킷 조각의 식별자와 번호를 바탕으로 온전한 데이터를 생성하여 개인키로 복호화하여 데이터와 관리자 IP를 확인한다.
16) 복호화에 성공한 관리자 에이전트는 데이터를 관리자에게 전달한다.

이와 같이 16개의 과정으로 본 논문에서 제안하는 솔루션을 간략하게 서술하였다. 해당 솔루션의 상세한 부분에 대해서는 3장에서 자세하게 서술한다.

본 논문의 나머지 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 연구와 관련된 트래픽 분석 방어 기법 연구에 대해 설명하고 기존 연구들의 한계점을 도출한다. 3장에서는 트래픽 난분석화 기법의 구현을 위한 공격자 모델 및 가정, 디자인에 대하여 기술한다. 4장에서는 본 논문에서 제안하는 트래픽 난분석화 기법의 보안 속성 평가를 수행한다. 마지막 5장에서는 결론에 대해 기술한다.

Ⅱ. 관련 연구

2.1. 산업 제어 시스템

산업 제어 시스템은 기존 독자적인 프로토콜을 실행하는 격리된 환경에서 IIoT와의 통합을 통해 보다 원활한 장비와의 상호작용 및 원격 관제 달성하기 위해 변화하고 있다[2,3]. 현재의 산업 제어 시스템은 IoT-Cloud 기반 원격 관제 시스템을 구축한 이후 관리는 용이해졌지만 반대로 네트워크 공격에 노출되는 문제가 발생하였다.

보안 관리자는 산업 제어 시스템을 위해 일반 시스템을 대상으로 한 네트워크 트래픽 난분석화 기법을 도입할 수 있으나, 산업 제어 시스템과 일반 시스템의 특성 차이로 인해 산업 제어 시스템 환경에 최적화된 솔루션을 고려해야 한다[15]. 트래픽 난분석화 기법 설계를 위해 본 논문에서 고려한 산업 제어 시스템의 특징은 다음과 같다.

- 저지연성: 일부 산업 제어 시스템은 관리자와의 상호작용에 대한 즉각적인 대응이 매우 중요하다.
- 가용성: 산업 제어 시스템 공정은 연속적이다. 또한 다른 산업 제어 시스템들과 상호 연결되기 때문에 중단이 생산에 큰 영향을 끼친다.

2.2. 트래픽 난분석화 연구

본 논문에서는 산업 제어 시스템을 위한 패킷 분할 및 병합 기반 산업 제어 시스템을 제안하였으며, 본 절에서는 해당 연구 분야의 관련 연구를 분석하고 본 논문에서 제안하는 시스템의 이점에 대하여 서술 한다.

Chaum은 1981년 최초로 익명 통신 시스템인 Mix Network를 제안하였다[13]. Mix Network는 일반적으로 송신자와 수신자 믹스 노드로 구성되며 네트워크 트래픽은 임의의 믹스 노드를 경유함으로써 공격자의 네트워크 트래픽 분석을 방어한다. Chaum이 제안한 연구의 믹스 노드는 공격자의 네트워크 트래픽 분석을 막기 위해 다음과 같은 기능을 수행한다.

첫 번째로 공격자가 패킷의 헤더를 분석하여 다음 목적지를 알 수 없도록 다음 목적지를 해당하는 믹스 노드의 공개키로 암호화하여 전송한다. 두 번째로 공격자가 네트워크 트래픽의 시간을 기반으로 트래픽을 분석하는 것을 방지하기 위해 믹스 노드에서 일정량의 메시지가 수신되었을 때 메시지를 재배치 후 전송한다. 이러한 믹스 노드를 Threshold 믹스노드라고 한다. 세 번째로 공격자가 패킷의 크기를 기반으로 트래픽을 분석하는 것을 방지하기 위해 패딩을 삽입하여 메시지의 크기를 동일하게 고정한다.

Chaum이 제안한 초기 믹스 네트워크는 공격자의 다양한 트래픽 분석 기법을 막을 수 있었다. 그러나 산업 제어 시스템의 특성을 고려하였을 때, 반드시 일정량의 메시지가 수신되어야 송신하기 때문에 트래픽양이 적을 경우 심각한 지연이 발생하여 저지연성을 저해할 수 있다[16].

이러한 믹스 네트워크의 지연을 개선하기 위하여 Kesdogan은 Stop-and-go Mixes(SG-mix)를 제안하였다[17]. SG-mix에서 메시지 개시자는 패킷의 경로에 있는 각각의 믹스 노드에서 무작위로 패킷을 지연한다. SG-mix의 믹스 노드별무작위 패킷 지연 방식은 Chaum과 비교하여 트래픽양이 감소하더라도 일정한 패킷 속도를 제공한다. 그러나 SG-mix는 여전히 타이밍 분석을 막기 위한 추가적인 지연이 존재하며, 트래픽양이 적을 때 익명성이 저하된다는 한계점이 존재한다[18]. 정해진 시간마다 메시지를 송신하는 전략인 Timed Mix는 트래픽양의 감소에 관계없이 일정한 지연을 유지한다는 장점이 있다[19]. 그러나 Timed Mix는 트래픽양이 적을 경우 공격자가 쉽게 패킷을 추적할 수 있다는 한계점이 존재한다[16].

본 논문에서 제안하는 트래픽 난분석화 기법은 트래픽양이 적더라도 성능에 영향을 끼치지 않으며 공격자가 패킷을 분석할 수 없도록 구현하였다. 또한 기존 패킷 지연 기반 방식이 아닌 새로운 분할 및 병합 방법을 사용하여 패킷 분석을 방어한다. 마지막으로 산업 제어 시스템과 참여자는 에이전트를 기반으로 통신하도록 하였다. 이를 통해 산업 제어 시스템에 트래픽 난분석화 기법 적용 시 최소한의 수정으로 빠른 배치를 통해 산업 제어 시스템의 중단을 최소화할 수 있다.

2.3. 저지연 트래픽 난분석화 연구

Vukovic은 연구에서 오버헤드와 익명성의 트레이드오프 관계를 조사하면서 Minstrel 기법을 제안하였다[20]. Minstrel 기법은 메시지가 목적지에 올바르게 도

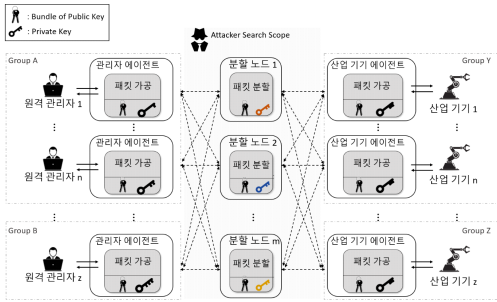
달하더라도 공격자가 누가 수신했는지 알 수 없도록 반드시 모든 믹스 노드를 거치게 하여 공격자가 발신자와 수신자를 알 수 없도록 하는 것을 목표로 하였다. 그러나 이 기법은 목적지에서 응답을 생성하는데 오랜 시간이 걸릴 경우 공격자는 지연 시간을 바탕으로 응답을 생성한 노드를 추론할 수 있다.

Huang은 지연 없이 트래픽 분석 공격을 막기 위해 메시지 split and merge 전략을 사용하였다[21]. 본 논문에서 Huang은 종단과 종단을 모니터링 할 수 있는 공격자 모델을 설정한 후, 메시지를 특정 믹스 노드에서 분할함으로써 종단만을 볼 수 있는 공격자에게 복수 개의 믹스노드로부터 패킷을 수신하는 것처럼 보이도록 구현하였다. Huang의 연구는 지연 기반 방식을 사용하지 않고 공격자를 방어할 수 있지만 전체 네트워크를 볼 수 있는 더 강력한 공격자를 대상으로 하였을 때, 트래픽 분석을 방어하는 것이 불가능하고 메시지를 수신한 수신자를 공격자가 알 수 있다는 한계가 존재한다.

산업 제어 시스템의 경우 중요 사회 기반시설을 대상으로 작동하기 때문에 산업 제어 시스템에 대한 공격이 국가에 막대한 피해를 입힐 수 있다. 산업 제어 시스템을 공격하여 이득을 얻을 수 있는 공격 단체는 주로 국가의 지원을 받아 조직적으로 활동하거나 막대한 자금을 바탕으로 한 공격자이기 때문에 일반적인 시스템을 대상으로 하는 공격보다 많은 컴퓨팅 자원을 활용하여 공격을 수행할 수 있다. 따라서 본 논문에서는 산업 제어 시스템과 관리자 사이의 모든 네트워크를 감시할 수 있는 강력한 공격자를 대상으로 통신 중인 송신자와 수신자를 식별할 수 없는 트래픽 난분석화 기법을 설계하였다.

Ⅲ. 분할 및 병합 기반 트래픽 난분석화 기법

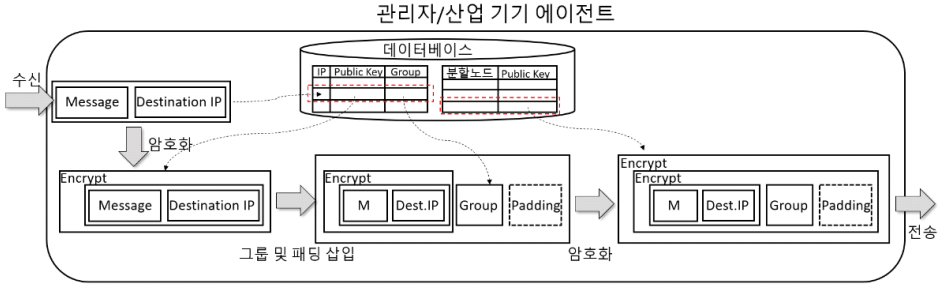
본 장에서는 가정과 공격자 모델, 트래픽 난분석화 기법의 전체적인 아키텍처, 핵심 기술에 대해 설명한다.



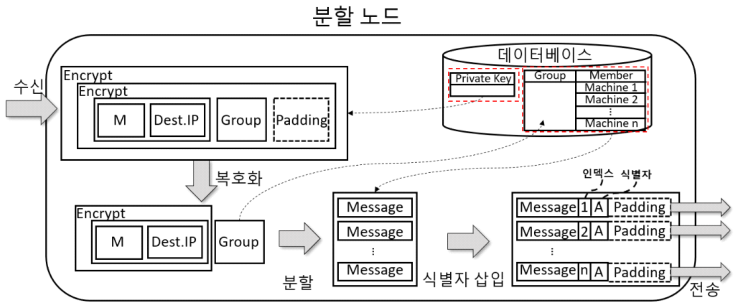
〔그림 2〕 산업 제어 시스템을 위한 트래픽 난분석화 기법 배경

본 논문에서 제안하는 기법은 그림 2와 같은 가정 사항으로 구성되어있으며 세부 사항은 다음과 같다.

- 모든 참여자는 각각의 공개키와 개인키를 가지며 공개키는 공유되어 있다.
- 그림 2의 시스템의 모든 참여자는 공공 IP를 가지고 있으며, n명의 관리자, n개의 산업기기는 그룹화 된다.
- 그림 2의 탐색 범위 내에서 공격자는 산업 제어 시스템과 기업 간의 모든 네트워크를 관찰할 수 있다.
- 산업 기기와 산업 기기 에이전트는 동일한 네트워크에 위치하여 LAN 통신을 수행한다.
- 관리자와 관리자 에이전트는 동일한 네트워크에 위치하여 LAN 통신을 수행한다.



〔그림 3〕 관리자, 산업 기기 에이전트 패킷 생성 과정



〔그림 4〕 분할 노드 패킷 분할 및 전송 과정

3.1. 트래픽 난분석화 기법

본 절에서는 패킷 분할 및 병합 기반 트래픽 난분석화 기법에 대하여 설명한다.

그림 1의 붉은 선과 같이 관리자는 원격에서 산업 기기를 관리하기 위해 모니터링 결과를 바탕으로 요청을 생성한다. 관리자가 데이터와 목적대상 산업 기기IP를 관리자 에이전트에게 전송하면 관리자 에이전트는 그림 3과 같이 데이터와 목적대상 IP를 받아 데이터와 목적대상 산업 기기의 IP를 목적대상 산업 기기의 공개키로 암호화한다. 그 후 암호화한 값에 목적지 산업 기기의 그룹 식별 값을 삽입하고 패킷을 동일한 크기로 만들기 위해 패딩을 삽입한다. 그리고 전송할 분할 노드의 공개키로 한 번 더 암호화한다.

패킷을 수신한 분할노드는 그림 4와 같이 분할노드의 개인키로 패킷을 복호화한 후 패딩을 제거한다. 분할노드는 패킷에서 암호화된 데이터와 그룹명을 획득한다. 분할노드는 데이터베이스에서 그룹명에 존재하는 산업 기기들의 개수에 맞추어 패킷을 분할한다. 그 후 분할된 각각의 패킷에 병합을 위한 패킷 순서인 인덱스 번호와 패킷을 구분할 수 있는 식별자, 크기를 동일하게 설정하기 위한 패딩을 삽입하여 각각의 산업 기기 에이전트로 패킷을 전달한다.

분할 노드로부터 패킷을 수신한 산업 기기 에이전트들은 수신한 패킷을 그룹 내의 다른 산업 기기 에이전트들을 대상으로 멀티캐스팅한다. 멀티캐스팅을 통해 모든 산업 기기는 온전한 패킷을 수신하게 된다. 이 중 목적대상 산업 기기 에이전트만이 자신의 개인키로 복호화하여 데이터를 확인할 수 있다.

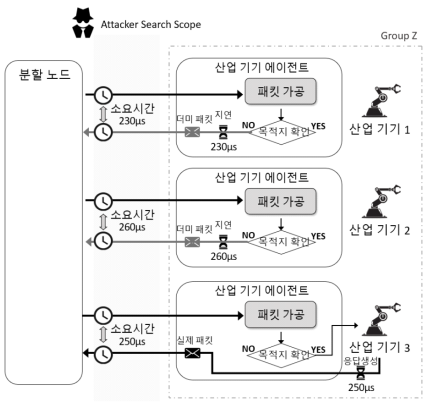
산업 기기의 응답은 그림 3과 같이 원격 관리자가 산업 기기에 요청을 생성할 때와 동일한 과정을 통해 원격 관리자에게 전달된다.

3.2. 공격자 기만 방법

본 절에서는 목적대상 산업 기기 에이전트 그룹 내의 타 산업 기기 에이전트들이 더미 응답을 일정시간 지연 후 분할노드에 전달하는 방법에 관하여 설명한다.

그림 5와 같이 공격자 기만을 위해 트래픽 난분석화 기법에서는 패킷의 목적지가 아닌 산업 기기 에이전트들 또한 더미 응답을 분할노드에 전달함으로써 공격자가 실제 패킷을 송수신하는 산업 기기 에이전트를 특정할 수 없도록 구현하였다. 만약 공격자가 모든 산업 기기의 응답 생성 시간을 측정한다면 목적지 산업 기기에서 응답을 생성하는 시간과 산업 기기들은 더미 응답 생성이 다르기 때문에 공격자가 목적지 산업 기기를 식별할 수 있게 된다. 저지연성을 요구하는 일반적인 동작 제어 시스템의 경우 250μs 부터 1 ms의 시간이 소요된다[22]. 이에 반해 더미 응답 생성 시간은 저장된 값을 바로 보내기 때문에 실제 응답 생성 시간과 같을 수 없다. 따라서 지연시간을 통해 목적 대상 산업 기기 식별을 시도하는 공격자를 기만하기 위해 모든 산업 기기 에이전트는 요청에 따른 응답 생성 시간을 저장하여 다른 산업 기기와 공유한다. 산업 기기 에이전트가 패킷을 수신했을 때 각각의 산업 기기 에이전트는 그림 5와 같이 다른 산업 기기와 사전에 공유한 요청에 따른 응답 생성 시간을 확인 후 해당 시간과 유사한 시간을 지연함으로써 공격자의 산업 기기 에이전트 식별에 혼란을 준다.

이 때 발생하는 지연은 실제 패킷이 아닌 공격자를 기만하기 위한 더미 패킷을 지연하는 것이기 때문에 실제 패킷 전송에 영향을 끼치지 않는다.



〔그림 5〕 지연을 통한 공격자 기만 방법

Ⅳ. 트래픽 난분석화 기법 성능 분석

4.1. 공격자의 수신자 식별 저지

본 절에서는 관리자 에이전트와 산업 기기 에이전트 사이의 모든 네트워크를 볼 수 있는 공격자가 분할 노드를 경유하는 송수신 패킷의 연관성을 분석하여 트래픽의 흐름을 식별하는 것을 트래픽 난분석화 기법으로 저지할 수 있는가를 설명한다.

그림 2와 같이 본 논문에서 설정한 강력한 공격자 모델은 산업 기기와 산업 기기 에이전트간의 통신을 제외한 원격 관리자 에이전트와 산업 기기 에이전트 사이의 모든 네트워크 트래픽을 관찰할 수 있다. 본 논문에서 제안한 분할 및 병합 기반 트래픽 난분석화 기법에선 분할노드가 수신한 1개의 패킷이 n개로 나뉘어 산업 기기 에이전트로 송신된다. 따라서 공격자는 1개의 패킷을 n개의 패킷과 연결하여야 한다. 하지만 n개의 패킷은 모두 진짜이며 동일한 그룹 내의 모든 산업 기기에게 전달되기 때문에 공격자는 어느 산업 기기가 실제 패킷의 목적지인지 식별할 수 없다. 공격자는 목적 대상이 어느 그룹에 포함되었는지 여부는 확인할 수 있지만 그룹 내의 산업 기기의 개수가 늘어날수록 식별 가능성이 낮아진다. 따라서 공격자는 전체 네트워크 트래픽을 관찰하더라도 패킷의 목적지 산업 기기를 식별할 수 없다.

4.2. 공격자의 응답 산업 기기 식별 저지

본 절에서는 산업 기기 에이전트가 관리자 에이전트에게 응답을 보낼 때 공격자가 어느 산업 기기가 응답을 생성했는지 식별하는 것을 본 논문에서 제안한 공격자 기만 기법으로 어떻게 저지할 수 있는가를 설명한다.

만약 그룹 내의 산업 기기 중 목적지 산업 기기만 응답을 생성하여 전달한다면 공격자는 해당 산업 기기가 어느 원격 관리자와 통신하는지 식별할 수 있다. 공격자의 통신 상태 식별을 방지하기 위해 그룹 내의 모든 산업 기기가 더미 응답을 생성함으로써 공격자에게 혼란을 줄 수 있다. 그러나 지능적인 공격자는 해당 그룹의 산업 기기들의 응답시간을 측정함으로써 더미 응답을 전송한 산업 기기와 실제 응답을 생성한 산업기기를 구분할 수 있다. 그러나 본 논문에서 제안한 그림 5의 공격자 기만 방법과 같이 모든 산업 기기 에이전트가 요청에 따른 응답 생성에 소요되는 시간을 사전에 공유하고 그 값을 바탕으로 패킷을 지연한 후 분할 노드에 응답을 전달한다면 공격자는 실제 수신한 산업 기기 에이전트가 누구인지 식별할 수 없다.

4.3. 트래픽양 감소에 따른 난분석성 저하 방지

본 절에서는 트래픽양이 적어질 경우 난분석성이 같이 저하되던 기존의 연구들의 한계점을 극복하기 위해 본 논문에서 제안한 트래픽 난분석화 기법이 트래픽양이 적어질 때 난분석성을 유지할 수 있는가에 대해 설명한다.

트래픽양이 지나치게 적어질 경우 일정 시간마다 패킷을 송신하는 기존 트래픽 난분석화 기법의 경우 익명성이 저하되는 현상을 보였다[19]. 또는 반드시 일정량의 패킷이 수신되었을 경우에만 패킷을 송신하여 과도한 지연이 발생하였다[13]. 그러나 본 논문에서 제안하는 방식은 트래픽양 감소에 관계없이 하나의 패킷을 n개로 분할한다. 패킷 분할 및 병합 기반 트래픽 난분석화 기법에서는 트래픽양이 감소하더라도 다른 패킷과 혼합하여 난분석성을 유지하는 것이 아닌 패킷을 분할함으로써 난분석성을 유지하기 때문에 트래픽양이 감소하더라도 동일한 난분석성을 유지할 수 있다.

V. 결 론

우리는 산업 제어 시스템을 위한 트래픽 난분석화 기법을 제안하기 위하여 산업 제어 시스템의 특성과 기존 네트워크 트래픽 난분석화 기법의 한계점을 바탕으로 요구사항 정의 후 트래픽 난분석화 기법을 설계하였다. 일부 산업 제어 시스템은 현재 상황에 따른 즉각적인 관리자의 응답을 필요로 할 수 있으며, 중단시간을 최소화해야하기 때문에 저지연성과 중단시간 최소화를 고려하여 구현하였다. 그리고 산업 제어 시스템을 대상으로 수행되는 공격은 사회 혼란이 목적인 적국의 공격자 또는 테러리스트가 주요 공격자이기 때문에 일반 시스템을 대상으로 한 공격보다 많은 지원을 바탕으로 조직적이고 고도의 기술을 갖추고 있는 경우가 많았다. 따라서 원격 관리자와 산업 제어 시스템 간의 모든 네트워크를 관찰할 수 있는 강력한 공격자를 설정했다. 기존 네트워크 트래픽 난분석화 기법 조사 결과, 트래픽양이 감소함에 따라 트래픽의 난분석성이 저하되거나 지연이 과도하게 발생하는 한계점이 존재하였다.

앞선 요구사항들을 고려하여 본 논문에서는 산업 제어 시스템을 위한 패킷 분할 및 병합 기반 트래픽 난분석화 기법을 설계하였다. 본 논문에서 제안한 트래픽 난분석화 기법은 에이전트를 기반으로 설계하여 산업 제어 시스템에 적용 시 다운타임을 최소화하였다. 또한 지연을 사용하지 않고 패킷 분할 및 병합 방식을 통해 공격자의 수신자 식별과 응답 산업 기기 식별을 저지할 수 있었으며, 트래픽양이 감소하더라도 일정한 성능과 난분석성을 유지하였다. 본 논문을 통해 산업 제어 시스템을 대상으로 한 트래픽 분석 공격을 보다 효율적으로 방어함으로써 네트워크 공격의 피해를 줄이고 추가적인 네트워크 공격을 차단할 수 있을 것으로 기대된다.

참 고 문 헌

[1] Derhab, Abdelouahid, et al. "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security." *Sensors* 19.14 (2019): 3119.

[2] Sajid, Anam, Haider Abbas, and Kashif Saleem. "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges." *IEEE Access 4* (2016): 1375-1384.

[3] Schoomaker, P. Supervisory control and data acquisition (SCADA) systems for command, control, communications, computer, intelligence, surveillance, and reconnaissance (c4isr) facilities. tech. rep., Headquarters, Department of the Army. USA Goverment, 2006.

[4] Koushik, Ashish N., and B. S. Rashmi. "4 th Generation SCADA Implementation for Automation." *International Journal of Advanced Research in Computer and Communication Engineering 5.3* (2016).

[5] Kaspersky, I. C. S. "Threat landscape for industrial automation systems." (1997).

[6] Prokupecz, Shimon, Tal Kopan, and S. Moghe. "Former official: Iranians hacked into New York dam." CNN, December 22 (2015).

[7] Maiziere, T. D. "Die lage der it-sicherheit in deutschland 2014." Bundesamt für Sicherheit in der Informationstechnik (2014).

[8] Zetter, Kim. "Inside the cunning, unprecedented hack of Ukraine's power grid." Wired Magazine 3 (2016).

[9] Verizon. "Data breach digest. Scenarios from the field." (2016).

[10] Assante, Michael J., and Robert M. Lee. "The industrial control system cyber kill chain." SANS Institute InfoSec Reading Room 1 (2015).

[11] Harakrishnan, Bhanu, et al. "Side-channel analysis for detecting protocol tunneling."

[12] Fu, Xinwen. On traffic analysis attacks and countermeasures. Diss. Texas A&M University, 2007.

[13] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* 24.2 (1981): 84-90.

[14] Wahal, Mrinal, and Tanupriya Choudhury. "Hydra－Anonymous network routing mechanism." 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS). *IEEE,* 2017.

[15] Stouffer, K. V. S. M., et al. "Guide to Industrial Control Systems (ICS) Security-NIST. SP. 800-82r2." NIST, US Department of Commerce, Gaithersburg, Maryland (2015): 1-247.

[16] Shirazi, Fatemeh, et al. "A survey on routing in anonymous communication protocols." *ACM Computing Surveys* (CSUR) 51.3 (2018): 1-39.

[17] Kesdogan, Dogan, Jan Egner, and Roland Büschkes. "Stop-and-go-MIXes providing probabilistic anonymity in an open system." *International Workshop on Information Hiding. Springer, Berlin, Heidelberg*, 1998.

[18] Diaz, Claudia, and Bart Preneel. "Taxonomy of mixes and dummy traffic." Information Security Management, *Education and Privacy. Springer,* Boston, MA, 2004. 217-232.

[19] Serjantov, Andrei, Roger Dingledine, and Paul Syverson. "From a trickle to a flood: Active attacks on several mix types." *International Workshop on Information Hiding. Springer,* Berlin, Heidelberg, 2002.

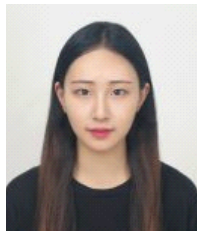
[20] Vukovic, Ognjen, Gyorgy Dan, and Gunnar Karlsson. "On the trade-off between relationship anonymity and communication overhead in anonymity networks." *2011 IEEE International Conference on Communications* (ICC). IEEE, 2011.

[21] Huang, Dijiang, and Vinayak Kandiah. "Low-latency mix using split and merge operations." *Journal of Network and Systems Management* 18.3 (2010): 244-264.

[22] Galloway, Brendan, and Gerhard P. Hancke. "Introduction to industrial control networks." *IEEE Communications surveys & tutorials* 15.2 (2012): 860-880.

〈저자소개〉

이 양 재 (Yangjae Lee)
학생회원
2018년 2월 : 세종대학교 정보보호학과 졸업
2018년 3월~현재 : 세종대학교 정보보호학과 석사과정
<관심분야> 클라우드, 트래픽 분석, 무선 충전 기술



정 혜 림 (Hye-Lim Jung)
학생회원
2015년 : 대전대학교 정보보호 학사
2017년 : 대전대학교 정보보호 석사
2019년 ~현재 :세종대학교 정보보호학과 박사과정
<관심분야> IoT, 스토리지, 헬스케어시스템 보안

안 성 규 (Sung-Kyu Ahn)
학생회원
2015년 : 전대학교 정보보호 학사
2017년 : 대전대학교 정보보호 석사
2017년~현재 : 세종대학교 정보보호학과 박사과정
<관심분야> IoT, 스토리지, 헬스케어시스템 보안

박 기 웅 (Ki-Woong Park)
종신회원
연세대학교 Computer Science 학사
KAIST Electrical Engineering 석사
KAIST Electrical Engineering 박사
2009년 : Microsoft Research, Network-Research Group, Graduate Research Fellow
2012년 : 국가보안기술연구소 연구원
2016년 : 대전대학교 정보보안학과 교수
2016년~현재 : 세종대학교 정보보호학과 교수
<관심분야> 시스템 보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식 등