# IoT 장비에 대한 Delay Attack 동향 분석

서영재* 조효진**

*숭실대학교(대학원생) **숭실대학교(교수)

# A Survey of Delay Attack on IoT Equipment

Yeongjae Seo* Hyojin Jo**

*Soongsil University(Graduate student) **Soongsil University(Professor)

**요 약**

최근 사물인터넷(Internet of Things)의 급속한 발전에 따라 스마트시티 시장의 규모가 성장하고 있다. 이에 IoT 환경에서 발생할 수 있는 다양한 공격 유형도 증가하고 있다. 그 중 Delay Attack은 연결된 장치 사이의 통신 지연을 악용하여 악의적인 공격을 시도하는 방법이다. 이러한 Delay Attack은 IoT 시스템의 보안 문제를 심각하게 증가시킨다. 본 논문은 IoT 환경에서 발생하는 Delay Attack에 대한 종합적인 이해를 돕고, 이러한 공격의 동향을 분석함으로써 IoT 환경에서 발생하는 지연과 이에 따른 잠재적 위험에 대한 인식을 높이는 데 기여한다.

## I. 서론

최근 사물인터넷(IoT, Internet of Things) 기술의 급속한 발전으로, IoT는 우리 생활에 연결된 장치들을 통해 상호작용하고 정보를 교환할 수 있는 스마트 환경을 만들어냈다. 글로벌 시장조사 기관인 마트앤마트는 2027년 전 세계 스마트시티 시장 규모가 1조 244억 달러에 이를 것으로 추산했으며, 14.9%의 연평균성장률을 기록할 것으로 추정했다[1]. IoT 기술 발전으로 생성된 스마트 환경이 삶을 윤택하게 만들지만, 동시에 새로운 보안 위협을 불러일으킨다.

IoT 장치와 시스템은 개인정보, 가정 보안, 비즈니스 프로세스 등 중요한 데이터와 기능을 처리하고 있다. IoT 장치의 고장, 해킹, 악성 소프트웨어 등의 공격으로 인해 서비스 중단이 발생하면 생활 편의성, 업무 효율성, 금전적 손실 등의 피해가 발생한다. 이에 IoT 보안은 개인과 기업에 중요한 문제로 대두되고 있다.

IoT 환경에서 발생하는 공격 중 Delay Attack이 주목받고 있다. Delay Attack은 공격자가 IoT 장치 또는 시스템의 정상적인 동작을 방해하거나 지연시키는 공격 방식이다. 이 공격은 스마트홈, 보안 시스템 등 다양한 산업 분야에서 중대한 위협으로 작용할 수 있으며, 공격자는 서비스 중단, 장치 기능의 제한 등 사용자들에게 피해를 줄 수 있다. IoT 장치의 수와 데이터의 양이 증가함에 따라 Delay Attack의 영향력 또한 증가할 것이다.

위와 같은 악의적인 공격을 막기 위해, 본 논문에서는 IoT 환경에서 발생할 수 있는 Delay Attack의 연구 동향을 분석하며, 이를 탐지하고 대응 방법을 정리하여 나타낸다.

본 논문은 다음과 같이 구성된다. 2장에서는 Smart Home System, IoT Server 및 Delay Attack에 관해 다루고, 3장에서는 IoT Delay Attack 기술 동향에 관해 다룬다. 마지막으로 4장에서는 결론을 맺는다.

## II. 배경지식

### 2.1 Smart Home System

Smart Home System은 IoT 기술을 이용하여 가정 내의 다양한 기기를 연결하고, 사용자가 스마트폰 장치를 통해 제어할 수 있는 시스템이다. 예를 들어, 이 시스템을 이용하여 조명,

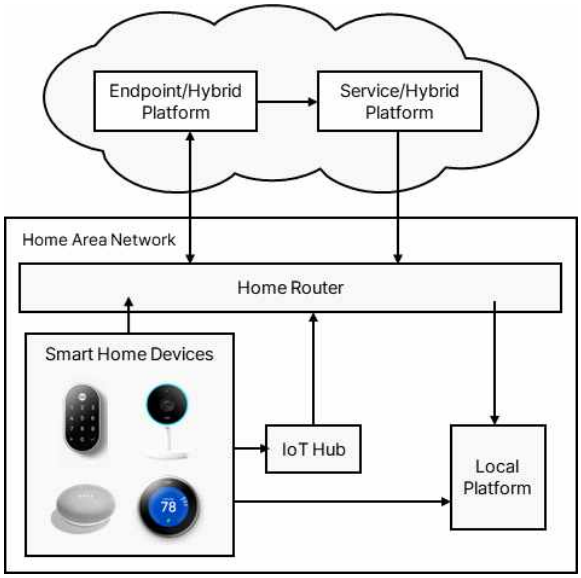


그림 1 Smart Home System Architecture

난방, 에어컨 등의 가전제품을 스마트폰으로 제어할 수 있으며, 카메라나 센서 등의 기기를 통해 설치 장소의 상황을 모니터링할 수 있다. IoT device, IoT Hub, Home Router 및 IoT Platform 등 다양한 구성요소가 포함되어 있으며, 그림 1은 Smart Home System의 아키텍처를 나타낸다.

### 2.2 IoT Server

IoT Server는 IoT 장치와 클라우드 기반 애플리케이션 간의 통신과 데이터 관리를 담당하는 중앙 서버 시스템이다. 이는 장치 간의 통신을 관리하며, 장치에서 생성된 데이터를 수집하고 처리한다. 또한 장치와 사용자 사이의 인터페이스 역할을 하여 사용자 웹 인터페이스나 앱을 통해 IoT Server에 접속하여 장치를 제어하거나, 장치에 생성된 데이터를 확인할 수 있다. IoT Server는 위치에 따라 IoT 서비스를 호스팅하는 Cloud Server과 로컬 장치에서 작동하는 Local Server로 분류할 수 있다. Cloud IoT Server는 IoT 장치 공급업체에서 운영하며 자체 장치와 직접 상호작용하는 endpoint 서버와 클라우드 간 통신을 사용하여 타사 IoT device와 간접적으로 상호작용하는 통합서버로 분류된다.

### 2.3 IoT Delay Attack

IoT Delay Attack은 악의적인 공격자가 IoT 장치 간 또는 중앙 서버 간의 정보 전송에 인위적으로 네트워크 또는 시스템의 동작을 지연시킴으로써 서비스를 방해하는 공격 방식이다. Delay Attack은 IoT 기반 시스템의 성능과 안정성에 심각한 영향을 미친다. 시스템의 응답 시간을 지연시키거나, 데이터 전송을 방해하거나, 심한 경우 전체 시스템의 기능을 완전히 마비시킬 수 있다.

과거 Delay Attack은 네트워크 트래픽을 불필요하게 증가시키는 방식으로 시스템의 작동을 방해하는 것과 같이 대체로 직접적이고 단순한 방식으로 이루어졌지만, IoT의 발전과 함께 고도화된 Delay Attack인 Delay-based Automation Interference Attack (DAI)[2]과 Phantom-Delay Attack[3]이 발표되었다. IoT 환경에 대한 고도화된 Delay 공격은 기존의 방어 메커니즘을 우회하거나 무력화시키는 데에 특히 효과적이다. 또한, Delay 공격은 특히 실시간 데이터 처리가 중요한 IoT 시스템에서 심각한 결과를 초래하며, 이에 따라 사회적, 경제적 손실이 발생할 수 있다.

## III. IoT Delay Attack 기술 동향

### 3.1 Delay-based Automation Interference Attacks(DAI Attack) [2]

[2]에서는 IoT 기반의 스마트홈에서 Delay-based Automation Interference (DAI) 공격이 가능하다는 것을 주장하고, 이를 방지하기 위한 대응책을 제안한다. DAI 공격은 스마트홈 자동화 시스템에서 발생하는 공격 유형으로, IoT 장치 간의 메시지 전송을 지연시켜서 스마트홈 자동화 시스템에서 불일치 및 불규칙성 문제를 악화시키는 공격이다. 해당 공격은 사용자가 자신의 스마트홈에 자동화 규칙을 잘못 구성할 때 발생하는 Cross-Rule Interference (CRI) 문제와는 달리 기존 방어 대응방안이 적용되지 않는 새로운 공격 방법으로, IoT 장치가 작동하지 않거나 다르게 동작하는 등 스마트홈 자동화 시스템에서 예기치 않은

| 공격 유형 | | | 설명 |
|---|---|---|---|
| DAI Attack [2] | Condition Overlapping Attack | Action Conflict | 서로 배타적인 조건을 가진 규칙이 동시에 실행되도록 만들어 규칙 간 충돌을 일으키는 공격 |
| | | Infinite Loop | 자동화 시스템에서 움직임-활성 이벤트를 지연하고, 무한 루프를 발생시켜 비정상적인 동작을 유발하는 공격 |
| | | Chained Execution | 하나의 규칙이 실행되면 그 결과로 다른 규칙이 자동으로 실행되어 비정상적인 동작을 유발하는 공격 |
| | Trigger-Cond. Overlapping Attack | | 서로 다른 규칙의 트리거와 조건이 상호 배타적이지만, 트리거 이벤트를 지연시켜 배타성을 깨고 두 규칙을 동시에 실행시켜 시스템의 비정상적인 동상을 유발하는 공격 |
| | Condition Diverging Attack | Disabled Parallel Execution | 병렬 실행 패턴에서 하나의 규칙이 다른 규칙의 트리거를 비활성화시켜 병렬 실행을 방해하고, Delayed Message Injection Attack과 Delayed Message Deletion Attack을 함께 사용하는 공격 |
| | | Disabled Chained Execution | 체인 실행 패턴에서 하나의 규칙이 다른 규칙의 트리거를 비활성화시켜 체인 실행을 방해하고, Condition Diverging Attack과 Delayed Parallel Execution 공격을 함께 사용하는 공격 |
| | Action Disordering Attack | | 서로 다른 규칙에서 발생한 명령어의 도착 순서를 변경하여, 시스템의 정상적인 동작을 방해하는 공격 |
| | Condition Disabling Attack | | 하나의 규칙이 다른 규칙의 조건을 불만족시키는 상태로 장치의 상태를 변경할 때, 시스템의 정상적인 동작을 방해하는 공격 |
| | Condition Enabling Attack | | 하나의 규칙이 다른 규칙의 조건을 만족시키는 상태로 장치의 상태를 변경할 때, 시스템의 정상적인 동작을 방해하는 공격 |
| | Action Delaying Attack | Disabled Parallel Execution | 여러 규칙이 동시에 실행되는 병렬 실행 환경에서 하나의 규칙이 다른 규칙의 실행을 지연시켜 시스템의 정상적인 동작을 방해하는 공격 |
| | | Disabled Chained Execution | 체인 실행 패턴에서 하나의 규칙이 다른 규칙의 트리거를 비활성화시켜 체인 실행을 방해하고, 이를 위해 Condition Disabling Attack과 Delayed Parallel Execution 공격을 함께 사용하는 공격 |
| IoT Phantom Delay Attack [3] | State-Update Delay Attack | | 이벤트의 발생 시간을 지연시켜서 사용자가 위험 상황을 인지하는 데 걸리는 시간을 늘리는 공격 |
| | Action Delay Attack | | 자동화 규칙의 트리거 이벤트와 액션 명령에 지연을 적용하여 액션을 지연시키는 공격 |
| | Erroneous Execution Attack | Spurious Execution | 실행되지 않아야 할 명령이 실행되는 공격 |
| | | Disabled Execution | 실행되어야 할 명령이 실행되지 않는 공격 |

표 1 Delay Attack 유형 분류

동작을 유발할 수 있다. 해당 연구에서는 DAI 공격 유형을 7가지로 분류하였으며, 이를 표 1에 나타내었다. [2]에서는 선택적 이벤트/명령 지연의 두 가지 공격 프리미티브를 활용하여, CRI 문제 분석에 지연을 통합한 새로운 스마트 홈 모델을 제시하였다.

해당 연구에서는 공격자가 스마트홈 시스템의 제어 획득, 상태 변경, 데이터 탈취 등 영향을 미칠 수 있으며 해당 공격은 사용자들에게 개인정보 유출, 악의적인 제어로 인한 안전 문제 및 재산상 손해 등의 위협을 가할 수 있음을 보였다. 두 개의 스마트홈을 대상으로 DAI 공격을 시뮬레이션하고, 이를 평가하기 위해 observation equivalence를 이용하여 DAI 공격을 식별하였다. 실험 결과, DAI 7가지의 모든 유형의 공격이 성공하였으며, 현재 IoT 프로토콜 스택의 어떤 레이어에서도 경고를 발생시키지 않고 공격할 수 있음을 보였다.

기존의 CRI 문제 해결 방법에 지연 요소를 추가하여 새로운 CRI 패턴을 발견하고, 이를 해결하기 위한 대응책을 제안하는 데 성공했음을 보여주었다.

### 3.2 IoT Phantom-Delay Attacks [3]

[3]에서는 IoT 자동화 시스템에서 발생하는 Timeout 동작에 대해 공격자가 스마트 환경에서 하나의 WiFi 장치를 제어함으로써 정상 IoT 장치의 메시지를 지연시키거나 악의적으로 자

동화된 작업을 비활성화, 활성화, 지연, 재정의할 수 있는 새로운 IoT Phantom-Delay Attack을 제안한다.

IoT 장치에서 발생하는 타임아웃 동작 취약점은 TCP+TLS로 구축된 IoT 장치의 중요한 설계 결함으로 작용한다. 해당 연구에서는 IoT 이벤트 및 명령 메시지 지연을 의미하는 IoT Event Message Delay (e-Delay)와 IoT Command Message Delay (c-Delay) 두 가지 공격 프리미티브를 이용하여 스마트홈에 대한 공격을 수행하는 방법을 제시한다. State-Update Delay, Action Delay, Erroneous Execution으로 분류한 공격을 표 1에 나타내었다.

해당 연구에서는 50개의 인기 있는 IoT 장치를 평가하였고, 이들 모두가 Phantom-Delay Attacks에 취약하다는 것을 보여주었다. 또한, 해당 연구에서는 이러한 공격에 대한 대응책도 논의하였으며, 여러 IoT 플랫폼에서 해당 취약점에 대해 알렸으며 일부 업체들은 문제를 인정했음을 보여주었다.

## IV. 결론 및 향후 연구 방향

본 논문에서는 IoT 환경에서 발생하는 Delay Attack의 유형을 분류하고 해당 공격들에 대한 대응방안을 표 2에 정리하였다. IoT 장치의 수가 증가하고, 생성 및 처리하는 데이터의 양이 증가함에 따라 이러한 Delay Attack의 영향력 또한 증가할 것이다. 하지만, 해당 공격과 기술들은 아직 초기 단계이므로 Delay Attack의 공격 특징과 패턴을 분석하고 이를 막기 위한 대응할 수 있는 새로운 보안 솔루션을 개발하여 안전하고 신뢰성 있는 IoT 환경을 구축해야 한다.

**ACKNOWLEDGEMENT** 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.00218853, 안전한 스마트홈 IoT 서비스를 위한 취약점 모니터링 연구)

| 공격 | 대응방안 |
|---|---|
| DAI Attack [2] | 스마트 홈 사용자는 다른 사람과 WiFi 네트워크를 공유하는 경우 강력한 WiFi 암호를 사용하고 IoT에 대해 격리된 하위 네트워크를 설정하여 공격자가 IoT 네트워크에 침입할 수 있는 기준을 높임 |
| | IoT 장치/허브 및 WiFi 라우터의 제조사는 제품의 보안을 강화해야 함 |
| | 장치 공급업체와 플랫폼 공급자는 TLS 보호 연결유지 메시지의 간격을 줄이고 이벤트 및 명령 메시지의 양방향 활성확인을 시행하여 허용된 지연을 크게 줄일 수 있음 |
| | TLS 보호 연결유지 메시지가 자주 발생하면 오버헤드가 높아지므로 IoT 설계에서 고려해야 함 |
| | 스마트 홈 시스템에서 배포정보를 추출하고 해당 정보를 공식 모델에 통합한 후, 관찰 동등성 기반 기술을 사용하여 CRI에 저항하는 규칙 쌍의 존재 여부를 확인함으로써 잠재적인 DAI 공격을 탐지할 수 있음 |
| IoT Phantom Delay Attack [3] | 기존 IoT 장치는 이벤트 메시지 승인에 대해 긴 제한 시간이 있으므로, 메시지 ACK 요구 및 ACK 타임아웃 단축해야 함 |
| | 타임스탬프 확인하여 지연된 트리거 이벤트로 인한 잘못된 실행을 방지할 수 있음 |

표 2 공격에 따른 대응방안

## [참고문헌]

[1] Smart Cities Market by Focus Area, Smart Transportation, Smart Buildings, Smart Utilities, Smart Citizen Services (Public Safety, Smart Healthcare, Smart Education, Smart Street Lighting, and E-Governance) and Region - Global Forecast to 2027, MarketsandMarkets, November, 2022

[2] Haotian Chi, Chenglong Fu, Qiang Zeng, Xiaojiang Du, “Delay Wreaks Havoc on Your Smart Home: Delay-based Automation Interference Attacks”, IEEE SP, 2022

[3] Chenglong Fu, Qiang Zeng, Haotian Chi, Xiaojiang Du, Siva Likitha Valluru, “IoT Phantom-Delay Attacks: Demystifying and Exploiting IoT Timeout Behaviors”, IEEE DSN, 2022