Journal of The Korea Society of Computer and Information
Vol. 24 No. 9, pp. 35-42, September 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.09.035

An Approach for Applying Network-based Moving Target Defense into Internet of Things Networks

Tae-Keun Park*, Kyung-Min Park**, Dae-Sung Moon**

Abstract

In this paper, we propose an approach to apply network-based moving target defense into Internet of Things (IoT) networks. The IoT is a technology that provides the high interconnectivity of things like electronic devices. However, cyber security risks are expected to increase as the interconnectivity of such devices increases. One recent study demonstrated a man-in-the-middle attack in the statically configured IoT network. In recent years, a new approach to cyber security, called the moving target defense, has emerged as a potential solution to the challenge of static systems. The approach continuously changes system's attack surface to prevent attacks. After analyzing IPv4 / IPv6-based moving target defense schemes and IoT network-related technologies, we present our approach in terms of addressing systems, address mutation techniques, communication models, network configuration, and node mobility. In addition, we summarize the direction of future research in relation to the proposed approach.

▸Keyword: Network-based moving target defense, internet of things, cyber security, attack surface

I. Introduction

IoT (Internet of Things)는 전자 장치와 같은 사물들의 높은 상호 연결성을 제공하는 기술이며, 인간의 삶을 혁신적으로 변화시킬 주요 기술 중 하나로 주목받고 있다 [1]. Gartner에 따르면 2020년 IoT로 연결되는 장치의 수가 거의 204억 개에 이를 것으로 예측되는데 [2], 많은 장치들의 상호 연결성이 높아짐에 따라 사이버 보안 위험성도 함께 증가할 것으로 예상되고 있다 [1].

IoT 네트워크에서의 사이버 공격을 시연한 연구 [3]에서는, IoT 네트워크에 악의적인 노드가 존재하는 경우, 외부 네트워크에 위치한 공격자가 악의적인 노드를 활성화 시킨 뒤, 중간자 공격 (Man-In-The-Middle attack)을 통해 IoT 네트워크의 로봇 팔을 악의적으로 제어할 수 있음을 보였다. 이와 같은 내부자 공격 (Insider Attack)은 신뢰할 수 없는 기관에 의해 제조되거나 프로그램된 장치에 의해 발생 가능한데, 일반적으로 IoT 네트워크를 구축할 때, Closed-Source Firmware가 로딩되어 있는 IoT 노드들이 포함될 수 있기 때문에, 이러한 종류의 내부자 공격은 현실적인 위협으로 인식되고 있다 [3].

공격자 우위의 시간적 비대칭성이란 설정이 정적으로 유지/관리되는 네트워크가 공격자들에게 목표 시스템의 취약점을 분석할 수 있는 충분한 시간을 제공하는 현상을 말한다 [4]. 최근 이러한 공격자 우위의 시간적 비대칭성을 극복하기 위하여, MTD (Moving Target Defense) 기법들이 개발되고 있다 [5].

MTD는 보호대상 시스템의 다양한 특징들을 시간의 변화에 따라 역동적으로 변경하여 각종 사이버 공격을 차단하는 능동

• First Author: Tae-Keun Park, Corresponding Author: Tae-Keun Park
*Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Applied Computer Engineering, Dankook University
**Kyung-Min Park (kmpark@etri.re.kr), Information Security Research Division, ETRI
**Dae-Sung Moon (daesung@etri.re.kr), Information Security Research Division, ETRI
• Received: 2019. 08. 07, Revised: 2019. 08. 26, Accepted: 2019. 08. 26.
• This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00213, Development of Cyber Self Mutation Technologies for Proactive Cyber Defense).
www.kci.go.kr

적 사전 보안 기술이다 [4]. MTD의 기술을 세분화하면, 첫째, 네트워크 특징 및 설정을 변경하는 네트워크 기반 MTD, 둘째, 시스템 플랫폼 특징을 변경하는 플랫폼 기반 MTD, 셋째, 런타임 환경 또는 응용 프로그램 코드를 변경하는 소프트웨어 기반 MTD, 넷째, 데이터의 포맷과 표현을 변경시키는 데이터 기반 MTD로 분류할 수 있다 [4-5].

본 논문에서는 이상의 MTD 기술 분류 중에서 네트워크 기반 MTD (NMTD: Network-based MTD)를 IoT 네트워크에 적용하는 접근 방법을 제안한다. 먼저, IPv4/IPv6 기반 NMTD 기법들과 IoT 네트워크 관련 기술들을 분석한 뒤, IoT 네트워크에 MNTD 기술을 적용할 때 고려해야 할 사항들에 대하여 서술한다 또한, 제안된 접근 방법과 관련하여 필요한 향후 연구 방향에 대하여 정리한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 전통적인 네트워크 인프라에서 동작하는 NMTD 기술에 대하여 간략히 살펴본 뒤, MT6D (Moving Target IPv6 Defense) 관련 기술 및 RPL (Routing Protocol for Low Power and Lossy Networks) 관련 기술을 소개한다. 제 3장에서는 IoT 네트워크에 NMTD 기술 적용을 위한 접근 방법을 제시하고, 제 4장에서는 추가적인 검토가 필요한 사항들에 대하여 정리한 뒤, 향후 연구 방향에 대하여 서술한다. 마지막으로, 제 5장에서 결론을 맺는다.

II. Related Works

본 장에서는, IoT 네트워크에 NMTD 기술을 적용하는 방안의 작성에 필요한 기술들을 크게 세 개의 부분으로 나누어 소개한다. 첫 번째는 전통적인 네트워크 인프라에서 동작하는 NMTD 기술이고, 두 번째는 MT6D 관련 기술이며, 세 번째는 RPL 관련 기술이다.

1. Network-based MTD

MTD는 보호대상 시스템의 다양한 특징들을 시간의 변화에 따라 역동적으로 변경하여 각종 사이버 공격을 차단하는 능동적 사전 보안 기술이다 [4]. 그 중에서, 네트워크 특징 및 설정을 변경하는 MTD를 네트워크 기반 MTD (NMTD: Network-based MTD)라고 분류한다. 본 절에서는 IPv4 기반의 전통적인 네트워크 인프라를 대상으로 하는 NMTD 기술들에 대하여 간략히 소개한다.

DYNAT (Dynamic Network Address Translation) [6]는 서버의 주소와 포트번호의 노출을 막기 위하여, 목적지 IP 주소의 네트워크 주소 부분을 제외한 나머지 정보를 모두 암호화하고 복호화한다. DYNAT는 암호 키 값 (Keying Parameter)이 시간에 따라 변화하는 NMTD 기법이다.

APOD (Applications that Participate in their Own Defense) [7]에서는, 패킷이 송신지 네트워크를 벗어날 때 패킷의 IP 주소와 포트번호를 각각 난수 발생기의 값들로 변경하고, 목적지 네트워크에 도착했을 때 동일한 난수 발생기를 활용하여 원래 IP 주소와 포트번호로 복원한다. 시간이 지남에 따라 난수 발생기의 값이 변경되기 때문에, APOD는 NMTD 기법으로 분류된다.

NASR (Network Address Space Randomization) [8]은 이미 작성된 웜 히트리스트 (Worm Hitlist)를 쓸모없게 만들기 위하여, 서버의 IP 주소를 빈번하게 바꾸는 기법이다. DHCP (Dynamic Host Configuration Protocol) 서버로부터 호스트들이 일정 시간 간격마다 새로운 주소를 임대하게 함으로써, 호스트의 IP 주소 변이 (Mutation)를 구현한다.

RHM (Random Host Mutation) [9]은 높은 예측불가능 (Unpredictability)를 제공하기 위하여, LFM (Low Frequency Mutation)과 HFM (High Frequency Mutation)을 사용한다. LFM은 각 서버에 할당될 수 있는 IP 주소의 범위를 바꾸는 변이이고, HFM은 LFM에서 할당된 IP 주소 범위에 속하는 하나의 IP 주소를 일정 시간 간격마다 각 서버에게 할당하는 변이이다. 즉, RHM은 서버의 IP 주소를 짧은 시간마다 바꾸기 위하여 HFM을 이용하고, 오랜 기간 모니터링하는 공격자에 대비하기 위하여 LFM을 이용하는 NMTD 방법이다.

DESIR (Decoy-Enhanced Seamless IP Randomization) [10]에서, 서버는 독립적인 노드로 존재하는 Randomization 컨트롤러로부터 일정 시간 간격마다 변경된 IP 주소를 할당받는다. 그리고, 서버는 새로운 주소를 할당받은 시점에 이미 서비스 중인 연결들이 끊어지지 않도록 마이그레이션 (Migration)한다. 정상적인 클라이언트는 인증 서버로부터 현재의 서버 IP 주소를 알아낼 수 있지만, 그렇지 못한 공격자의 패킷들은 디코이 (Decoy)에게 전달되도록 하여 공격자가 허튼 곳에 시간과 자원을 낭비하도록 하는 NMTD 기법이다.

HIDE (Host IDEntity anonymization) [11]는 전문적인 지식을 소유한 인간 공격자에 대한 방어를 위하여 제안된 기법이다. 기본적으로 HIDE의 NMTD 방법은 RHM과 동일하다. 그러나, HIDE는 목적지 주소가 서버의 IP 주소가 아닌 패킷들을 모두 디코이에게 전달하도록 한다. 서버와 동일한 서비스 목록을 제공하는 다수의 디코이를 배치하고 이에 대한 변이도 수행함으로써 서버의 핑커프린트 익명화와 변이 (Fingerprint Anonymization and Mutation)를 제공한다.

SSCM (Scalable and Seamless Connection Migration) [12]은 DESIR의 연결 마이그레이션의 확장성 문제를 해결하기 위하여 제안된 NMTD 방법이다. SSCM은 주소를 변이하는 호스트가 물리적으로 이동하는 것이 아니기 때문에 해당 호스트는 짧은 시간 동안 새로 할당받은 IP 주소뿐만 아니라 이전 IP 주소를 이용하여 패킷을 송수신할 수 있다는 사실에 근거하여 설계되었다. 그 결과, SSCM은 서버가 동시에 많은 수의 연결을 서비스하고 있는 경우, 연결 마이그레이션 때문에 발생하는 서비스 중지 시간을 DESIR에 비하여 월등히 줄일 수 있다.

www.kci.go.kr

HTN (Hidden Tunnel Networking) [13]은 1초 이내의 매우 짧은 주소 변이 주기 (Address Mutation Interval)에서도 서버가 주소 변이를 수행할 수 있는 것을 목표로 설계되었다. 주소 변이 주기가 짧다는 것은 이전의 스캐닝 공격을 통해 공격자가 획득한 정보의 유효기간이 짧아진다는 것을 의미한다. 이를 위하여, HTN은 첫 번째 단계에서 인증에 성공한 클라이언트와 서버는 익명 주소 생성에 사용되는 세션 키를 분배한 뒤, 두 번째 단계에서 익명 주소 생성 및 변이를 수행한다.

2. MT6D and Its Extension

앞 절에서 살펴본 NMTD 기술들은 모두 IPv4를 사용하는 전통적인 네트워크 인프라에서의 적용을 위해 개발된 것들이다. 그러나, IPv4의 주소 공간 크기가 2^{32}개에 불과하기 때문에, NMTD의 효과를 극대화하기 위하여 2^{128}개의 주소 공간 크기를 가지는 IPv6에서의 NMTD에 대한 연구가 진행되었다.

IPv6 [15] 주소는 세 개의 부분으로 구성된다. 상위 48비트는 라우팅 prefix이고, 그 다음 16비트는 서브넷 ID이며, 하위 64비트는 호스트 정보를 나타내는 IID (Interface Identifier)이다. IPv6를 두 개의 부분으로 나누어 설명하는 경우도 있는데, 이 경우에는, 상위 64비트는 라우팅을 위하여 사용되고, 하위 64비트는 호스트를 식별하는데 사용된다.

MT6D [14]는 버지니아 공대에서 개발한 NMTD 기술로서, 악의적인 노드의 탐지를 피하기 위하여 방대한 IPv6의 주소 공간 내에서 호스트의 주소를 임의로 이동시키는 기술이다. MT6D는 SLACC (Stateless Address Auto-Configuration) 프로토콜의 EUI-64 (Extended Unique Identifier-64) 주소 계산에 내제된 약점을 해결하기 위하여 설계되었다. SLACC에 내제된 약점이란 호스트가 인터넷의 어느 곳으로 이동하더라도 IPv6 주소의 하위 64비트인 IID가 고정적이라는 것이다. 왜냐하면, 이 고정적인 주소 부분을 활용하여, 악의적인 노드가 인터넷에서 특정 호스트를 추적할 수 있기 때문이다. MT6D는 IPv6의 고정적인 주소 부분을 제거하였을 뿐만 아니라, 몇 초에 한 번씩 IID를 변경할 수 있는 기능을 제공한다.

그러나 MT6D가 동적으로 IID를 계산하기 위해서는, 모든 구성 정보 (Configuration Information)가 정적으로 구성되고 배포되어 있어야 한다. 예를 들어, 임의의 두 피어는 서로 공유하는 비밀 키 (Shared Secret Key)와 상대 피어의 서브넷 주소를 미리 알고 있어야 한다. 이러한 제약은, 통신에 참여하는 노드의 수가 증가하면, 확장성과 보안 측면에서 문제를 야기할 수 있다. 또한, MT6D는 P2P (Peer-to-Peer) 통신만을 위하여 제안되었다. 이러한 제약 조건들을 극복하기 위하여, 클라이언트-서버용 MT6D 확장이 제안되었다 [16].

MT6D에서 구성 정보는 수동으로 배포될 뿐만 아니라 배포된 구성 정보는 정적 구성 파일에 보관된다. 이에 반하여, 클라이언트-서버용 MT6D 확장에서 구성 정보는 동적으로 생성되고 인증된 방식으로 네트워크를 통해 교환된다. 클라이언트-서버용 MT6D 확장은 구성 정보의 안전한 교환을 위하여, 블라인드 랑데부 (Blind Rendezvous) 기술을 활용한다. 블라인드 랑데부란 사전 지식 없이 피어를 찾는 방법을 의미한다 [16]. 클라이언트-서버용 MT6D 확장에서는 블라인드 랑데부를 위해 비트토렌트 (BitTorrent) DHT (Dynamic Hash Table)를 사용한다. 비트토렌트 DHT는 인터넷에서 사용 중인 대규모 개방형 분산 시스템 중 하나이며, 블라인드 랑데부와 정보 교환 등에 활용될 수 있다.

클라이언트-서버용 MT6D 확장에서, 서버는 특성 시간 구간 (Time Period) T 동안에 사용될 구성 정보를 생성하여 DHT에 게시한다. 구체적으로, 서버는 T 동안 사용될 디스크립터 (Descriptor) d_T와 메시지 (Message) m을 생성한다. 서버는 디스크립터를 생성할 때, 서버의 개인 키와 클라이언트의 공개 키를 사용하는데, ECDH (Elliptic Curve Diffie-Hellman) 함수 [17]의 특성 때문에, 클라이언트도 자신의 개인 키와 서버의 공개키를 이용하여 동일한 디스크립터 d_T를 생성할 수 있다. 서버가 생성한 메시지 m은 (1) 서버의 Seed IP 주소와 (2) MT6D 대칭 키 및 (3) 주소 회전 주기 (Rotation Period)를 서버의 개인 키로 전자 서명한 후, 클라이언트의 공개 키로 암호화하여 생성된다. 클라이언트가 생성된 메시지 m을 검색할 수 있도록, 서버는 디스크립터 d_T를 사용하여 DHT에 메시지 m을 게시한다.

클라이언트-서버용 MT6D 확장에서, 클라이언트는 자신이 연결하고자 하는 서버의 공개 키와 자신의 개인 키를 이용하여 디스크립터 d_T를 생성한 뒤, DHT에서 검색하여 서버의 메시지 m을 획득한다. 그런 다음, 클라이언트는 자신의 개인 키와 서버의 공개 키를 이용하여 메시지의 암호를 해독하고 메시지의 유효성을 검증한다. 결과적으로, 클라이언트는 서버가 특성 시간 구간 (Time Period) T 동안에 사용할 구성 정보인 (1) 서버의 Seed IP 주소와 (2) MT6D 대칭 키 및 (3) 주소 회전 주기를 획득하게 된다.

이제 클라이언트는 서버의 Seed IP 주소와 주소 회전 주기 및 MT6D 대칭 키를 이용하여, 서버가 자신을 위해 Listen 중인 IPv6 주소를 계산할 수 있다. 이 주소를 통해, 클라이언트가 서버에 초기 접속을 시도하면, 클라이언트와 서버는 공개 키와 개인 키를 사용하여 서로를 인증한 뒤, 새로운 세션 키를 나누어 가진다. 이후, 이 새로운 세션 키를 사용하여, 특정 클라이언트와 서버 사이에서만 유효한 MT6D 주소 집합을 생성한 뒤, 클라이언트와 서버는 NMTD 방식에 따라 주소를 변이한다.

지정된 시간 구간 T가 끝나면, 서버는 새로운 시간 구간 동안 사용될 디스크립터 d_T와 메시지 m을 새로 생성한 뒤, DHT에 다시 게시한다. 클라이언트는 새로 게시된 메시지 m을 DHT로부터 획득한 뒤, 이상에서 서술한 동작을 반복한다.

클라이언트-서버용 MT6D 확장에서, 원래 MT6D의 구성은 두 호스트 (클라이언트와 서버)간의 소개 동작을 위한 수단으로만 사용됨에 주의할 필요가 있다. 서버는 확장성을 위하여, 여러 클라이언트를 위하여 Listen하는 주소를 하나 생성한 뒤, 이를 메시지 m에 포함시켜 게시한다. 그러면, 서버는 여러 클라

www.kci.go.kr

이언트들의 초기 접속을 위한 오직 하나의 MT6D 주소 집합만 유지하면 되며, 이는 서버의 자원을 절약할 수 있도록 해준다. 초기 접속을 위한 MT6D 주소 집합의 현재 IPv6 주소로 특정 클라이언트가 접속해 오면, 서버는 그 클라이언트와 새로운 세션 키에 동의한 뒤, 앞서 언급한 바와 같이, 클라이언트와 서버는 동의된 새로운 세션 키를 이용하여 새로운 MT6D 주소 집합을 생성하고 통신을 수행한다.

3. RPL

MT6D와 클라이언트-서버용 MT6D 확장에서 언급되지는 않았지만, IoT 네트워크에 MTD를 적용하기 위해서는 IoT 네트워크에 사용될 라우팅 프로토콜의 특성을 이해할 필요가 있다.

모든 IoT 네트워크가 저전력 및 손실 네트워크 (LLN: Low Power and Lossy Networks)일 수는 없겠지만, 배터리로 동작하는 사물들로 구성된 무선 네트워크는 일반적으로 저전력 및 손실이 발생 가능하다는 특성을 가진다. 이러한 특성을 가지는 멀티 홉 메시 네트워크 (multi-hop mesh networks)에서 다양한 응용 프로그램들을 지원하는 대표적인 IPv6 라우팅 프로토콜이 RPL (Routing Protocol for Low Power and Lossy Networks)이다 [18].

RPL은 트리 형태의 라우팅 토폴로지를 사용하며, 루트 노드를 시작점으로 하는 DODAG (Destination-Oriented Directed Acyclic Graph)를 생성한다. DODAG를 구성하는 RPL 노드는 라우팅 기능의 유/무에 따라 라우터 노드와 리프 노드로 구분된다. 라우터 노드는 라우팅 기능을 제공하는 노드이고, 리프 노드는 라우팅 기능을 가지지 않는 노드이다.

RPL에서 라우팅은 DODAG 루트로부터 RPL 노드 방향의 하향 라우팅과 반대 방향의 상향 라우팅으로 구성된다. 상향 경로 설정은 RPL 노드들이 DODAG 루트 노드 방향으로 부모 노드를 선택함으로써 설정되고, 하향 경로 설정은 저장 모드 (Storing Mode) 또는 비저장 모드 (Non-Storing Mode) 중 하나의 모드에 따라 설정된다.

저장 모드로 동작할 때, 라우터 노드는 하향 경로용 라우팅 정보를 라우팅 테이블로 저장한다. 이에 반하여, 비저장 모드로 동작할 때, 하향 경로 통신을 위한 라우팅 정보는 DODAG 루트에 모두 보관되며, 루트 노드가 각 패킷에 삽입한 라우팅 경로 정보에 따라, 라우터 노드들은 소스 라우팅 (Source Routing) 방식으로 패킷을 라우팅한다. 이 두 가지 모드는 각각 단점을 가지고 있다. RPL 노드의 수가 늘어남에 따라, 저장 모드로 동작하는 RPL 라우터 노드는 라우팅 테이블의 크기 증가에 의한 메모리 부족 현상이 발생할 수 있고, 비저장 모드로 동작하는 네트워크에서는 소스 라우팅의 사용에 따른 트래픽 오버헤드 증가 및 많은 패킷 단편화가 발생할 수 있다.

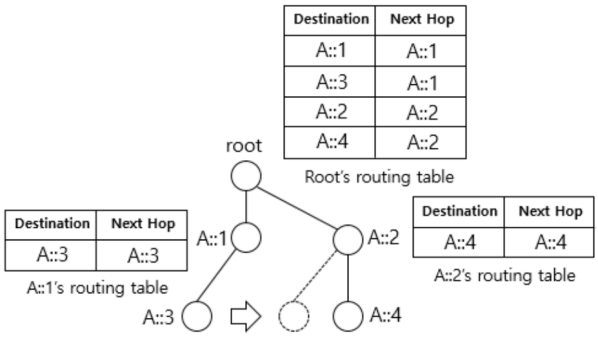

Fig. 1. State of the Routing Table according to the Movement of a Mobile Node in the Storing Mode [19]

RPL 노드가 모바일 노드라면 저장 모드에서는 또 다른 문제가 발생할 수 있다. 그림 1은 저장 모드에서 모바일 노드의 이동에 따른 RPL 라우터 노드의 라우팅 테이블 예를 보여 준다 [19].

그림 1에서 리프 노드 A::3이 라우터 노드 A::2 방향으로 이동하기 전에는 A::3을 위한 하향 라우팅 정보가 라우터 노드 A::1의 라우팅 테이블에 저장되어 있다. 그런데, 리프 노드 A::3이 라우터 노드 A::2에게로 이동하게 되면, 리프 노드 A::3을 위한 하향 라우팅 정보는 라우터 노드 A::1 뿐만 아니라 A::2의 라우팅 테이블에 모두 존재하는 현상이 발생하게 된다. 이와 같은 모바일 노드의 움직임이 증가하면, 라우터 노드의 가용 메모리 양은 급격히 감소하게 된다. 라우터 노드들의 저장 공간이 부족해지면, 결국 라우팅 실패로 이어질 수 있다.

RPL의 저장 모드와 비저장 모드에서 발생 가능한 문제를 해결하기 위하여 몇 개의 연구가 진행되었는데, 그 중에 하나가 하이브리드 하향 라우팅 모드 (Hybrid Downward Routing Mode) [19]이다.

하이브리드 하향 라우팅 모드의 핵심은 DODAG에서 리프 노드로의 라우팅 정보와 라우터 노드로의 라우팅 정보를 서로 분리하여 저장하고 관리하는 것이다. 리프 노드로의 라우팅 정보는 비저장 모드와 마찬가지로 DODAG 루트 노드에 저장되는 반면에, 라우터 노드로의 라우팅 정보는 저장 모드와 마찬가지로 라우터 노드에 저장된다. 이러한 정보의 분리는 RPL 노드의 수가 늘어나더라도 라우터 노드의 메모리 부족 현상 발생을 완화할 수 있다.

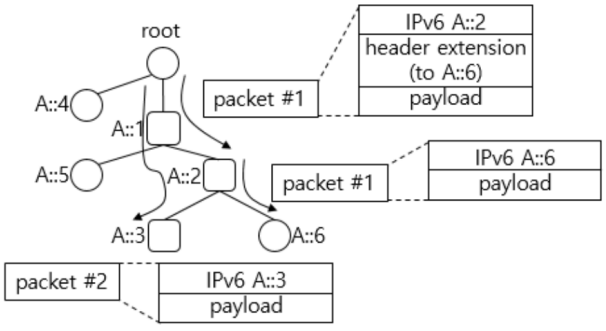

Fig. 2. An Example of Downward Packet Transmission in the Hybrid Mode [19]

www.kci.go.kr

그림 2는 하이브리드 하향 라우팅 모드에서의 하향 라우팅 경로로 패킷을 전송하는 예를 보여준다 [19]. 그림 2에서 사각형 노드는 라우터 노드이고, 루트 노드를 제외한 원형 노드는 리프 노드이다. 하이브리드 하향 라우팅 모드에서 라우터 노드의 라우팅 테이블에는 라우터 노드들에 대한 정보만 저장되어 있다. 따라서, 루트 노드가 리프 노드 A::6에게 패킷 #1을 전송하고자 하는 경우, 목적지 주소는 라우터 노드 A::2로 지정되고, 헤더 확장 영역에 최종 목적지가 리프 노드 A::6임을 명시되어 전송된다. 그러면, 패킷 #1은 라우터 노드 A::2에 도착할 때까지 저장 모드와 동일하게 라우팅 되다가, 확장 헤더가 존재함을 인식한 라우터 노드 A::2에 의해 패킷 #1의 목적지 주소가 리프 노드 A::6로 변경된다. 만일 패킷 #2와 같이 목적지가 라우터 노드 A::3이라면, 헤더의 확장 영역은 사용되지 않는다.

이와 같이 동작하는 하이브리드 하향 라우팅 모드에서는 리프 노드가 이동하더라도 그림 1에서 살펴본 문제가 발생하지 않는다. 그러나 리프 노드 이동에 따른 라우팅 정보 관리를 위한 메시지 교환 절차는 여전히 필요하다. 왜냐하면 이동한 리프 노드가 DODAG 루트 노드로의 상향 라우팅 경로 설정을 위한 메시지 교환이 필요할 뿐만 아니라, 하향 라우팅 경로 설정을 위해 DODAG 루트 노드로의 정보 전송이 필요하기 때문이다. 본 논문에서는 저장 모드, 비저장 모드, 하이브리드 모드에서의 라우팅 정보 관리를 위한 구체적인 메시지 교환에 대해서 소개하지 않는다.

III. The Proposed Approach

IoT 네트워크에서의 사이버 공격을 시연한 연구 [3]에서 중간자 공격의 가능성을 증명하기 위하여 구축한 플랫폼의 구성도는 그림 3과 같다.

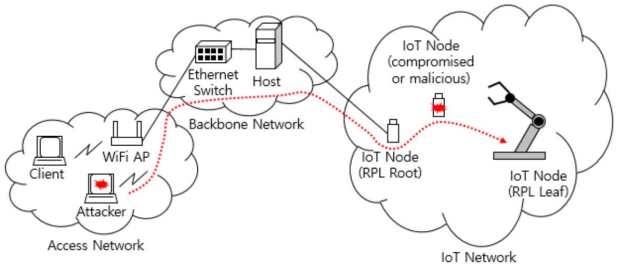

Fig. 3. A Small IoT Platform Illustrating a Man-In-The-Middle Attack

악의적인 코드를 포함하고 있는 노드가 IoT 네트워크를 구축하는 단계에서 설치되었고, 이 노드는 외부의 공격자가 명령을 내릴 때까지 정상적인 노드처럼 동작한다고 가정하자. 이 악의적인 노드는, 정상적인 노드처럼 동작하면서, RPL의 라우팅 토폴로지에서 루트 노드에 가능한 가까운 라우터 노드로 선택되고자 노력한다. 이는 Rank Attack, Version Number Attack 등과 같이 RPL 취약성을 악용함으로써 달성할 수 있다 [3]. 결과가 성공적이면 악의적인 노드는 공격자가 원하는 시점에 여러 가지 공격을 시도할 수 있게 된다. 공격자는 악의적인 노드의 특정 리소스에 HTTP 요청을 보내는 방식으로 악의적인 동작을 활성화시킬 수 있다. 활성화된 악의적인 노드는 전송 중인 메시지를 중간에서 수정할 수 있을 뿐만 아니라, Black-Hole Attack 및 정보 유출 (Information Leakage)과 같은 공격도 수행할 수 있다 [3].

실제 공격에 앞서 공격자는 공격할 목표 시스템에 대하여 정보를 상세하게 수집하고 취약점을 분석하는 정찰 (Reconnaissance) 단계를 수행하여야 한다. 대부분의 네트워크에서는 설정이 정적으로 유지/관리되는데, 이러한 네트워크에서 공격자는 충분한 시간을 가지고 목표 시스템의 취약점을 사전에 분석할 수 있다. 이러한 현상을 공격자 우위의 시간적 비대칭성이라고 하며, 이를 극복하기 위하여 앞서 살펴본 여러 NMTD 기법들이 제안되었다. 하지만 기존의 NMTD 기법들은 전통적인 네트워크 인프라 또는 SDN (Software-Defined Network) 환경을 위해 개발된 것이기 때문에, 이들 기법들을 수정없이 IoT 네트워크에 적용하기는 어렵다. 따라서 본 장에서는 IoT 네트워크에 NMTD의 적용을 위해 고려해야 할 사항들에 대하여 살펴보면서 어떻게 접근하는 것이 적절한 지에 대하여 정리한다.

먼저, IoT 네트워크에서 사용할 주소 체계를 결정하여야 한다. IPv6 주소 체계가 제안된 이후 많은 시간이 지났지만 실제 네트워크에서는 여전히 IPv4 주소 체계가 사용되고 있다. 따라서 앞서 관련 연구에서 살펴본 바와 같이 대부분의 NMTD 기법들은 IPv4 주소 체계의 사용을 가정하고 있다. 하지만 연결되는 장치의 수가 급격히 늘어날 것으로 예상되는 IoT 네트워크에서는 IPv6 주소 체계의 사용을 가정하는 것이 보다 현실적이다. 또한, NMTD의 효과를 극대화하기 위해서는 2^{128}개의 주소 공간 크기를 가지는 IPv6 주소 체계의 사용이 필수적이다. 따라서 본 접근 방법에서는 IoT 네트워크에서 사용할 주소 체계로 IPv6를 선택한다.

다음으로, 기존의 NMTD 기법 중 어떤 기법을 기본적으로 적용할 기법으로 선택할 것인지를 결정하여야 한다. 앞서 IPv6를 사용할 주소 체계로 결정하였기 때문에, NMTD에 참여하는 호스트가 변이할 주소를 스스로 계산하는 것이 고려된 NMTD 기법이 대상으로 고려되어야 한다. 이에 해당하는 NMTD 기법으로는, 앞서 살펴본, MT6D[14]와 클라이언트-서버용 MT6D 확장 [16]이 존재한다. 그러나 MT6D는 구성 정보가 정적으로 구성되고 배포되어야 하기 때문에, 통신에 참여하는 노드의 수가 증가함에 따라, 확장성과 보안 측면에서 문제를 야기할 수 있다. 따라서 본 접근 방법에서는 클라이언트-서버용 MT6D 확장 [16]을 IoT 네트워크에 적용할 기본 NMTD 기법으로 선정한다.

그림 3의 시나리오에서 액세스 네트워크에 존재하는 클라이언트는 IoT 네트워크의 로봇 팔에게 직접 메시지를 전송한다.

www.kci.go.kr

이와 관련하여 결정해야 할 사항은 IoT 네트워크의 노드 (로봇 팔)와 외부의 클라이언트가 P2P 통신 모델로 메시지를 교환할 것인지, 아니면 클라이언트-서버 통신 모델로 메시지를 교환할 것인지 여부이다. 앞서 기본 NMTD 기법으로 결정된 클라이언트-서버용 MT6D 확장 [16]은 두 가지 모델 모두에서 동작 가능하므로, 이 사항에 대해서는 본 장에서 결정하는 대신에, 다음 장에서 두 가지 모델의 사용에 대하여 추가적으로 분석하도록 한다.

다음으로 결정해야 할 사항은 IoT 노드의 주소 변이 (Address Mutation)가 IoT 네트워크에서의 경로 변경을 허용하는 형태로 이루어질 것인지에 대한 여부이다. 전통적인 네트워크 인프라에서 동작하는 NMTD 기법들은 하나의 서브넷 내에서의 주소 변이를 주로 고려한다. 왜냐하면, 다른 서브넷 주소로의 주소 변이는 중간 라우터들의 라우팅 테이블 업데이트를 필요로 하기 때문이다. 이러한 이유로 높은 예측불가능을 제공하는 것이 목표였던 RHM [9]은 LFM (Low Frequency Mutation)과 HFM (High Frequency Mutation)라는 두 개의 주소 변이를 사용하였다. 그리고 LFM 마다 MG (Media Gateway)들이 IGP (Integior Gateway Protocol)을 이용하여 라우팅 테이블을 업데이트하도록 하였다.

IoT 네트워크에서 사용할 주소 체계로 IPv6를 선택하였기 때문에, 하나의 서브넷 내에서 변이 가능한 주소의 수가 최대 2^{64}개로 매우 크기는 하지만, 그림 3에서와 같이 악의적인 노드가 RPL 경로의 라우터 노드로 존재하는 경우, RPL 리프 노드는 주소 변이를 수행하더라도 상향/하향 경로가 정적이라면, 악의적은 노드의 영향권을 완전히 벗어날 수는 없다. 따라서 본 접근 방법에서는 IoT 네트워크에서 하나의 RPL 노드가 여러 개의 DODAG에 속할 수 있어야 한다고 결정한다.

하나의 네트워크에는 하나 이상의 RPL 인스턴스가 존재할 수 있으며, 하나의 RPL 노드는 동시에 여러 개의 RPL 인스턴스에 참여할 수 있다 [20]. 그림 4는 하나의 RPL 노드가 두 개의 RPL 인스턴스에 동시에 참여하는 예를 보여준다. 그림 4에서 리프 노드 A::13과 A::17은 동일한 노드이다.

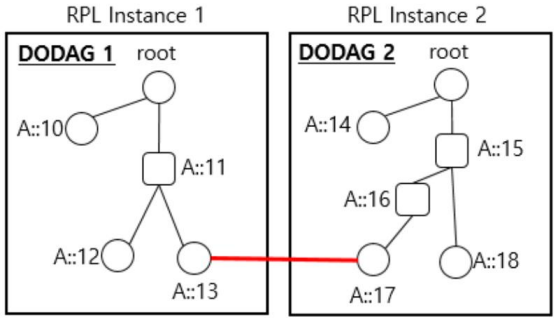

Fig. 4. RPL Network with Two Instances and Two DODAGs

IoT 네트워크에 NMTD가 적용된다면, 그림 4에서 동일한 노드인 A::13과 A::17은 특정 시간에 어느 하나만 활성화되어 있는 형태로 보여져야 한다. 즉, 클라이언트-서버용 MT6D 확장 [16] 기법이 적용된 경우, 해당 노드가 현재의 주소로 A::13를 사용한다면, 그 시점에 주소 A::17은 사용 중이지 않거나 허니팟 (Honeypot)으로 포워딩하는 용도로 사용되어야 한다.

이와 같은 방법으로, RPL 리프 노드가 시간의 변화에 따라 RPL 인스턴스 사이를 옮겨 다닐 수 있다면, 그림 3에서와 같이 악의적인 노드가 RPL 라우터 노드로 자리 잡고 있는다 할지라도 NMTD 기법의 사용을 통하여 리프 노드는 악의적인 노드의 영향권을 일정 시간 동안 완전하게 벗어날 수 있게 된다.

하지만, RPL 관련 연구에서 살펴본 바와 같이, RPL 루트 노드로부터 RPL 리프 노드로의 적절한 하향 경로 관리 방법이 제시되지 않으면, 문제를 야기할 수 있다. 이에 대해서는 다음 장에서 살펴 보도록 한다.

IV. Discussion

본 장에서는 제안하는 접근 방법과 관련하여 보다 구체적으로 살펴보아야 할 두 가지 사항에 대하여 정리한 뒤, 향후 연구 방향에 대하여 서술한다.

첫 번째 사항은 그림 3의 시나리오에서 액세스 네트워크에 존재하는 클라이언트와 IoT 네트워크의 노드 (로봇 팔) 사이의 통신 모델에 대한 것이다. 본 논문에서 제안하는 접근 방법에서는 클라이언트-서버용 MT6D 확장 [16]을 기본 기법으로 결정하였기 때문에, P2P 모델과 클라이언트-서버 모델 모두 구현 가능하다.

먼저 P2P 모델의 경우, 외부 연결을 허용하는 RPL 노드들은 블라인드 랑데부를 위하여 디스크립터와 메시지를 생성하여 DHT에 게시하여야 한다. 이에 반하여, 그림 3의 백본 네트워크에 MT6D 서버를 두는 경우, RPL 노드들이 블라인드 랑데부를 위하여 디스크립터와 메시지를 생성하여 DHT에 게시할 필요는 없다. 대신에 백본 네트워크의 서버가 RPL 노드들을 위하여 디스크립터와 메시지를 생성하여 DHT에 게시하면 된다. 즉, 블라인드 랑데부를 위한 동작이 백본 네트워크와 IoT 네트워크에 제한된다. 보안 측면에서 볼 때, RPL 노드들과의 블라인드 랑데부를 위한 구성 정보들이 액세스 네트워크로 전달될 필요가 없는 클라이언트-서버 모델이 보다 선호될 수 있다.

하지만, 백본 네트워크의 MT6D 서버가 단일 고장점 (Single Point of Failure)이 될 수 있다. 이 문제를 해결하기 위해서 여러 대의 MT6D 서버를 구축하고, MT6D 서버들의 보호를 위하여 전통적인 네트워크 인프라에서의 NMTD 기법을 적용하는 방법을 생각해 볼 수 있다.

두 번째 사항은 RPL 리프 노드가 시간의 변화에 따라 여러 RPL 인스턴스 사이를 옮겨 다님에 의하여 야기되는 하향 경로 관리의 오버헤드에 대한 것이다. 앞서 살펴본 하이브리드 하향 라우팅 모드를 사용한다면, 저장 모드와 비저장 모드를 사용하

www.kci.go.kr

는 것보다는 오버헤드가 줄어들 것으로 예상되지만, 이와 관련하여 여러 환경에서 시뮬레이션을 수행해 볼 필요가 있다.

따라서 향후 연구에서는 시뮬레이션을 통하여, RPL 리프 노드가 시간의 변화에 따라 여러 RPL 인스턴스 사이를 옮겨 다닐 때 저장 모드, 비저장 모드, 하이브리드 모드의 성능을 분석하고, 필요시 새로운 기법을 개발할 계획이다. 또한, 개념 증명 구현 (Proof of Concept Implementation)을 통해 P2P 모델과 클라이언트-서버 모델의 적합성을 비교 분석할 계획이다.

V. Conclusions

IoT 네트워크의 등장으로 인간의 삶이 혁신적으로 변화할 것으로 기대되고 있다. 그러나 IoT 네트워크를 구성하는 전자 장치들의 수가 많아지고 상호 연결성이 높아짐에 따라 사이버 보안 위험성도 함께 증가할 것으로 예상된다. 본 논문에서는 IoT 네트워크에서 공격자 우위의 시간적 비대칭성을 극복하기 위하여, IoT 네트워크에 NMTD 기술 적용을 위한 접근 방법을 제시했다. 제안하는 접근 방법에서, IoT 네트워크에서의 주소 체계는 IPv6이고, 기본적인 NMTD 기법은 클라이언트-서버용 MT6D 확장 기법이며, RPL 노드는 동시에 여러 인스턴스에 참여하도록 제안되었다. 아직, RPL 리프 노드가 시간의 변화에 따라 여러 RPL 인스턴스 사이를 옮겨 다니는 것을 허용하기에 가장 적합한 하향 경로 관리 방법을 결정하지 못하였고, 액세스 네트워크에 존재하는 클라이언트와 IoT 네트워크의 노드 (로봇 팔) 사이의 통신 모델로 무엇이 더 적합한지 판단하지 못하였다. 이 두 가지 사항에 대하여 향후 연구를 수행할 계획이다.

REFERENCES

[1] M. F. Razali, M. N. Razali, F. Z. Mansor, G. Muruti, and N. Jamil, “IoT Honeypot: A Review from Researcher’s Perspective,” Proceedings of the 2018 IEEE Conference on Applications, Information and Network Security, pp. 93-98, Nov. 2018.

[2] J. Rivera and R. van der Meulen, “Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015,” http://www.gartner.com/newsroom/id/2905717.

[3] R. E. Navas, H. L. Bouder, N. Cuppens, F. Cuppens, G. Z. Papadopoulos, “Demo: Do Not Trust Your Neighbors! A Small IoT Platform Illustrating a Man-in-the-Middle Attack,” Proceedings of the 17th International Conference on Ad Hoc Networks and Wireless, pp. 120-125, September 2018.

[4] K. Kang, T. Park, and D. Moon, “Analysis of Threat Model and Requirements in Network-based Moving Target Defense,” Journal of The Korea Society of Computer and Information, Vol. 22, No. 10, pp. 83-92, October 2017.

[5] T. Park, K. Park, and D. Moon, “Design of a Protected Server Network with Decoys for Network-based Moving Target Defense,” Journal of The Korea Society of Computer and Information, Vol. 23, No. 9, pp. 57-64, September 2018.

[6] D. Kewley, R. Fink, J. Lowry and M. Dean, “Dynamic Approaches to Thwart Adversary Intelligence Gathering,” Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 176-185, August 2001.

[7] M. Atighetchi, P. Pal, F. Webber and C. Hones, “Adaptive Use of Network-Centric Mechanisms in Cyber-Defense,” Proceedings of the sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, pp. 183-192, 2003.

[8] S. Antonatos, P. Akritidis, E. P. Markatos, K. G. Anagnostakis, “Defending against Histlist Worms using Network Address Space Randomization,” Computer Networks, vol.51, no.12, pp.3471-3490. August 2007.

[9] J. H. Jafarian, E. Al-Shaer and Q. Duan, “An Effective Address Mutation Approach for Distructing Reconnaissance Attacks," IEEE Transactions on Information Forensics, vol.10, no.12, pp. 2562-2577, August 2015.

[10] J. Sun and K. Sun, “DESIR: Decoy-enhanced seamless IP randomization," Proceedings of the IEEE INFOCOM, 2016.

[11] J. H. Jafarian, A. Niakankahiji, E. Al-Shaer and Q. Duan, “Multi-dimensional Host Identity Anonymization for Defeating Skilled Attacks," Proceedings of the 2016 ACM Workshop on Moving Target Defense, pp. 47-58, 2016.

[12] T. Park, K. Kang, and D. Moon, “A Scalable and Seamless Connection Migration Scheme for Moving Target Defense in Legacy Networks,” IEICE Trans. Inf. & Syst., In Press, Vol.E101-D, No.11, November 2018.

[13] K. Park, S. Woo, D. Moon, K. Koo, I. Kim, and J. Lee “Pseudonym Address based Hidden Tunnel Networking for Network Address Mutation,” KOREA Patent App. No. 10-2018-0076029, 2018.

[14] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, “MT6D: a moving target IPv6 defense,” Proceedings of the Military Communications Conference, pp. 1321-1326, 2011.

[15] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specication,” RFC 2460, December 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935,

www.kci.go.kr

6946.
[16] C. F. Morrell, “Improving the Security, Privacy, and Anonymity of a Client-Server Network through the Application of a Moving Target Defense,” Doctoral Dissertation in Computer Engineering, Virginia Tech Blacksburg, Virginia, USA, 2016.
[17] D. J. Bernstein, "Curve25519: new die-hellman speed records," Proceedings of the 9th Iternational Conference on Theory and Practice in Public Key Cryptography, pp. 207-228, Springer, 2006.
[18] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks," RFC 6550, 2012.
[19] S. Oh, D. Y. Hwang, K. Kim, and K. H. Kim, “A hybrid mode to enhance the downward route performance in routing protocol for low power and lossy networks,” International Journal of Distributed Sensor Networks, Vol. 14(4), April 2018.
[20] A. Kamble, V. S. Malemath, and D. Patil, “Security Attacks and Secure Routing Protocols in RPL-based Internet of Things: Survey,” Proceedings of 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), pp.33-39, Feb. 2017.

Authors

Tae-Keun Park received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea in 1991, 1993, and 2004, respectively. He joined POSTECH PIRL in 1993 and moved to SK Telecom in 1996. From 2000 to 2001 and from 2001 to 2002, he worked for 3Com Korea and Ericsson Korea, respectively. In 2004, he joined in the department of Multimedia Engineering, Dankook University, Korea. He is currently on the faculty of the department of Applied Computer Engineering at Dankook University. His research interests include network security, IoT, wireless/mobile communications, and distributed services.

Kyung-Min Park received his B.S., M.S., and Ph.D. degree in Computer Engineering from Chungnam National University, Rep. of Korea, in 2010, 2013, and 2019. He joined the Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea, in 2017. His research include network protocols & security, network middleware, and distributed computing.

Dae-Sung Moon received his MS degree in computer engineering from Pusan National University, Rep. of Korea, in 2001. He received his PhD degree in computer science from Korea University, Seoul, Rep. of Korea, in 2007. He joined the Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea, in 2000, where he is currently working as the director of Network&System Security Research Section. He has also been a Chief major professor with the Department of Information Security Engineering, University of Science and Technology, Daejeon, Rep. of Korea. His research interests include network security, machine learning, biometrics, and image processing.

www.kci.go.kr