*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.655

# IPv6 기반의 사물인터넷 환경에서 악성 노드의 패킷 유실 공격 탐지 및 우회 기법 분석*

최 재 우,† 권 태 경‡
연세대학교 정보보호연구실

# An Analysis of Detection of Malicious Packet Dropping and Detour Scheme in IoT based on IPv6*

Jaewoo Choi,† Taekyoung Kwon‡
Information Security Lab, Graduate School of Information, Yonsei University

요 약

본 논문에서는 IPv6를 적용한 표준인 IEEE 802.15.4e와 RPL을 기반으로 하는 사물인터넷 환경에서 가용성을 확보하기 위하여 패킷 유실 공격 탐지 기법과 우회 기법을 제안한다. RPL의 순위값과 패킷 유실 연속성을 고려하여 패킷 유실 탐지 메트릭을 개선하였고 RPL을 통해 생성된 라우팅 경로에서 형제노드 및 자식노드를 활용한 우회기법을 구성하였다. 시뮬레이션을 통해 제안한 탐지 기법의 탐지 속도가 향상되었음을 확인하였고 제안한 우회 기법의 우회 성공률이 향상되었음을 확인하였다.

ABSTRACT

In this paper, we propose new detection and detour methods against packet drop attacks for availability in the Internet of Things (IoT) based on the IEEE 802.15.4e and RPL protocol standards that employ IPv6. We consider the rank value of RPL and the consecutive packet drops to improve the detection metrics, and also take into account the use of both sibling and child nodes on a RPL routing path to construct the detour method. Our simulation results show that the proposed detection method is faster than the previous result, and the detour method improves the detour success rate.

**Keywords:** IoT, Packet drop detection, Detour algorithm

## I. 서 론

사물인터넷 (IoT : Internet of Things) 환경은 일반적인 사물에 컴퓨팅 능력을 탑재하고 이를 인터넷에 연결시켜 새로운 가치 창출을 목적으로 한다. 인터넷에 연결되기 위해서는 IP가 부여되어야 하는데 이를 위해 폭발적으로 증가할 것으로 예상되는 IP 주소 수요를 충족시키기 위해 무선 네트워크 환경에 IPv6를 적용시키려는 노력이 이루어지고 있다[1]. IETF (Internet Engineering Task Force)에서는 무선 네트워크의 물리/MAC 계층을 위한 표준인 IEEE 802.15.4에 IPv6를 적용시킨 IEEE 802.15.4e를 제시하였고 네트워크 계층을 위한 라우팅 프로토콜인 RPL (IPv6 Routing Protocol for Low-power Lossy Networks)을 제시하였다. 6TISCH 그룹은 이 두 표준을 IoT를 위한 대표적인 표준으로 고려하고 있다.

본 논문에서는 IoT 서비스 가용성 확보를 위해 기

Received(01. 07. 2016), Modified(06. 01. 2016), Accepted(06. 01. 2016)
* 본 연구는 한국연구재단 연구과제(No. NRF-2015R1A2A2A01004792) 지원 및 한국대학교 논문연구소 관리로 수행하였습니다.
† 주저자, jw.choi@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

존 MANET (Mobile Ad Hoc Network)환경에서 연구된 패킷 유실 공격 탐지 기법을 IoT를 위한 환경에 적용시켜 탐지 속도를 향상시키고자 하였고 패킷 유실 공격의 대응책으로 우회기법을 제시하였다.

## II. 관련 연구

무선 네트워크 환경에서 패킷 유실 공격을 다루는 솔루션은 ACK 기반 솔루션, 평판 기반 솔루션, 그리고 탐지 기반의 솔루션으로 구분할 수 있다.

Balakrishnan 등[2]은 라우팅 경로에 있는 2 홉 떨어진 노드로부터 응답을 요구하는 기법을 제안하였다. TWOACK 패킷을 사용하여 TCP에 비해 짧은 타임아웃 시간과 예측 가능성을 향상시켰다. Liu 등[3]은 TWOACK를 기반으로 하여 악의적인 링크를 탐지하기 위한 기법을 제안하였다. 통신량의 부담을 줄이기 위해 데이터 패킷의 일부분만을 ACK 패킷으로 활용하여 ACK 패킷의 크기를 줄이는 방식을 사용하였다.

Miranda 등[4]은 노드의 리소스를 확보하기 위해 이기적으로 행동하는 노드를 탐지하기 위한 기법을 제안하였다. 포워딩 메시지를 거부한 내용을 공개적으로 알리는 방법을 사용하여 노드들의 형평성을 관리하였다. 복잡한 평판 시스템을 탈피하는 자체적 분산화를 도입하여 전체 시스템에 형평성을 향상시켰다. Basile 등[5]은 노드가 패킷을 전송하기 위해 1 홉 떨어진 이웃 노드로부터 일정 수의 동의를 구하는 방식인 내부 원 일관성 방식 (Inner-circle consistency)을 제안하였다. 결정적 또는 통계적 방법의 두 가지 투표 알고리즘을 활용하는 내부 원 투표 프로토콜을 통해 탐지 속도를 향상시켰고 에러와 공격을 억제하였다.

Nadeem 등[6]은 MANET 환경에서 라우팅 탐색 절차에서의 DDoS 공격을 탐지하기 위해 카이 제곱 검증과 명령 차트를 조합하는 탐지 시스템을 제안하였다. 앞선 연구를 기반으로 Nadeem 등[7]에서는 악의적인 노드를 탐지 후 대응 방법에 관한 연구를 진행하였다. 예상 공격 신뢰도와 예상 네트워크 성능 저하 수치를 기반으로 반응 행동을 결정하는 지식 기반의 처리를 제안하였다.

## III. 제안기법

본 장에서는 RPL의 특성을 반영한 패킷 유실 공격 탐지 기법과 패킷 유실 공격이 발생하고 있는 노드에 대해 주변 노드들이 우회할 수 있는 기법을 제안한다.

### 3.1 속도 개선을 위한 악성 노드 탐지 기법

Sanchez-Casado 등[8]은 MANET 환경에서 패킷 포워딩이 수행되는 일반적인 절차에 대한 모델링을 통해 패킷 유실 확률을 계산하는 메트릭을 정의하여 패킷 유실 탐지에 활용하였다. 위의 기법에서는 CTS/RTS 메커니즘과 Watchdog을 통한 패킷 포워딩 수행 여부를 통해 패킷 유실 확률을 계산한다. 하지만 CTS/RTS 메커니즘은 MAC 계층에서 수행되기 때문에 패킷 유실 공격이 발생할 때 해당 메커니즘은 정상적으로 수행될 수 있다. 따라서 본 논문에서는 패킷 포워딩 여부를 중점적으로 고려하여 IoT 환경에서 고려할 수 있는 요소를 적용시켜 패킷 유실 공격 탐지 속도를 향상시키는 것을 목적으로 하였다.

RPL상의 노드는 OF (Objective Function)에 의해 순위값이 부여되며 이를 기반으로 노드 간의 부모, 자식 관계가 형성된다. n개의 노드에 대해 RPL로 형성된 그래프를 완전 이진 트리의 형태로 가정한다면 노드는 자신의 순위값인 rank에 따라 패킷 유실 공격에 대한 중요도가 다르다고 볼 수 있다. 위의 내용을 기반으로 순위값에 따른 패킬 유실 민감도를 식 (1)로 정의하였다. $W_{rank}$값은 하나의 패킷 유실에 대해 노드의 순위값에 따른 가중치를 의미한다.

$$W_{rank} = \log(\log_2 n - rank) \quad (1)$$

Bai 등[9]은 신뢰도 분석을 위해 연속적인 패킷 유실을 직접적인 메트릭으로 고려하였다. 이를 기반으로 노드 간의 모니터링을 통해 확인할 수 있는 연속적인 패킷 유실을 탐지 메트릭에 적용하였다. A, B 두 노드 간의 패킷 포워딩을 모니터링을 할 때 두 가지를 검사한다. 첫 번째는 A 노드가 전송하는 패킷의 순서 $seq(i)$이다. 두 번째는 A 노드가 전송한 패킷을 B 노드가 포워딩할 때의 순서인 $seq(r(i))$이다. 위의 두 측정값을 적용하여 식 (2)와 같이 연속적인 패킷 유실 에러 추정치인 $P_e$와 연속적인 패킷 유실에 대한 가중치 $P_n$을 계산한다.

$$P_e = \frac{seq(r(i)) - seq(i)}{seq(r(i))}$$
$$P_n = P_{n-1} + P_e \quad (2)$$

위의 두 가중치를 적용하여 Sanchez-Casado 등[8]에서 제안한 패킷 유실 공격 탐지 메트릭을 개선하였다. 식 (3)은 개선한 패킷 유실 공격 탐지 메트릭을 나타낸다. $p_{\mathrm{col}}$은 기존 기법에서 일반적인 통신 오류를 정의한 변수이며 $data_{recv}$는 A 노드가 포워딩한 패킷 수, $data_{fwd}$는 B 노드가 A 노드에게 받은 패킷을 전송한 수, $data_{drop}$은 유실된 패킷 수, $\tilde{p_{fwd}}$은 패킷 전송이 실패할 확률, $p_{drop}$은 패킷 유실 확률을 의미한다.

$$data_{drop} = data_{recv} - data_{fwd}$$
$$\tilde{p_{fwd}} = \frac{data_{fwd} - (data_{drop} \times W_{rank} + P_n)}{data_{recv}} \quad (3)$$
$$p_{drop} = 1 - \frac{\tilde{p_{fwd}}}{1 - p_{\mathrm{col}}}$$

### 3.2 RPL 우회 기법

RPL에서 악의적인 노드에 대해 형제 노드를 통해 우회하는 기법이 존재한다[10]. 하지만 RPL을 통한 라우팅 경로 설정은 노드의 위치에 의존적이기 때문에 형제 노드가 존재하지 않을 수 있다. 따라서 형제 노드와 자식 노드를 동시에 활용하는 것을 고려할 수 있다. 각 노드는 RPL의 OF를 통해 계산된 순위값을 기반으로 부모노드, 형제노드, 그리고 자식노드 리스트를 관리한다. 만약 한 노드의 부모노드가 패킷 유실 공격으로 인해 정상적으로 동작하지 않는 다면 형제노드, 자식노드 순으로 우회 경로를 탐색한다.

## IV. 분 석

제안한 패킷 유실 공격 탐지 기법의 탐지 속도 비교와 우회 기법의 우회 성공률을 검증하기 위하여 MATLAB과 C++을 통하여 시뮬레이션을 진행하였다.

### 4.1 탐지 속도 비교

제안 기법의 탐지 효율성을 측정하기 위해 기존 탐지 기법 Sanchez-Casado[8]과의 비교 분석을 MATLAB 환경에서 실시하였다. 원하는 목표치를 얻기 위해 표(1)과 같이 RPL을 통해 형성되는 그래프의 최대 높이는 8, 측정 노드의 순위값은 5, 그리고 패킷 유실 임계치는 0.4로 설정한 후 한 개의 노드에서 패킷을 전송할 때 50번째 패킷까지는 정상적으로 동작한 후 60% 확률로 패킷 유실이 발생하도록 하여 패킷 유실 확률을 측정하였다. Fig. 1은 위의 시뮬레이션의 결과를 나타내는 그래프이다. 제안 기법은 69(50번 째 패킷 이후 19)번째 패킷 포워딩에서 패킷 유실 임계치에 도달하였고 기존 기법은 135(50번 째 패킷 이후 85)번째 패킷 포워딩에서 패킷 유실 임계치에 도달하였다. 이를 통해 기존 기법에 비해 제안 기법의 탐지 속도가 약 1.95배 향상되었음을 확인하였다.

Table. 1. The simulation environment variable

| Variable | Simulation Value |
|---|---|
| Ranking of node | 5 |
| Packet dropping threshold | 0.4 |
| Packet dropping probability | 60% (Only, n≥50, n is packet number) |

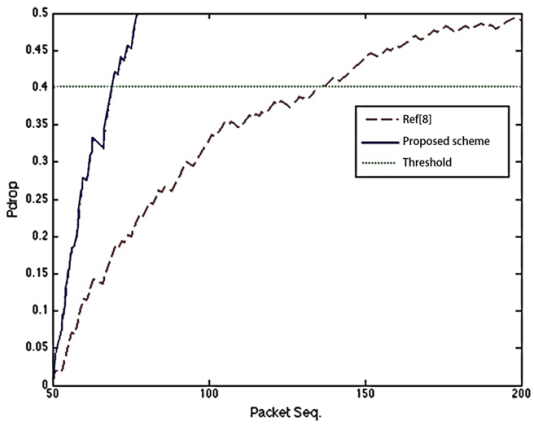



Fig. 1. The comparison of packet drop detection

### 4.2 우회 성공 확률 비교

이 분야의 연구로 적절한 Hong 등[10]을 비교 대상으로 선정하여 형제 노드를 통한 우회 기법과 본 논문에서 제안한 우회 기법 간의 성능 측정을 위해 C++ 언어를 사용하여 시뮬레이션을 진행하였다.

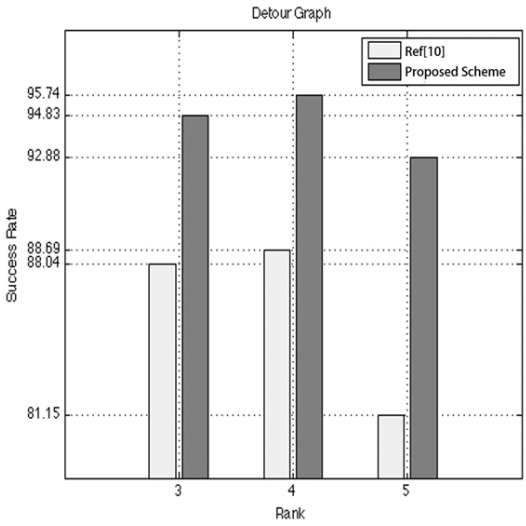



Fig. 2. The comparison of detour success probability

1000 x 1000 지형에 100개의 노드를 임의로 배치한 후 RPL을 기반으로 노드의 순위값을 계산하였다. 이후 3~5 사이의 순위를 가지는 한 개의 노드를 임의로 지정하여 패킷 유실 공격이 발생한다고 가정하였다. 이 때, 해당 노드의 자식 노드들의 우회 성공 여부를 측정하였고 각 노드 순위 마다 30회씩 반복하여 측정하였다. Fig. 2는 우회 성공률에 대한 기존 기법과의 비교 결과를 나타낸다. 제안 기법은 기존 기법에 비해 약 6~10% 향상된 우회 성공률을 보였다. 하지만 노드의 위치에 의존적인 기법이기 때문에 우회할 수 있는 경로가 존재하지 않을 수 있다.

## V. 결 론

본 논문에서는 IPv6 기반의 사물인터넷 환경을 고려하여 패킷 유실 공격에 대한 서비스 가용성을 확보하기 위해 두 가지 기법을 제안하였다. 기존의 패킷 유실 공격 탐지 메트릭에 RPL의 특성과 패킷 유실 연속성을 적용하여 탐지 속도를 향상시키고자 하였다. 또한, RPL을 통해 생성된 라우팅 토폴로지에서 형제 노드 및 자식 노드를 통한 우회 기법을 통해 우회 성공률을 향상시키고자 하였다. 각 기법에 대한 시뮬레이션을 통해 약 1.95배의 탐지 속도 향상과 6~10%의 우회 성공률을 확인하였다.

## References


[1] M. Jung, C. Reinisch, and K. Wolfgang, "Integrating building automation systems and ipv6 in the internet of things," *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conf.* IEEE, p. 683-688, Jun. 2012.

[2] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: preventing selfishness in mobile ad hoc networks," *Wireless communications and networking Conf. IEEE*, Vol. 4, pp. 2137-2142, Mar. 2005.

[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *IEEE Trans. on Mobile Computing,* Vol. 6, no. 5, pp. 536-550, May. 2007.

[4] H. Miranda and L. Rodrigues, "Friends and foes: Preventing selfishness in open mobile ad hoc networks," *in Proc. of Distributed Computing Systems Workshop IEEE*, pp. 440-445, May. 2003.

[5] C. Basile, Z. Kalbarczyk, and R. Iyer, "Inner-circle consistency for wireless ad hoc networks," *IEEE Trans. on Mobile Computing*, Vol. 6, no.1, pp. 39-55, Jan. 2007.

[6] A. Nadeem and M. Howarth, "Adaptive intrusion detection & prevention of denial of service attacks in manets," *in Proc. of the Wireless Communications and Mobile Computing ACM*, pp. 926-930, Jun. 2009.

[7] A. Nadeem and M. Howarth, "An intrusion detection & adaptive response mechanism for manets," *Ad Hoc Networks*, Vol. 13, pp. 368-380, Feb. 2014.

[8] L. Sanchez-Casado, G. Macia-Fernandez, P. Garcia-Teodoro, and R.

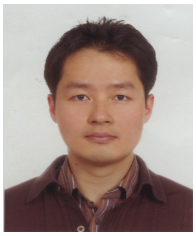
Magan-Carrion, "A model of data forwarding in manets for lightweight detection of malicious packet dropping," *Computer Networks*, Vol. 87, pp. 44-58, Jul. 2015.

[9] F. Bai and H. Krishnan, "Reliability analysis of dsrc wireless communication for vehicle safety applications," *in Proc. of Intelligent Transportation Systems IEEE*, pp. 355-362, Sep. 2006.

[10] K. Hong and L. Choi, "Dag-based multipath routing for mobile sensor networks," *in Proc. of ICT Convergence*, pp. 261-266, Sep. 2011.

## 〈저자소개〉

최 재 우 (Jaewoo Choi) 학생회원
2014년 2월: 한국산업기술대학교 게임공학과 졸업
2014년 3월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 정보보호, 센서 네트워크 보안 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 공학박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, HCI 보안 등