

# Yen의 알고리즘을 응용 한 임의 경로 선택 방식

정제성\*, 신승원\*, 김광조\*

카이스트 정보보호대학원\* / 전산학과†

## Random Route Mutation using Yen's algorithm

Je-Seong Jeong\*, Seungwon Shin\*, Kwangjo Kim\*

Graduate School of Information Security\* / Dept. of Computer Science, KAIST†

### 요 약

현재 우리는 인터넷을 통해서 다양한 정보들을 주고 받고 있으며, 이를 통해 다양한 업무를 수행하고 있다. 그리고 스마트폰의 보급이 증가함에 따라 인터넷은 더욱더 중요해 지고 있다. 이런 인터넷 사용이 급증한 것은 유선과 무선 네트워크가 다양하게 구성이 되었기 때문이다. 하지만 인터넷의 사용이 증가함에 따라 불법적인 공격자에 의한 분산 서비스 거부 공격(Distributed Denial of Service)이나 도청(Eavesdropping)과 같은 불법 행위가 증가하고 있다. 무선 네트워크에서는 Random Route 기법을 이용하여 이런 공격을 방어하고 있지만 유선 네트워크에서는 Disjoint Route를 찾는 것이 쉽지 않아 무선 네트워크와 같은 방법을 사용하기에는 제한사항이 있다. 또한, Random Route를 적용 시 현재보다 전송 시간이 오래 걸려 정상적인 인터넷 이용을 할 수 없다는 단점이 있어, 현재의 유선 네트워크는 대부분 고정 경로를 이용하여 인터넷을 이용한다. 물론, Load balancing과 같은 방법을 사용하여 경로를 일부 변경 방법도 있으나, 이는 공격자가 얼마든지 예상을 할 수 있기 때문에 기존의 공격에 여전히 취약하다. 따라서 본 논문에서는 Yen의 알고리즘을 활용하여 계층별로 Random Route를 제안하고자 한다. 본 방법이 적용 될 경우, 계층에 따른 Random Route로 정보 전송의 효율성을 유지 할 수 있으며 계층의 보안성을 향상 시킬 수 있다.

### 1. 서 론

현대 사회는 다양한 정보들을 인터넷을 통해서 전송하고 있으며, 이를 통해 업무를 하고 있다. 그리고 이러한 현상은 스마트폰의 급속한 보급으로 기하급수적으로 증가하고 있는 추세이다. 이는 유무선 네트워크 기술이 발전함에 따라 가능하게 되었다. 하지만 인터넷의 사용이 증가함에 따라 공격자들로부터 분산 서비스 거부 공격(Distributed Denial of Service), 도청(Eavesdropping), Blackhole 공격 등과 같은 악성공격을 받는 사례도 증가하고 있다. 무선 네트워크에서는 이러한 공격에 대응하기 위해서 Random Route를 사용하고 있다. 하지만 유선 네트워크에서는 Load balancing을 제외하고는 고정된 데이터 전송 경로를 이용한다. 이는 공격자가 예상경로를 충분히 예상 할 수 있기 때문에 위에서 언급한 공격에 취약하다. 따라서 유선 네트워크에도

무선 네트워크와 같은 Random Route를 적용하는 것이 필요하다. 하지만 기존 임의 경로 선택 방식(Random Route Mutation)은(4) 유선 네트워크에서 Random Route에만 중점적인 연구를 하여 정보 전송의 효율성이 떨어져서 정보를 전송 하는데 문제가 생길 수가 있다. 따라서, 본 논문에서는 유선 네트워크에 Yen의 알고리즘을 활용 한 Random Route를 일반 네트워크와 소프트웨어 정의 네트워크(Software Defined Network, SDN)에 적용하는 방안을 제시한다. 이는 네트워크 사용자의 중요도에 따라 경로를 다르게 편성하여 보안성 및 효율성을 동시에 충족시킬 것으로 예상된다.

본 연구의 구성은 다음과 같다. 2장에서는 Yen의 알고리즘과 임의 경로 선택 방식(Random Route Mutation, RRM), SDN에 대한 간단한 설명을 하며 3장에서는 상하 간 조직이 분명한 경찰 조직을 이용하여 네트워크 사용 계층 구분 기준을 제시한다. 4장에서는 활용방안에 대해서 설명하며, 5장에서는 결론과 향후 과제를 제시한다.

\* 주저자 : 정제성 (taegm01@kaist.ac.kr)

\* 공동저자 : 신승원 (claude@kaist.ac.kr)

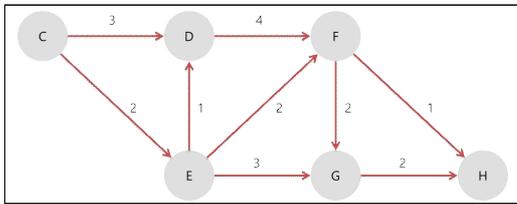
† 교신저자 : 김광조 (kkj@kaist.ac.kr)

## II. 관련 연구

본 장에서는 최적 경로를 찾는 Yen의 알고리즘과 데이터 전송 경로를 무작위로 변경하는 임의의 경로 선택 방식과 소프트웨어 정의 네트워크(Software Defined Network, SDN)에 대해서 간단히 기술한다.

### 2.1 Yen의 알고리즘

Yen의 알고리즘(1)은 1971년 발표되었으며 그래프에서 음수 값을 가지지 않는 경로를 이용하여 Loopless 한 최단 경로를 계산하는 방식으로 최단 경로와 그 다음 최적 경로를 찾는 데 사용된다(2). [그림 1]은 Yen의 알고리즘을 설명하기 위한 예시이다.



[그림 1] Yen의 알고리즘 예시

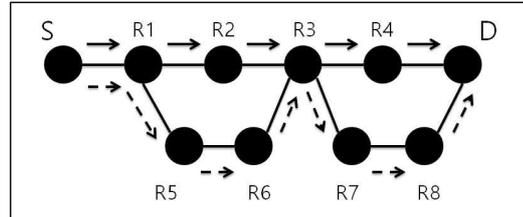
[그림1]에서 "C"는 source node이고 "H"는 destination node이다. 먼저, Dijkstra의 알고리즘(3)을 이용하여 "C"에서 "H"로의 최단 경로를 찾아낸다. Dijkstra의 알고리즘은 음수를 가지지 않는 지향성 그래프에서 출발점과 도착점 사이의 최단 경로를 찾아내는 알고리즘이다. 그림[2]에서 최단 경로는 (C) - (E) - (F) - (H) 이고 Cost는 5이다. 이 경로는  $A^1$ 으로 정의한다. 이후  $A^1$  경로의 Source node와 Destination node를 제외한 Node에서 이용한 경로를 제외 한 다른 경로를 이용하여  $A^1$  경로 다음의 최적 경로를 찾게 한다. 예를 들면,  $A^1$  경로에서 Node E에서F로 이동을 했다면 이 경로를 제외한 Node D 또는 G로 이동을 하게 하는 것이다. 이와 같은 방법으로 다음 최적 경로들을 구하면 Cost가 7인  $A^2 = (C) - (E) - (G) - (H)$ 와 Cost가 8인  $A^3 = (C) - (D) - (F) - (H)$ 가 되겠다.

위와 같이 Yen의 알고리즘은 Source node에서 Destination node로의 경로를 최적 값부터 순서대로 구해낸다.

### 2.2 임의의 경로 선택 방식

본 방식은 고정된 경로를 무작위로 경로 편성하여

공격자가 분산 서비스 거부 공격이나 도청 등의 공격을 하지 못하게 하는 것이다. 이 방법은 현재 무선 네트워크에서는 널리 사용이 되나 유선 네트워크에서는 Disjoint Route를 찾기가 어려워 널리 사용되고 있지 않다. 이를 고려한 Proactive Random Route를 기존 논문에서는 제안하고 있다(4). 이 방법은 Packets을 전송하기 전 이동 경로를 미리 정하여 Label을 붙여 전송을 하는 방식이며, 두 단계로 나누어진다. [그림 2]는 RRM의 예시이다.



[그림 2] RRM의 예시

첫째, 출발점 S에서 도착점 D로 가는 최적 경로를 구한다. [그림 2]에서 최적 경로는  $S \rightarrow R1 \rightarrow R2 \rightarrow R3 \rightarrow R4 \rightarrow D$ 이다. 둘째, 최적 경로에서 Hub node를 제외하고 겹치지 않는 경로들을 구하면  $S \rightarrow R1 \rightarrow R5 \rightarrow R6 \rightarrow R3 \rightarrow R7 \rightarrow R8 \rightarrow D$ 이다. 위 경로를 살펴보면 R1과 R3는 모든 경로가 지나야만 하는 것을 알 수가 있다. 이를 이용하여 R1과 R3의 보안성을 향상 시킨다면 전체적인 네트워크 보안성을 향상 시킬 수가 있다.

### 2.3 소프트웨어 정의 네트워크

SDN은 기존 네트워크와는 달리 데이터 계층(data layer)과, 제어 계층(control layer), 애플리케이션 계층(application layer)으로 나뉜다. 데이터 계층은 SDN의 특정 인터페이스를 통해 제어를 받는 계층으로서, 데이터 흐름의 전송을 담당한다. 제어 계층은 데이터의 흐름을 제어하는 계층으로서 애플리케이션과 네트워크 서비스를 통하여 데이터 흐름을 라우팅 할 것인지, 전달을 할 것인지, 거절할 것인지를 결정한다. 또한 데이터 계층의 동작들을 정리하여 API(Application Programming Interface) 형태로 애플리케이션 계층에 전달한다. 마지막으로 애플리케이션 계층은 제어 계층에서 제공한 API들을 이용하여 네트워크의 다양한 기능들을 수행 할 수 있도록 한다(5). OpenFlow는 제어 계층이 데이터 계층을 통제하기 위해 사용되는 인터페이스이다.

### III. 계층 구분

본 장에서는 경찰조직을 예시로 네트워크 사용자 등급을 나누어서 어떻게 적용을 할 수 있는지 설명하겠다. 먼저 [표 1]은 2014년도 기준 경찰 계급별 인원 구성표이다.

[표 1] 경찰 계급별 인력구성(기준: '14년말)[6]

총 계	치안총감	치안정감	치안감
급 수	차관 급	1급	2급
109,364(명)	1	6	25
경무관	총경	경정	경감
3급	4급	5급	6급 (갑)
49	507	2,171	6,429
경위	경사	경장	순경
6급 (을)	7급	8급	9급
13,795	23,274	29,725	33,382

[표 1]에서 인원 및 임무 중요도에 따라 구분을 한다면 1 ~ 5급과 6 ~ 9급으로 나눌 수가 있다. 1 ~ 5급을 1등급 사용자로 정의를 하고 6 ~ 9급을 2등급 사용자로 정의한다. 그리고 이를 근거로 1등급 사용자 간 전송하는 데이터는 보안성과 효율성을 만족하는 Random Route를 이용하여 데이터를 전송하고 2등급 사용자 간 전송하는 데이터는 1등급 사용자에게 비해 효율성은 떨어지지만 보안성이 보장되는 Random Route를 이용하여 데이터를 전송하게 하면 전체적인 네트워크의 효율성을 유지 할 수 있을 뿐만 보안성도 보장되어 공격자로부터 안전한 네트워크망을 구성 할 것이다.

### IV. 활용방안

3장에서와 같이 조직에서 총인원 및 계층에 따른 임무를 확인 후 보안 중요도가 높은 그룹과 보안성이 상대적으로 중요하지 아니한 그룹으로 나누어 높은 그룹은 좀 더 강도 높은 RRM을 적용을 하고 중요도가 낮은 그룹은 그 보다는 강도가 낮은 RRM을 적용하면 되겠다. 이는 계층 간으로 구성된 공무원 집단 또는 군, 또는 일반 기업 내부망에 적용을 할 수가 있을 것이다.

### V. 결론

현재의 네트워크는 사용량이 증가함에 따라 구조도 날로 복잡해지고 있다. 하지만 유선 네트워크에서의

대부분의 데이터 전송은 고정된 경로를 사용함으로써 공격자들이 쉽게 악성행위를 할 수 있게 한다. 따라서 이에 대한 대비가 필요하다. 하지만, 기존 논문에서 발표되었던 방식[4]은 효율성이 떨어져서 현재 네트워크에 적용하는 데는 제한이 있다. 본 논문에서는 Yen의 알고리즘을 이용하여 중요도에 따라 계층을 나눈 후 Random Route를 하는 방안을 제시하였다. 향후 과제로는 Yen의 알고리즘을 실제 구현한 후 계층별 Random Route를 현재 네트워크와 SDN에 적용을 하여 효율성 및 보안성을 검증하는 것이다.

### References

- [1] Yen, Jin Y. (1970). "An algorithm for finding shortest Route from all source nodes to a given destination in general networks". Quarterly of Applied Mathematics 27: 526 - 530.
- [2] Yen, Jin Y. (Jul 1971). "Finding the k Shortest Loopless Paths in a Network". Management Science 17 (11): 712 - 716.
- [3] E. W. Dijkstra: A note on two problems in connexion with graphs. In: Numerische Mathematik, 1 (1959), S. 269 - 271
- [4] Qi Duan, Ehab Al-Shaer and Haadi Jafarian, "Efficient Random Route Mutation Considering Flow and Network Constraints", Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, USA, 2013 IEEE
- [5] Taejune Park, Seungsoo Lee, Seungwon Shin, "A reflectornet Based on Software Defined Network", The Journal of Korea Information and Communications Society '14-06 Vol.39B No.06
- [6] 사이버경찰청, 경찰통계자료, [http:// www.police.go.kr/portal/main/contents.do?menuNo=200189](http://www.police.go.kr/portal/main/contents.do?menuNo=200189)