情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

Ad-hoc 네트워크 역추적 기술 동향

이 동 희*, 여 돈 구, 장 재 훈, 염 흥 열**

요 약

Ad-hoc 네트워크는 노드가 자유롭게 이동하면서 네트워크를 구성하며, 어떠한 고정된 AP(Access Point)의 도움 없이 자신들의 연결만을 통해 통신망을 제공한다. Ad-hoc 네트워크에서는 기존 인터넷 망에서 존재하는 공격이 가능하다. 이런 공격에 대응하기 위하여 기존 유선망에서의 IP기반 역추적 기술을 바탕으로 ad-hoc 네트워크에서의 역추적 연구가 이루어지고 있다. 본 논문에서는 ad-hoc 네트워크 및 기존 유선망에서의 IP기반 역추적 기술들에 대하여 알아 본 후, 최근 발표된 ad-hoc 네트워크기반의 역추적 대표적인 기술들의 기법들에 대해 살펴본다.

Ⅰ. 서 론

Ad-hoc 네트워크는 어떠한 고정된 AP의 도움 없이 이동 가능한 노드들에 의해서 네트워크를 자유롭게 구성한다. 노드들은 자체적으로 무선 인터페이스와 라우팅 기능을 가지게 된다[1]. 하지만 ad-hoc 네트워크는 노드의 이동성, 노드의 대역폭 등의 문제를 가지고 있다. Ad-hoc 네트워크는 기존 유선망에서 존재하였던 다양한 공격들이 가능하며 유선망에서의 역추적 기법들을 ad-hoc 네트워크에 적용하려는 역추적 연구가 이루어지고 있다.

본 논문의 구성은 2장에서는 ad-hoc 네트워크와 ad-hoc 네트워크에서 기반으로 하는 IP기반 역추적 기술에 대해서 알아본다. 그리고 3장에서는 대표적인 ad-hoc 네트워크 역추적 관련 기술을 살펴본 후, 4장에서 ad-hoc 네트워크 역추적 관련 기술을 비교 분석한다. 그리고 5장에서 결론을 내린다.

Ⅱ. 관련 연구

2.1 Ad-hoc 네트워크

Ad-hoc 네트워크[1,2]는 AP(Access Point)가 없이 흩어져 있는 무선으로 통신이 가능한 노드들끼리 서로 통신을 하는 자율적인 구조의 네트워크를 말한다.

Ad-hoc 네트워크 프로토콜은 노드의 이동으로 인한 네트워크 변화에도 빠르게 적응할 수 있고 노드가 임의 시간 동안 송/수신 기능이 멈출 수 있기 때문에 이러한 주기를 수용할 수 있는 등 몇 가지 사항이 프로토콜에 요구된다.

Ad-hoc 네트워크에는 통신을 제어하는 노드가 없기 때문에 ad-hoc 네트워크를 구성하는 노드들 간에 통신을 위해 각 노드는 이웃한 노드에 전달(forwarding)과 중계(relay) 기능을 제공해야 하며, 이러한 기능이 자신의 통신 거리 밖의 노드와 통신할 수 있게 해주는 특징을 갖는다. 또 다른 특징은 서로 다른 종류의 장치로도 네트워크 형성이 가능하다는 것이다. 이것은 동일한 ad-hoc 통신 프로토콜을 통해 이기종 단말간에 통신이 가능한 네트워크를 구성할 수 있다.

2.2 IP 기반 역추적 기술

IP 기반 역추적 기술[3,4]은 공격자의 위치를 식별하고 추적하거나 공격에 이용되는 경로의 일부 또는 전부를 확인하기 위한 기술로써 자신의 위치를 감추고 공격 패킷을 전달하는 공격자로의 경로와 위치를 추적한다.

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.
(NIPA-2010-(C1090-1031-0005))

* 순천향대학교 정보보호학과 석사과정 (leemeca@sch.ac.kr)
** 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)

IP 기반 역추적 기술은 전향적 역추적(proactive IP traceback) 기술과 대응적 역추적(reactive IP traceback) 기술로 나눌 수 있으며, 두 분류에는 여러 종류 역추적 기술이 있다.

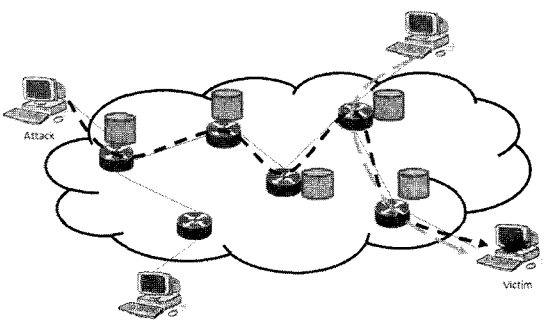
하지만 본 장에서는 역추적 기술을 분류하여 모든 IP 기반 역추적 기술을 설명하지 않는다. 우리는 대표적인 ad-hoc 네트워크에서 언급하는 역추적 기술들인 로깅, 해쉬기반 역추적에 대해 간략히 설명한다.

2.2.1 로깅(logging)

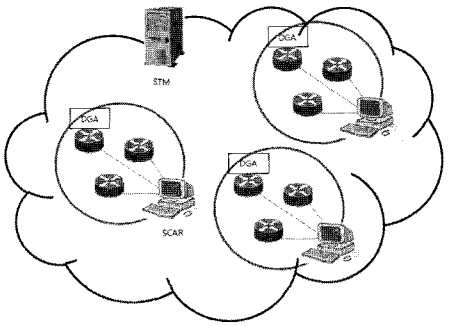
로깅[3,4,5]은 라우터로부터 전송된 패킷의 특성을 저장해 놓은 후에 데이터 마이닝 등의 추론 시스템을 적용하여 공격 근원지를 역추적 하는 기술이다. 많은 양의 데이터를 처리해야 되기 때문에 확률적인 샘플링 기법과 필터 기법을 등을 적용하여 처리와 판별 과정을 줄인다.

2.2.2 해쉬기반 역추적(hash-based traceback)

해쉬기반 역추적[3,4,6]은 SPIE(Source Path Isolation Engine) 시스템을 중심으로 네트워크 내 서브 그룹을 관리하는 SCAR(SPIE Collection and Reduction Agents)가 있고, 라우터내에서는 DGA(Data Generation Agent)를 통해 라우터를 지나는 패킷 요약 정보(IP헤더, 페이로드)에 블룸 필터를 적용하여 결과를 저장한다. 공격이 발생하면 SPIE는 서브 그룹들을 관리하는 STM(SPIE Traceback Manager)에 패킷 정보를 요청하고, DGA에 저장된 정보와 비교하여 분석하고 이를 SPIE 시스템에 보내면 이 정보로 공격 경로를 재구성하게 된다.



〔그림 1〕 로깅 기술



〔그림 2〕 SPIE 시스템

2.2.3 블룸 필터(bloom filter)

블룸 필터[6]는 패킷 다이제스트를 포함하는 다이제스트 테이블을 구성하고 공간을 효율적으로 이용한다. k개의 패킷 다이제스트를 계산하고, 2^n 크기의 비트 배열의 인덱스로 n bit 값을 저장한다. 배열은 모두 0으로 초기화 되어 있고, 값이 입력되면 1로 설정된다.

Ⅲ. Ad-hoc 네트워크 역추적 기술

Ad-hoc 네트워크 역추적 기술은 IP기반 역추적 기술들을 바탕으로 연구되고 있다. 하지만 다음과 같은 이유로 유선 IP 환경에서 이용되는 역추적 기술을 ad-hoc 네트워크에서 그대로 적용할 수 없으며 ad-hoc 네트워크에서 역추적을 어렵게 한다[8].

- 고정된 인프라가 없으며, 각 노드가 터미널, 호스트 그리고 라우터의 역할이 가능하다.
- 노드의 이동성 때문에 네트워크 토폴로지의 변경이 빈번하다.
- 네트워크 대역폭과 배터리 전원이 제한되어 있다.

이런 문제를 해결하기 위해 다음과 같은 역추적 기술이 연구 되고 있다. 주요 ad-hoc 네트워크 역추적 기술로는 SWAT(Small World-based Attacker Traceback), 크로스 레이어 모니터링(cross-layer monitoring) 그리고 핫스팟기반 역추적(Hotspot-based Traceback) 그리고 시간 태그 블룸 필터(time-tagged bloom filter)가 있다.

3.1 SWAT(Small World-based Attacker Traceback)

SWAT[7]은 스몰 월드 효과1)의 개념을 바탕으로 공격 경로를 찾기 위해 주변의 노드로부터의 보고를 기반

으로 한다. 이 기술은 Contact 노드와 TPM(Traffic Pattern Matching), TVM(Traffic Volume Matching)을 사용한다.

- Contact 노드: 자신 주변으로 R 홉(hop) 범위의 노드를 설정하여 스몰 월드 구축하며 피해자 노드에게 전체 네트워크의 구성을 제공하여 패킷을 빠르게 전달 할 수 있도록 해준다. 그리고 각 노드들로부터 TPM과 TVM 보고를 모으는 역할을 한다.
- TPM: 트래픽 패턴의 유사성을 검사하는 프로세스로, A와 B 노드에서 트래픽 량의 변화를 수집하여, 두 트래픽 시그니쳐(signature) 사이의 연관성을 나타낸다. 시그니쳐의 연관성은 노드 A에서 $[a_1, a_2, \cdots, a_n]$, 노드 B에서는 $[b_1, b_2, \cdots, b_n]$의 트래픽 변화량을 관찰 할 수 있을 때, 다음과 같은 연관 계수 $r(A,B)$을 구할 수 있다. 계산식에서 n은 측정한 트래픽의 수, S_A와 S_B는 표준 편차, $\overline{A}$와 $\overline{B}$는 $(a_1, a_2, \cdots, a_n)$과 $(b_1, b_2, \cdots, b_n)$의 평균을 나타낸다.

$$r(A,B)=\frac{1}{nS_AS_B}\sum_{i=1}^{n}(a_i-\overline{A})(b_i-\overline{B}) \quad (1)$$

$$\begin{cases} S_A=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(a_i-\overline{A})^2} \\ S_B=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(b_i-\overline{B})^2} \end{cases} \quad (2)$$

TPM이 나타내는 연관 계수 $r(A,B)$은 0과 1 사이의 값을 가지며, 1에 가까울수록 트래픽 A는 트래픽 B와 연관성이 높다. 트래픽 A와 B의 연관성이 높다는 것은 전송된 트래픽의 유사성이 높다는 것을 의미하며, [7]에서는 $r(A,B)$의 값이 0.7 이상이면 트래픽 A와 B가 같다고 본다.

- TVM: TPM를 보완해주는 역할을 해주며, 노드 A와 B 두 지점에서의 트래픽 량을 비교하여 동일한지를 확인하는 프로세스이다. 수학적으로, 트래픽 량이 동일한지 확인하기 위해 TVM에서는 최소제곱법을 사용한다.

$$c=\frac{\sum_{i=1}^{N}a_ib_i}{\sum_{i=1}^{N}a_i^2} \quad (3)$$

노드 A와 노드 B에서 전송된 트래픽의 양이 같다면, c는 1을 나타낸다.

트래픽 패턴과 트래픽 볼륨은 공격 트래픽의 비정상적인 특성을 나타낸다. SWAT에서 트래픽 패턴 및 볼륨을 이용하여 공격 트래픽을 특성화하여 수집하는 정보의 양과 저장할 데이터의 양을 최소화한다.

SWAT 기술은 각 노드에서는 IDS(Intrusion Detection System)에 의해 공격을 탐지할 수 있다고 가정한다. 그리고 각 노드는 자신의 주변 노드 정보를 바탕 Contact 노드를 지정하며, 자신을 지나가는 패킷을 저장한다.

앞서 SWAT에 대하여 설명하였고, 역추적 단계는 다음과 같다.

① 그림 3에서 피해자 노드 V가 공격을 탐지하였다면, 피해자 노드는 TPM과 TVM에서 사용할 공격 시그니쳐를 추출한다. 그리고 1 홉만큼 떨어진 경계에 있는 노드를 통해 level-1 Contact(C_L1a, C_L1b)에게 쿼리(query)를 보내며, 쿼리에는 SN(Sequence Number)와 공격 시그니쳐가 포함된다.

② level-1 Contact는 쿼리를 전달받고, 각 노드는 Contact로부터 요청을 받고 응답을 보내준다. 그리고 각 노드는 SN과 V를 기록해두어, 만약 같은 SN과 V로 리퀘스트(request)를 받으면, 재방문하는 것을 방지하기 위해 쿼리를 폐기한다.

③ 2개의 level-1 Contact 중 하나의 level-1 Contact에서 자신의 그룹 내의 노드들로부터 TPM과 TVM 값을 수집한다. 트래픽의 양에 대한 유사성인 TVM이 1을 나타내고, 트래픽 패턴의 유사성인 TPM이 0.7 이상이면 level-1 Contact의 네트워크에서 트래픽을 전송한 노드를 찾은 것이다. 만약 TVM과 TPM이 값을 만족하지 않으면 그 지역을 제외한다.

1) 스몰 월드 효과는 임의로 선택한 2명의 사람이 6명의 사람만 거치면 서로 연관이 되어 있다는 이론으로, "six degrees of separation"이라고도 한다. 이 이론은 Duncan Watts, Steven Strogatz라는 두 학자가 "Nature"에 기고한 논문을 통해서 알려지게 되었다. 클러스터링(clustering)과 경로 길이(path length)라는 개념이 존재하는데, 클러스터링은 노드 간의 연결 정도, 경로 길이는 한 점으로부터 다른 점까지의 거리를 뜻한다. 클러스터링이 큰 네트워크에서 몇 개의 독특한 연결이 존재한다면 임의의 두 지점 간의 경로가 규칙적으로 연결된 네트워크보다 짧아지는 것을 의미한다.

④ ③에서 찾은 level-1 Contact(C_L1b)에서 level-2 Contact(C_L2c, C_L2d)에게 쿼리를 보낸다.

⑤ 그리고 ②에서 ④까지의 과정을 반복한다. 더 이상 Contact 보고가 없거나 범위 밖에 다른 노드가 없을 때, 마지막 Contact 보고를 통해 피해자 노드를 위한 공격 경로가 완성된다.

3.2 크로스-레이어 모니터링(cross-layer monitoring)

크로스-레이어 모니터링[8]은 크로스-레이어(네트워크 계층과 MAC 계층)를 관찰하여 공격 트래픽을 특성화하고, 목적지 주소와 이전 홉의 MAC 주소를 활용하여 잡음(noise) 트래픽을 줄이기 위해 제안되었다. 여기서 잡음 트래픽이란 공격과 관련이 없는 노드로부터 전달된 트래픽을 의미한다.

크로스-레이어 모니터링에서는 각각의 노드는 네트워크/MAC 계층 활동을 감시하고 있어야 한다. 그리고 공격자를 찾기 위해서 SWAT의 스몰 월드 모델을 사용하고, 각 노드에서 도청(overhearing) 능력을 통해 정보를 수집하여 공격 경로를 재구성한다.

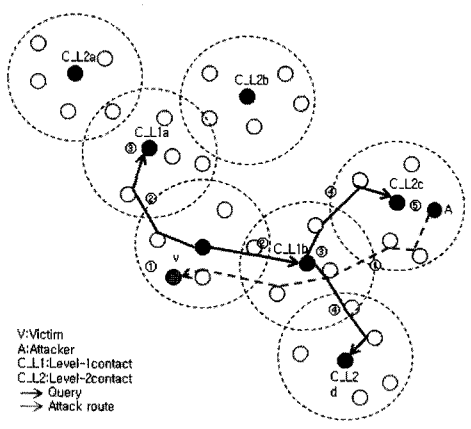
이 기술은 검색의 효율성을 높이기 위해 SWAT의 스몰 월드 모델을 사용하지만, 다음과 같은 문제점을 지적하고 있다.

① SWAT는 많은 양의 잡음 트래픽이 존재할 때 공격자에 대한 역추적이 실패할 수 있다.

② SWAT는 분산 서비스 거부(Distributed DoS, DDoS) 공격을 시도하는 공격자의 추적에 약하다.

③ SWAT는 역추적을 위해서 공격 트래픽을 보고하는 노드들에 의존하기 때문에, 잘못된 보고와 공격자에게 노드가 타협될 경우 취약할 수 있다.

④ SWAT는 역추적 후 대책 메커니즘을 제공하지 않는다.



〔그림 3〕 SWAT 역추적

이러한 문제를 해결하기 위해 크로스-레이어 모니터링은 크로스-레이어의 정보를 통해 역추적의 정확성을 높이고 시그니쳐 에너지(signature energy)를 사용하여 잘못된 보고를 줄인다. 또한 역추적에 도움이 되는 대책을 제공한다.

크로스-레이어 모니터링의 프로토콜 프레임워크는 이상 탐지, 이상 특성화, 이상 비교, 이상 검색, 대책으로 이루어져 있다.

- 이상 탐지: 이상 정보의 기록을 시작하기 위해 필요하다. 각 노드는 이상을 탐지하면 역추적을 위한 이상 정보와 크로스-레이어 계층 정보(목적지 주소와 이전 홉의 MAC 주소)를 저장한다. 이상을 탐지하기 위해서는 정상 정보를 필요로 하는데 정상 정보 A_R은 $[t_0,t_n]$의 시간동안 관찰된 정보, A_S는 단위 시간에 주어진 프레임의 수라고 할 때, 이상 레벨 $Dist$는 다음과 같이 정의된다.

$$Dist = \frac{A_s - A_R}{A_R} \tag{4}$$

만약 이상 레벨이 특정 한계점을 넘는다면, 그것을 의심스러운 트래픽으로 판단하고 노드는 정보를 저장한다.

- 이상 특성화: 이상 비교를 위한 특성화 값을 만드는 것으로 누적 분포 함수[13]를 사용한다. 이상 특성화에서 사용하는 데이터는 모니터링하는 시간 동안에 노드를 지나간 프레임 $(a_1,a_2,\cdots,a_n)$의 개수로, $y_1<y_2<\cdots<y_n$이 크기가 n인 $a_1,a_2,\cdots,a_n$의 순서 통계의 측정값일 때, 분포 함수는 다음과 같이 정의된다.

$$F_n(x) = \begin{cases} 0, x < y_1, \\ k/n, y_k \le x < y_{k+1}, \\ 1, y_n \le x. \end{cases} \tag{5}$$

식에서 k는 상수, $F_n(x)$는 특성화된 공격 시그니쳐 또는 후보 공격 시그니쳐로 사용된다. 그리고 이상 탐지에서 저장한 크로스-레이어 정보를 통해 잡음 트래픽을 제거한다.

- 이상 비교: 두 개의 특성화된 값을Kolmogorov-

Smirnov(KS) 통계 D_n[13]으로 계산하여 두 개의 특성화된 값이 비슷하거나 같은 노드를 찾는다. 계산식은 다음과 같이 정의되고, $F_i(x)$는 중간에 있는 노드에 의해 관찰된 후보 공격 시그니쳐, $F_0(x)$는 공격 시그니쳐를 의미한다.

$$D_i = sup_x[|F_i(x) - F_0(x)|] \quad (6)$$

만약 D_i 값이 충분히 작다면 $F_i(x)$와 $F_0(x)$가 같다고 본다.

- 이상 검색: 공격 경로를 재구성하기 위한 것으로 SWAT에서 사용한 스몰 월드 모델과 노드에서의 MAC 계층의 도청 능력을 사용한다. 크로스-레이어 모니터링에서 사용한 스몰 월드 모델은 SWAT에서 사용한 스몰 월드 모델과 차이가 있는데 크로스-레이어 모니터링은 시그니쳐 에너지와 과반수 투표(majority voting)를 사용한다.

시그니쳐 에너지는 개별 공격 시그니쳐 에너지(individual attack signature energy, E)와 지역 공격 시그니쳐 에너지(regional attack signature energy, RE)로 구분되는데, 개별 공격 시그니쳐 에너지는 다음과 같이 정의된다.

$$E^i = \frac{1}{D_i} \quad (7)$$

공격 시니그쳐와 후보 공격 시그니쳐가 높은 이상 매칭이 되었을 때 D_i가 작아지게 되고, 결과적으로 E^i가 증가된다.

지역 공격 시그니쳐 에너지는 다음과 같이 정의되고, $E^i_{1/2}(u)$는 이상을 관찰한 Contact u와 노드들 사이에 시그니쳐 에너지의 중간 값이다. $\mu_{1/2}$는 Contact부터 유사한 이상을 탐지한 노드까지의 홉 수의 중간 값이다.

$$RE = \frac{E^i_{1/2}(u)}{\mu_{1/2}} \quad (8)$$

계산식에서 평균 대신 중간 값을 받는 이유는 악의적이거나 타협된 노드로부터의 허위 보고의 부정적인 영향을 방지하기 위한 것이다.

또한 RE는 다음과 같은 과반수 투표 식을 만족해야 하는데, α는 과반수 투표수, N는 Contact의 주변 노드의 총 개수, n은 이상을 관찰한 노드의 수를 나타낸다.

$$\alpha = \frac{n}{N} > \delta \quad (9)$$

식에서 α가 지나치게 낮다면, 거짓 보고의 가능성이 높음을 추론할 수 있다.

앞서 크로스-레이어 모니터링 프로토콜 프레임워크를 알아보았고, 크로스-레이어 모니터링의 공격자 역추적은 다음과 같은 단계로 이루어진다.

① [그림 4]에서 피해자 노드 V가 공격을 탐지하였다면, 피해자 노드는 피해자 노드는 특성화 값을 추출한다. 그리고 1 홉만큼 떨어진 경계에 있는 노드를 통해 level-1 Contact(C_L1a, C_L1b)에게 쿼리(query)를 보내며, 쿼리에는 SN(Sequence Number)와 공격 시그니쳐가 포함된다.

② level-1 Contact는 쿼리를 전달받고, 각 노드는 Contact로부터 요청을 받고 응답을 보내준다. 그리고 각 노드는 SN과 V를 기록해두어, 만약 같은 SN과 V로 요청을 받으면, 재방문하는 것을 방지하기 위해 쿼리를 폐기한다.

③ level-1 Contact는 자신의 그룹에 속한 노드들로부터 수집된 E를 이용해 RE를 구하고, 어떤 노드에 대한 RE 값이 다른 노드들과의 RE 값 보다 높게 나타나면, 그 노드는 공격에 사용된 경로로 본다.

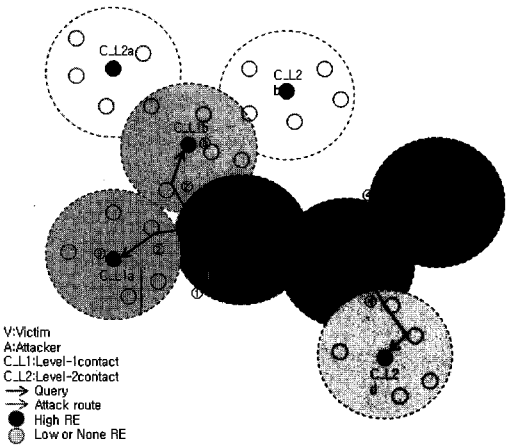
④ ③에서 찾은 공격 경로상의 노드가 속한 네트워크의 level-1 Contact(C_L1c)에서 level-2 Contact (C_L2c, C_L2d)에게 쿼리를 보낸다.

⑤ 그리고 ②와 ④의 과정을 반복한다. 더 이상 Contact 보고서가 없거나 범위 밖에 다른 노드가 없을 때, 마지막 Contact 보고를 통해 피해자 노드를 위한 공격 경로가 완성된다.

- 크로스-레이어 모니터링의 대책은 역추적 단계에 포함이 되지는 않지만 역추적에 도움을 주기 위한 것으로 공격 트래픽에 대한 최적의 방어 전략을 제공하고 합법적인 트래픽에서 부정적인 영향을 감소시킨다. 이상 매칭 레벨을 기반으로 하여 패킷 필터링과 임계치(rate limit)를 적용한다. 이상 매칭 레벨이 낮다면 임계치를 통해, 레벨이 높다면 패킷 필터링을 적용하여 패킷을 폐기시킨다.

3.3 핫스팟기반 역추적(hostspot-based traceback)

핫스팟(hotspot)기반 역추적[9]은 유선 IP 망에서 해쉬



〔그림 4〕 크로스-레이어 모니터링 역추적

기반 역추적을 ad-hoc 네트워크의 구조에 맞도록 분산된 구조로 변경한다.

해쉬기반 역추적에서 사용하는 SPIE(Source Path Isolation Engine) 시스템[11]의 STM과 SCAR 에이전트의 기능을 하는 조사 노드(IV: investigator)를 사용한다. IV는 역추적 세션을 시작하는 IDS 에이전트 노드를 지칭하며, 이 기술에서는 전체 네트워크에 노드기반 또는 클러스터기반 IDS가 네트워크에 존재한다고 가정한다. IV는 공격 패킷의 다이제스트가 포함된 요청을 브로드캐스트를 하여 이전에 패킷을 전달했던 모든 노드로부터 응답을 모은다. 하지만 이와 같은 방법은 고정된 라우터를 필요하기 때문에 동적 토폴로지에서는 사용하기 어렵다.

핫스팟기반 역추적에서는 모든 노드가 전달받은 IP 패킷의 TTL 값을 관찰하고 자신의 전송 범위에 있는 노드들에 대한 이웃 목록(neighbor list)을 요구한다. 하지만 TTL 값은 공격자에 의해서 수정될 수 있기 때문에 RTTL(Relative TTL)이란 값으로 변환하여 패킷에 저장한다. 패킷 P에 대한 RTTL 값은 다음과 같이 계산된다.

$$RTTL(P) \equiv TTL(P) \bmod (2^c - 2) \qquad (10)$$

계산식에서 $TTL(P)$는 P의 IP 헤더의 TTL 값을 의미한다. 만약 노드 A로부터 노드 B로 패킷 P을 전달하고 노드 A, B를 모두 안전한 노드라고 가정한다면, 노드 A와 B에 저장된 P에 대한 $RTTL$ 값의 안전성은 다음과 같으며, 2^c-2는 네트워크에서 최대 경로 길이이며, c는 비트 수이다.

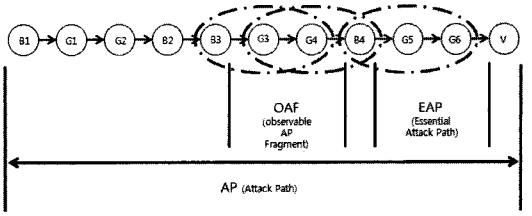
$$RTTL_A(P) = RTTL_B(P) + 1 (\bmod 2^c - 2) \qquad (11)$$

핫스팟기반 역추적은 다음과 같은 정의를 한다.

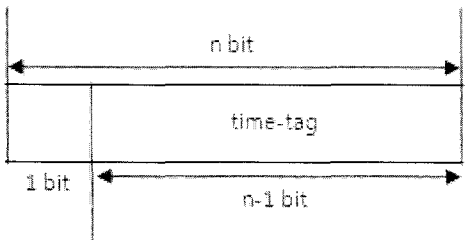
- 핫스팟: 하나 이상의 알려지지 않은 공격 노드가 존재할 가능성이 있고, 안전한 노드 주변에 의심스러운 노드의 존재가 예상되는 지역으로 정의한다.
- AP(Attack Path): 공격자 노드에서 피해자 노드까지 패킷이 전송되는 경로이다.
- AP fragment: 공격 경로 안에서 안전한 노드가 연속적으로 존재하는 경로를 말한다.
- OAF(Observable AP Fragment): AP fragment의 일정 구역을 나타내며, OAF 안에서의 모든 노드는 피해자 노드와 같은 패킷의 다이제스트로 동일하게 계산한다.
- EAP(Essential Attack Path): OAF의 특별한 경우로, 피해자 노드에 가장 근접한 OAF이다. 여기서 EAP에는 피해자 노드가 포함이 될 수도 있고 되지 않을 수도 있다.

[그림 5]에서 공격자 노드 B_1부터 피해자 노드 V까지가 공격 경로이다. 모든 B 노드는 정상적인 동작을 따르지 않고 임의의 동작을 수행하는 의심스러운 노드이고, 모든 G 노드는 정상적인 동작을 따르는 안전한 노드이다.

B_3 노드에서 패킷 다이제스트가 변경되고, B_4 노드에서 패킷 다이제스트에 변경이 없다고 할 때, EAP를 포함하는 두 개의 OAF을 확인할 수 있다. 공격 경로에서 G_1 노드를 관찰하지 않기 때문에 B_1 노드가 패킷 다이제스트를 변경하였는지를 확인할 수 없다. 공격을 탐지한 노드 IV는 전체 네트워크에 존재하는 노드들에게 공격 패킷의 다이제스트를 브로드캐스트하고 RTTL 값과 이웃 목록을 수집하고 OAF 안에 존재하는 G_3, G_4, G_5를 중심으로 하는 3개의 hotspot를 확인할 수 있다. Hotspot를 통해 B_3과 B_4가 악의적인 노드라는 것을 알



〔그림 5〕 공격 경로



〔그림 6〕 시간 태그 블룸 필터

수 있고, hotspot을 온/오프라인으로 저장된 정보를 분석하여 공격 경로를 찾는다.

3.4 시간 태그 블룸 필터(time-tagged bloom filter)

시간 태그 블룸 필터[10]는 로깅기반 IP 역추적(logging-based IP traceback)에서 토폴로지 변경 문제와 리소스 문제를 해결하기 위해 블룸 필터의 타임 태그를 수정하여 제안되었다.

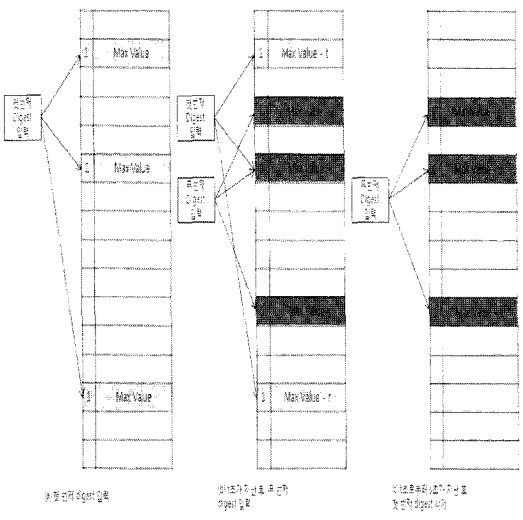
시간 태그 블룸 필터 기술은 효과적인 데이터 수집을 위해 네트워크를 클러스터(cluster)로 나누고 각 CH (Cluster Head) 노드는 지나가는 패킷을 모니터링하기 위해 N-IDS(Network Intrusion Detection System)가 있다고 가정한다. CH 노드는 로그를 축적하고, 한 노드가 현재 CH 노드 범위 밖으로 이동하게 되면 이동하게 된 CH 노드에게 공격 패킷, 공격 목표, 공격 시간이 담긴 역추적 정보를 제공함으로서, 네트워크 토폴로지가 변경되더라도 새로운 CH 노드에 전달되어 공격 경로가 유지될 수 있도록 한다. 패킷 정보는 각 입력의 수명 시간(life time)을 보여주는 시간 태그 블룸 필터에 저장된다. 시간 태그를 사용하여 제한된 저장 공간에서 새로운 로그 정보를 유지할 수 있다.

시간 태그 블룸 필터는 [그림 6]과 같이 n 비트의 길이에 1비트는 기존 블룸 필터와 같이 값의 저장 여부를 표시하고, 1비트를 제외한 나머지 비트는 시간 태그로 n-1 비트의 MAX 값으로 설정하여 사용할 수 있다. 이 MAX 값은 일정 시간이 지나면서 감소하여 삭제된다.

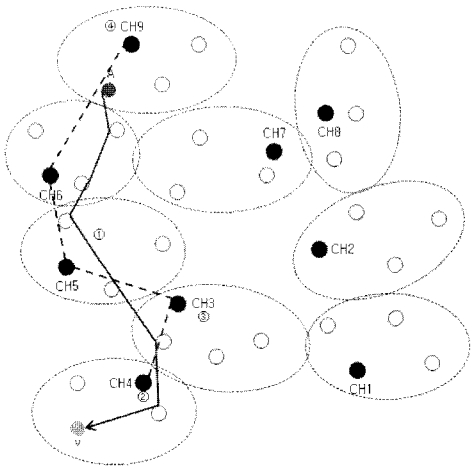
아래 [그림 7]은 시간 태그 블룸 필터의 예로, 첫 번째 다이제스트가 입력되고 3개의 비트에 표시되고 time-tag에 MAX의 값이 저장된다. 그리고 임의의 t초가 흐른 후 두 번째 다이제스트가 입력되고 또 다른 3개의 비트가 표시되면서 첫 번째 다이제스트 입력과 동일한 위치의 비트가 있다면 그 비트의 time-tag는 MAX 값으로 덮어씌워지고 첫 번째 입력의 나머지 두 비트는 MAX 값에서 t초만큼 감소된다. 그 후 임의의 s초가 지나 첫 번째 다이제스트 입력의 MAX 값이 다 소모된다면 처음에 저장된 비트는 삭제되고 두 번째 입력의 비트들은 MAX 값에서 s초만큼 감소된다.

시간 태그 블룸 필터는 전체 네트워크는 클러스터로 구성되어 있고, 노드는 H-IDS(Host-based Intrusion Detection System)에 의해서 보호되고 있다고 가정한다.

한 노드에서 공격을 탐지하게 되면 공격 패킷, 공격 목표, 공격 시간이 담긴 정보와 타겟 다이제스트를 가진 CH 노드인지를 확인하는 메시지를 포함하여 역추적 메



〔그림 7〕 시간 태그 블룸 필터의 예



〔그림 8〕 시간 태그 블룸 필터 역추적

〔표 1〕 IP 기반 역추적 분석

(×:N/A △:좋음,높음 □:보통 ▽:나쁨,낮음)

항목 / 기술	관리 시스템 부하	피해 시스템 부하	메모리 요구	대역폭 부하	확장성	필요 패킷 수
Logging	△	×	△	×	□	1
PPM	▽	△	△	×	△	△
iTrace	▽	△	△	▽	△	△
Hash-based	△	▽	▽	▽	□	1

시지를 만들고 CH 노드는 이 메시지를 저장한다. 만약 역추적 메시지에 포함된 타겟 다이제스트가 이미 CH 노드에 있다면 메시지를 무시한다.

시간 태그 블룸 필터에서 역추적 단계를 다음과 같다.

① 그림 8에서 공격자 노드 A는 피해자 노드 V로 공격 패킷을 보낸다. 그러면 공격 경로에 있는 모든 CH 노드는 이 공격 패킷에 대한 패킷 정보가 있어야 한다.

② V 노드는 공격을 탐지하면 자신이 속해있는 클러스터의 CH4 노드에 역추적을 요청하고 CH4 노드는 자신의 주변 클러스터의 CH 노드에 역추적 정보를 전달한다.

③ 주변 클러스터의 CH 노드 중에서 CH3 노드가 역추적 정보에 응답하고 자신의 이웃 클러스터의 CH 노드에 역추적 정보를 제공한다.

④ 이러한 과정을 반복하여 CH4 노드부터 CH3, CH5, CH6를 지나 CH9 노드에 도달하게 되고 CH9 노드의 역추적 정보를 바탕으로 공격 노드를 찾아낸다.

Ⅳ. 분석

4장에서는 앞서 살펴본 역추적들을 비교 분석한다. 역추적을 비교 분석하기 위한 관리 시스템 부하, 피해 시스템 부하, 메모리 요구, 대역폭 부하, 견고성, 확장성, 필요 패킷의 수를 비교한다. 각 항목에 대한 설명은 다음과 같다[3,4,10].

- 관리 시스템 부하: 관리 시스템 부하 발생 정도
- 피해 시스템 부하: 피해 시스템 부하 발생 정도
- 메모리 요구: 역추적 정보를 저장하기 위한 공간을 필요로 하는 정도
- 대역폭 부하: 역추적 메시지로 인해 네트워크 트래픽이 증가하는 정도
- 견고성: DDoS 공격에 효과적이고 안전한 정도
- 확장성: 역추적 매커니즘의 크기가 역추적 정확성을 유지하며 사용자 수의 증대에 유연하게 대응할 수 있는 정도
- 필요 패킷 수: 공격 경로를 재구성 하는데 필요 패킷의 수

[표 1]에서는 IP 기반 역추적에 대하여 비교 분석한 것이고, 아래 [표 2][10]는 ad-hoc 네트워크 역추적에 대해서 작성한 것이다.

시스템 부하는 time-tagged bloom filter가 CH 노드에서만 역추적 정보를 수집하기 때문에 CH 노드에서만 부하가 발생하지만, 다른 기술들은 각각의 노드에서도 역추적 정보를 수집해야만 되기에 각각의 노드에서도

〔표 2〕 Ad-hoc 네트워크 역추적 분석

(×:N/A △:좋음,높음 □:보통 ▽:나쁨,낮음)

항목 / 기술	관리 시스템 부하	피해 시스템 부하	메모리 요구	대역폭 부하	확장성	필요 패킷 수
SWAT	△	△	△	▽	△	1
Hotspot-Based	△	▽	▽	□	△	1
Cross-layer Monitoring	△	△	△	▽	△	1
Time-Tagged Bloom Filter	△	×	▽	▽	△	1

부하가 발생한다. 하지만 hotspot-based는 역추적 경로에 필요한 핫스팟에서만 역추적 정보를 수집하기에 상대적으로 적은 부하가 발생한다. 메모리 요구는 SWAT와 cross-layer monitoring은 직접적으로 공격 시그니쳐를 저장하기 때문에 상대적으로 많은 양의 저장을 필요로 한다. 하지만 hotspot-based와 time-tagged bloom filter는 블룸 필터를 사용하여 제한적인 저장 공간을 필요로 한다. 대역폭 부하는 SWAT, cross-layer monitoring, time-tagged bloom filter는 역추적 메시지를 위해 멀티캐스트를 사용하지만, hotspot-based에서는 브로드캐스트를 사용한다. 확장성은 전반적으로 모든 기술이 좋은 확장성을 보이고 있다. SPIE 시스템 구조는 역추적 프로세스가 정립되어 있어 확장성을 얻기 어렵지만, hotspot-based는 IV를 통해서 확장성을 향상 시켰다.

V. 결론

Ad-hoc 네트워크는 환경이 빠르게 변하기 때문에 구성이나 규모를 예측하기가 어렵다. 이런 이유가 ad-hoc 네트워크에서 역추적을 어렵게 만든다. 하지만 ad-hoc 네트워크에서도 기존 인터넷 망에서 발생한 공격의 위협이 존재한다. 이런 공격에 대응하여 공격 근원지를 파악하기 위한 역추적 연구가 진행되고 있고, 우리는 대표적인 ad-hoc 네트워크 역추적의 개념과 동작에 대해서 살펴보았다.

기존의 IP기반 역추적 기술들이 실제 네트워크에 적용하지 못하는 문제점을 가지고 있는 것과 마찬가지로 ad-hoc 네트워크 역추적도 실제로 적용하지 못하는 문제점이 있다. 이러한 문제를 해결하기 위한 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] 김길한, 이형우, "Ad-Hoc 네트웨크에서의 패킷 마킹 기법을 이용한 공격 근원지 역추적 기법," 한국멀티미디어학회 춘계학술발표대회논문집, pp. 21-24, 2004년 5월.

[2] 정희영, 이우용, 김용진, "MANET(Mobile Ad-Hoc NETwork)의 연구 동향," ITFIND , 1998년 9월.

[3] 한정화, 김락현, 류재철, 염흥열, "역추적 기술 및 보안 요구사항 분석," 한국정보보호학회 18(5) pp. 132-141, 2008년 10월.

[4] 이형우, "네트워크 해킹 공격 대응을 위한 IP Traceback 기술", 한국통신학회지 24(9) pp. 120-131, 2004년 9월.

[5] S. Savage, D. Wetherall, and A. Karlin, T. Anderson, "Network Support for IP Traceback," IEEE/ACM Transactions on Networking Vol. 9 No.3, Jun. 2001.

[6] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T. Kent, W. Timothy Strayer, "Single-packet IP traceback," IEEE/ACM Transactions on Networking Vol.10, issue 6, Dec. 2002.

[7] Yongjin Kim, Ahmed Helmy, "SWAT : Small World-based Attacker Traceback in Ad-hoc Networks," MOBIQUITOUS, Jul. 2005

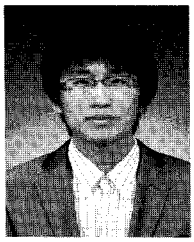
[8] Y Kim, A Helmy, "Attacker Traceback with Cross-layer Monitoring in Wireless Multi-hop Networks", SASN, Oct. 2006.

[9] Yi-an Huang, Wenke Lee, "Hotspot-Based Traceback for Mobile Ad Hoc Networks," WiSE, Sep. 2005.

[10] Il Yong Kim, Ki Chang Kim, "A Resource-efficient IP Traceback Technique for Mobile Ad-hoc Networks Based on Time-tagged Bloom Filter", ICCIT, Nov. 2008.

[11] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, W. T. Strayer, "Hash-based IP traceback", In Proceedings of the ACM Conference on Applications, Dec. 2002.

〈著者紹介〉



이 동 희 (Dong-Hee Lee)

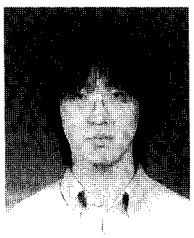
학생회원

2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 역추적

여 돈 구 (Don-Gu Yeo)

학생회원

2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, USN 보안, 클라우드 컴퓨팅 보안, IPTV 보안, 역추적



장 재 훈 (Jaehoon Jang)

학생회원

2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 역추적, IPTV 보안, USN 보안, 웹 보안

염 흥 열 (Heung-Youl Youm)

종신회원

1981년 2월: 한양대학교 전자공학과 졸업
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜