Journal of The Korea Society of Computer and Information
Vol. 22 No. 3, pp. 69-79, March 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.03.069

Comparison and Analysis of P2P Botnet Detection Schemes

Kyungsan Cho*, Wujian Ye**

Abstract

In this paper, we propose our four-phase life cycle of P2P botnet with corresponding detection methods and the future direction for more effective P2P botnet detection. Our proposals are based on the intensive analysis that compares existing P2P botnet detection schemes in different points of view such as life cycle of P2P botnet, machine learning methods for data mining based detection, composition of data sets, and performance matrix. Our proposed life cycle model composed of linear sequence stages suggests to utilize features in the vulnerable phase rather than the entire life cycle. In addition, we suggest the hybrid detection scheme with data mining based method and our proposed life cycle, and present the improved composition of experimental data sets through analysing the limitations of previous works.

▸ Keyword : P2P botnet detection, life cycle, machine learning, data sets

I. Introduction

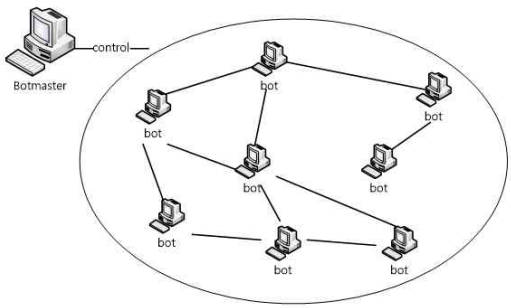
프로세서의 처리 능력이 향상되고 메모리의 용량과 입출력의 전송율이 증가됨에 따라, P2P(Peer-to-Peer) 네트워크를 통한 자원의 공유와 모바일화가 활성화되었다. 하지만, P2P 네트워크의 사용이 증가하고 P2P 트래픽이 인터넷 트래픽의 상당한 부분을 차지하면서, 대역폭과 보안 및 관리상의 문제도 증가하였다[1].

다양한 공격을 수행하는 분산 구조를 제공하는 봇넷(botnet)은 악성 소프트웨어를 수행하도록 감염된 호스트인 봇(bot)들로 구성된 네트워크이다. 특정 네트워크 또는 인터넷 상의 취약한 호스트에 트로이 목마나 바이러스와 같은 다양한 공격을 통해 악성 소프트웨어가 설치되어 감염되면, 이 호스트는 봇이 되어 봇넷에 합류된다. 이후에, 봇들은 실제 공격자인 봇마스터의 원격 명령을 받아 목적지 노드들에게 DDoS(Distributed Denial of Service) 공격, 이메일 스팸, 피싱(Phishing), 클릭 사기(Click Fraud), 민감 정보 절도등과 같은 다양한 공격을 수행한다[2].

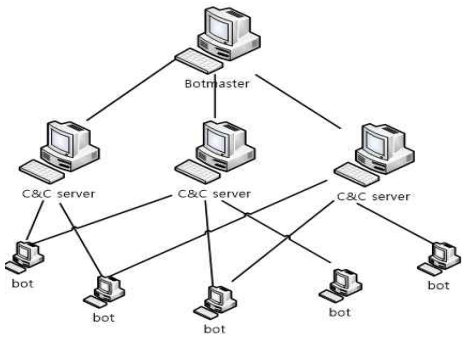
Fig. 1(a)와 같이 초기의 봇넷은 전통적인 중앙 집중적인 서버/클라이언트 구조로 형성되었으며, C&C 서버가 봇마스터를 대신하여 봇들을 관리하였다. C&C 서버와 봇 사이에 형성된 C&C 채널을 통해 전송되는 트래픽인 C&C 트래픽은 공격을 위한 명령과 갱신 정보의 전송과 수신을 위해 사용된다. P2P 분산 구조가 여러 분야에서 다양하게 활용하게 됨에 따라, 봇넷에 P2P 기술을 효율적으로 접목한 P2P 봇넷이 등장하였다. Fig. 1(b)와 같이 P2P 봇들은 인터넷 상의 어느 곳에나 존재할 수 있으므로 봇넷의 탐지는 쉽지 않다. 또한 일부 봇들이 탐지되어 제거되어도 봇넷은 계속 악성 공격 활동이 가능하다.

P2P 봇넷이 등장한 이후 P2P 봇넷을 발견하여 제거하기 위한 탐지 기법들이 제안되었다. 즉, 탐지 대상과 생애주기에서의 탐지 단계 및 탐지 기술에 따라 많은 탐지 기법과 탐지 시스템들이 제시되었다.

• First Author: Kyungsan Cho, Corresponding Author: Kyungsan Cho
* Kyungsan Cho (kscho@dankook.ac.kr), Dept. of Software Science, Dankook University
** Wujian Ye (yewjian@126.com), School of Information Engineering, GuangDong University of Technology
• Received: 2017. 03. 03, Revised: 2017. 03. 14, Accepted: 2017. 03. 21.



(a) Centralized Botnet



(b) Distributed P2P Botnet
Fig. 1. Architecture of Botnet

탐지 기법을 개선하거나 새로운 탐지 기법의 개발을 위해서는 기존 탐지 기법들의 비교 분석이 필요하다. 하지만, 기존의 P2P 봇넷 비교 분석 연구들은 탐지 기법을 분류하거나 각 탐지 기법의 특성을 나열식으로 소개만 하였다. 본 논문에서는 P2P 봇넷의 생애주기와 탐지 기법의 분류, 탐지에 사용된 데이터셋과 검증에 사용된 성능 지표 등의 다양한 측면에서 기존 P2P 봇넷 탐지에 대한 체계적인 비교 분석을 통하여 제한점을 지적하고 효율적인 탐지를 위한 연구 방향을 제시하려한다.

본 논문은 다음과 같이 구성된다. 2장은 관련 연구로 기존의 P2P 봇넷 탐지 기법과 P2P 봇넷 탐지의 비교 탐구 연구를 소개한다. 3장에서는 기존 P2P 봇넷 탐지 기법들을 생애 주기, 탐지 기법, 데이터셋, 성능 지표와 검증 결과를 기준으로 비교하고 분석한다. 4장에서는 3장의 비교 분석에 근거한 결론을 도출하고 본 논문을 마무리한다.

II. Related works

1. P2P Botnet Detection Methods

여러 악성 활동과 사이버 공격을 수행하여 네트워크 또는 인터넷의 보안을 위협하는 P2P 봇넷에 대응하는 가장 중요한 역할은 탐지이며, 다양한 탐지 기법들이 제안되었다.

실제 탐지되는 대상에 따라, 탐지는 P2P 봇 탐지 또는 P2P 봇넷 트래픽 탐지로 분류된다. P2P 봇 탐지는 정상 호스트와 구별되는 감염된 호스트(봇)를 탐지하며, P2P 봇넷 트래픽 탐지는 정상 인터넷 트래픽에서 봇넷 트래픽을 탐지한다[3]. 또한, P2P 봇넷의 생애 주기를 구성하는 어떤 단계에서 탐지하는가에 따라 탐지에 적용되는 트래픽의 특성이나 활동이 다르게 정해지므로, 이러한 특성을 이용하여 생애주기의 각 단계에서 적용되는 탐지 기법들도 제안되었다[4].

실제 P2P 봇넷의 탐지에 사용되는 기법으로는 P2P 트래픽의 탐지에서 이미 사용되었던 포트 기반, 시그니처 기반, 데이터 마이닝 기반, 트래픽 활동에 따른 비정상 기반 및 하이브리드 기법의 5가지 기법이 제안되었다[3,5]. Storm, Nugache 및 Waledac 같은 P2P 봇넷은 임의의 포트 번호를 동적으로 사용하고, 메시지 전송 시에 암호화를 사용하므로, 포트 기반과 시그니처 기반 기법은 P2P 봇넷 탐지에는 적합하지 않다[6]. 데이터 마이닝 기반 기법은 패킷 크기, 패킷 도착 간격 등과 같은 트래픽으로부터 추출된 통계적 특징에 따라 인터넷 트래픽을 분류하며, 방대한 트래픽 자료의 처리를 위해 기계학습 기법이나 클러스터링 기법들이 사용된다[7]. 비정상 기반 기법은 수집된 트래픽의 패턴이나 활동을 정상적인 트래픽의 패턴이나 활동과 비교하여 비정상의 특성을 가진 봇넷을 탐지한다[5,8]. 패킷의 포트 번호나 유효부하의 검색에 의존하지 않으며 새로운 P2P 봇넷 탐지에도 적용할 수 있어, 데이터 마이닝 기반이나 비정상 기반 기법이 많이 사용되고 있다. 하지만, 한 가지 기법만으로는 P2P 봇넷을 분류하는 데는 제한이 있으므로, 두 개 이상의 탐지 기법들을 다단계로 수행하는 하이브리드 기법도 제안되었다[3].

2. Analysis of P2P Botnet Detection Methods

기존 P2P 봇넷 탐지 기법에 대한 비교 분석은 여러 탐지 기법들을 분류하거나 각 탐지 기법들의 개요와 장단점들을 나열하여 설명하는 연구가 대부분이었다.

일부 연구에서는 봇넷 탐지 기법을 분류하고, 탐지 기법의 특성을 나열식으로 제시하였다. 즉, 봇넷 탐지 기법을 시그니처 기반, 비정상 기반(anomaly-based), DNSS 기반, 마이닝 기반의 4가지로 분류한 연구에서는, 13개의 봇넷 탐지 기법에 대해 새로운 봇넷 탐지 기능, 프로토콜 및 구조에 대한 독립 특성, 암호화의 탐지 기능, 실시간 탐지 기능 등의 특성들을 나열하였다[2]. 또한, 봇넷 탐지 기법들을 탐지 알고리즘에 따라 신경 네트워크 기반, 휴리스틱 한계 기반 및 마이닝 기반 기법의 세 가지로 분류한 연구에서는, 탐지 기법에 따라 플로우 기반, 노드 기반, 자원 공유 활동 모니터링 기반, 대화 기반, 플로우 기반과 대화 기반의 혼합 기법의 5가지로도 분류하였다[9].

P2P 봇넷 탐지의 12가지 문제점을 제시하고, 이에 대해 기존 P2P 봇넷 탐지 기법에서 제시된 해결책과 P2P 봇넷은 제어 플로우의 안정성 특성이 미비하거나, 다른 피어와의 연결을 위해 ICMP 패킷을 비정상적으로 많이 발생하거나, 또는 함수 호

출의 주기에 의해 정상 트래픽과 구별된다는 등의 발견점을 나열한 연구도 있었지만, 몇 줄 정도의 간략한 설명으로 구체적인 기법의 소개나 검증 결과는 제시되지 않았다[10].

P2P 봇넷 탐지 기법들을 탐구한 다른 연구들은 여러 탐지 기법들을 나열식으로 설명하였다. M. Elhalabi 등은 16개의 P2P 봇넷 탐지 접근 기법을 탐지 구조 및 장단점과 함께 간략하게 나열하고, 기존 탐지 기법의 제한점을 제시하였다[11]. P. Vadidu 등은 스팸 공격을 탐지하는 Botgraph, 오버레이 네트워크에 의해 형성된 통신 그래프를 조사하여 P2P 봇넷을 탐지하는 Botgrep, 유사한 통신 패턴과 악성 행위의 호스트들을 봇넷으로 탐지하는 Botminer의 구조와 탐지 기법을 장단점이나 탐지 성능에 관한 언급없이 나열식으로 설명하였다[12].

또 다른 연구에서는 P2P 봇넷의 생애 주기와 성능 지표를 소개하며 P2P 봇넷 탐지의 상세한 기법 설명은 제시하지 않거나[13], 기존 탐지 기법의 약점을 극복하는 최근의 P2P 봇넷 탐지 기법들의 장단점과 정확도를 나열하기도 하였다[14].

향후 P2P 봇넷 탐지 연구에 활용되기 위해서는 앞에서 소개된 기존 연구처럼 P2P 봇넷 탐지 기법들의 설명을 나열하기 보다는 여러 측면에서 서로 비교하여 개선되어야할 제한점을 분석할 필요가 있다.

III. Comparison and Analysis of P2P Botnet Detection Schemes

본 장에서는 기존의 P2P 봇넷 탐지 연구들을 생애주기를 고려한 탐지 단계, 탐지 기법, 데이터셋의 구성과 탐지 대상, 사용된 성능 지표와 성능 결과를 기반으로 비교 분석하고 제한점과 개선점을 제시하여 향후 탐지 연구에 기여하도록 한다. 주제의 특성상, 기존 기법들을 참고 문헌의 번호로 직접 표시한다.

1. Life Cycle and Detection of P2P Botnet

인터넷(또는 네트워크)에 연결된 호스트가 감염되어 봇이 탄생되어, 봇넷에 합류하고, 명령을 받아 공격을 수행하고, 봇넷의 정보를 갱신하는 등의 전 과정이 봇넷(또는 봇)의 생애주기이다. 생애 주기의 중요성은 특정한 단계에서 발견되는 봇넷의 특징들을 활용하면 각 단계에서 봇넷을 효율적으로 탐지할 수 있다는 것이다.

기존 연구에서는 P2P 봇넷 탐지 기법의 제안을 위해 봇넷의 생애 주기를 다룬 경우가 대부분이지만, [15-17]에서는 탐지 기법의 제안없이 생애 주기와 단계별 탐지 기법을 제시하였다. [15]에서는 P2P 봇넷의 생애주기를 한 단계에서 차단되면 다음 단계로 진행할 수 없는 선형적 순서의 특성을 갖는 conception 단계, recruitment 단계, interaction 단계, marketing 단계, attack execution 단계, attack success 단계의 6 단계로 정의하고, 각 단계에서의 일반적인 방어 전략을 제시하였다. 다른 연구에서는 다루지 않는 봇넷 생성의 동기를 제시하는 conception 단계와 봇넷의 사용 용도를 지정하는 marketing 단계는 봇넷 설계자의 활동으로, 봇넷의 방지에 매우 중요한 기능을 제공한다. [16]에서는 봇넷의 생애를 spreading and injection 단계, command and control 단계, application 단계의 3단계로 분류하고, 16 유형의 봇넷(이중에서 2 유형만 P2P 봇넷이다)에 대해 각 단계의 실 예와 대표적인 대응 기법을 도표화하였다. [17]에서는 Storm 봇넷에 대한 4단계의 생애 주기를 제시하였다. 4단계 생애주기는 infection 단계, initial 단계, communication and download 단계, secondary injection 단계로 구성된다.

봇넷 탐지 기법에 대한 여러 탐구 연구에서도 봇넷의 생애 주기를 제시하였다. [2]에서는 중앙집중적 프로토콜로 동작하는 봇넷의 생애 주기를 initial infection 단계, secondary injection 단계, connection 단계, malicious command and control 단계, update and maintenance 단계의 5단계로 설명하고, 네트워크 트래픽의 분석에 근거하여 기존의 봇넷 탐지 기법들을 분류하였다. [11,18]에서는 formation 단계, C&C 단계, attack 단계, post attack 단계로 구성되는 4단계의 봇넷 생애주기를 제시하였다. 봇넷의 구조 또는 환경을 갱신하는 과정이 있은 후에 봇넷은 다시 공격 단계로 가기 위해 C&C 단계를 거쳐야 하므로, C&C 단계와 post attack 단계는 한 단계로 통합하여 처리하는 것이 적절하며, 앞에서 소개된 [2]의 update and maintenance 단계도 connection 단계와 통합하는 것이 적합하다. 이와 유사한 제안으로 [13]에서는 P2P 봇넷의 생애주기를 construction 단계, C&C 단계, attack 단계의 3 단계로 소개하였다. [14]에서는 initial infection 단계, connection 단계, secondary injection단계, maintenance 단계의 4 단계로 제안하였는데, 같은 이유로 connection 단계와 maintenance 단계는 한 단계로 통합하는 것이 적절하다.

제안된 생애주기의 초기 단계에 봇넷을 탐지하도록 제안한 다음의 연구들도 있었다. [19]에서는 생애주기를 infection 단계, connection 단계, download 단계, attack 단계의 4단계로 설명하고, 초기의 infection 단계에서 봇넷을 탐지하여 네트워크 관리자에게 보고하였다. [20]에서는 infection 단계, construction 단계, C&C 단계, attack 단계의 4 단계로 봇넷의 생애 주기를 설명하였다. 봇넷을 찾아 합류하는 construction 단계는 봇넷 생성이 실패할 수 있는 취약한 단계이므로, 다른 봇들의 목록이나 웹 캐시를 탈취하여 봇넷의 확장을 방지할 수 있다고 제시하였다. [21]에서는 initial infection 단계, peer propagation 단계, secondary infection 단계, attack 단계의 4 단계로 P2P 봇넷 생애주기를 소개하였다. 악의적인 행동이 취해지기 전에 peer propagation 단계에서 정상 트래픽에서 봇넷 트래픽을 탐지할 수 있는 기법을 제안하였다.

[22-23]에서는 4단계의 생애주기 중에서 봇이 봇넷에 연결된 후의 C&C 채널을 통해 통신하는 waiting 단계에서의 탐지

를 제시하였다. 즉, 생애 주기의 4단계를 Infection 단계, rally 단계, waiting 단계, executing 단계로 제시하였다. [22]에서는 waiting 단계에서 서로 다른 IP주소를 갖는 호스트들 사이의 통신 특성을 활용한 P2P 봇넷 탐지 기법 “Entelecheia”를 제안하고 높은 탐지 적중률을 보였다. [23]에서는 P2P 봇넷의 특성을 플로우가 아닌 대화(서로 다른 두 IP 주소를 갖는 호스트들 사이의 통신) 단위로 분석하고 rally 및 waiting의 두 단계에서 봇넷을 탐지하였다.

[24]와[25]에서는 P2P 봇넷 생애주기의 특정한 단계가 아닌 생애 주기의 전 과정을 통하여 다단계로 수행되는 탐지를 제안하였다. [24]에서는 봇넷의 생애 주기에 대한 설명없이, 감염된 봇이 봇넷에 접속하는 단계에서 P2P 노드를 탐지하고, C&C 단계에서 P2P 네트워크를 탐지하고 공격 단계에서 P2P 봇넷을 탐지하는 3 단계 모델을 제시하였다. [25]에서는 [26]에서 제시한 initial 단계, trance 단계, attack 단계의 세 단계로 생애 주기를 설명하고 각 단계의 트래픽 특징을 이용한 다단계 탐지 기법을 제안하였다.

다음 연구들에서는 봇넷의 생애 주기에 대한 설명은 없이, 특정 단계에서 수행되는 탐지 기법을 제안하였다. [27]에서는 P2P 봇넷의 선제적 탐지를 위해 C&C 단계에서 기계학습 기반의 세 분류기법을 비교하였다. [28]에서는 C&C 단계에서 인터넷 상의 원격 C&C 서버와 긴 연결 또는 다중의 단기 연결을 하는 감염된 호스트를 탐지하였다. [29-30]에서도 C&C 단계에서의 탐지를 제시하였다. [31]에서는 정해진 시간 구간에서 TCP/UDP 네트워크 플로우 특성을 관측하여 C&C 단계와 공격 단계에서 P2P 봇넷 트래픽을 정상 트래픽에서 탐지하였다.

[32]에서는 봇넷의 생애 주기를 recruiting members 단계, forming the botnet 단계, standing by for instructions 단계의 3단계로 설명하고 봇넷을 방어할 수 있는 두 기법인 index poisoning과 sybil attack을 제안하였다. [13]에서는 P2P 봇넷의 생애주기를 construction 단계, C&C 단계, attack 단계의 3단계로 소개하였고, [14]에서는 initial infection 단계, connection 단계, secondary injection단계, maintenance 단계의 4 단계로 제안하였다.

앞에서 소개된 바와 같이, 기존 연구에서는 생애 주기 모델의 특정한 한 두 단계 또는 세 단계를 통해 탐지한다. 즉, 특정한 단계에서의 탐지가 만능일 수는 없다. 서로 다른 봇넷은 생애주기의 각 단계에서 서로 다른 트래픽 특성을 보일 수 있으므로, 해당 P2P 봇넷이 주어진 환경의 가장 취약한 단계에서 탐지하여 처리하는 것이 더 효율적이다.

본 연구에서는 다음과 같은 P2P 봇넷의 4 단계 생애주기를 제안하고, 각 단계에서의 특성과 탐지 방법을 함께 제시한다.

1) 봇의 감염 단계: 여러 경로를 통해 호스트를 감염시키는 과정으로 악성 활동의 특성이나 시그니처 등과 같이 감염 방법에 따라서 적합한 침입 탐지 시스템으로 탐지한다.
2) 봇넷 합류 단계: 감염된 봇이 봇넷의 일원이 되는 과정으로 해당 P2P 봇넷에 합류하는 초기 패킷의 특성 또는 패킷 교환 트래픽의 특성을 이용해 탐지가 가능하다. 봇넷에 합류하기 위해 접촉할 다른 봇들의 목록 또는 공유 웹 캐쉬를 탈취하여 공격을 무력화 시킬 수 있다.
3) C&C/유지 단계: 악성 공격이 시작되기 이전에 봇들이 필요한 정보나 명령을 송수신한다. 또한 봇넷을 유지하고 갱신하는 과정도 포함한다. 지속적인 일정한 크기의 작은 패킷의 발생과 패킷과 패킷 사이의 긴 도착 시간, 봇과 봇 사이의 오랜 연결 시간과 같은 해당 P2P 봇넷의 트래픽 특성과 플로우 특성을 이용하여 탐지가 가능하다.
4) 공격 단계: 봇마스터의 명령에 따라 지시된 공격을 수행하는 과정으로, 공격의 유형과 특성에 따라 기존의 침입 탐지 기법으로 탐지가 가능하다.

실제 봇은 감염, 봇넷 합류, C&C, 공격 단계 이후에는 C&C/유지와 공격 단계를 반복하게 된다.

Table 1.은 기존 연구에서 소개된 봇넷의 생애 주기를 본 연구에서 제안한 4 단계의 생애주기를 기준으로 정리한 것이다.

Table 1. Proposed Life Cycle of P2P Botnet

phase	infection	connection	C&C/main-tenance	attack
[15]	* => recruitment	Interaction => **		attack /success
[16]	spreading/injection	C&C		application
[19]	**infection**	connection	download	attack
[20]	infection	**construction**	C&C/update	attack
[21]	initial infection	**propagation**	2nd infection	attack
[23]	infection	**rally**	**waiting**	executing
[22]	infection	rally	**waiting**	executing
[32]	recruiting	**forming**	**standing**	***
[31]	***	***	**C&C**	**attack**
[24]	***	**join botnet**	**C&C**	**attack**
[25]	***	**initial**	**trance**	**attack**
[17]	injection	initial	connection/ download	2nd injection
[13]	construction		C&C	attack
[11] [18]	formation		C&C/post attack	attack
[14]	initial infection	connection/maintenance		2nd injection

*: conception stage, **: marketing stage, ***: not specified
bold type means the proposed detection stage of the reference

2. P2P Botnet Detection Methods

본 절에서는 P2P 봇넷 탐지 기법들을 탐지 기술을 기반으로 포트 기반, 시그니처 기반, 통계 및 데이터 마이닝 기반, 비정상 기반 및 하이브리드 기반의 기법으로 분류하고 실예와 특성을 제시한다.

2.1 Port-based and Signature-based

특정한 포트 번호를 이용해 연결되던 초기에 사용되었던 포트 기반의 기법은 사용되는 포트 번호를 검사하여 P2P 봇넷 트래픽을 쉽게 탐지할 수 있고, 시그니처 기반의 기법은 Snort 같

은 침입탐지 시스템에서 알려진 봇넷의 유용한 시그니처를 적용하여 정확하게 봇넷을 탐지할 수 있다. 대부분의 P2P 봇넷은 임의의 유용한 포트 번호를 사용하고 또한 메시지 전송에 암호화 기법을 사용하므로, 이 기법들은 현재는 보조적인 수단으로 사용되고 있다[6][33].

2.2 Statistics and Data mining-based

서로 다른 응용에 의해 생성되는 트래픽은 각각 고유한 특징을 가질 수 있다. 데이터 마이닝 기반의 기법은 트래픽의 추적에서 추출된 통계적 특징에 따라 다양한 트래픽을 구별한다. 트래픽의 양과 특징의 수가 증가함에 따라 수작업으로 특징들을 여러 트래픽 유형으로 매핑하기는 어려운 일이다. 따라서, 기계 학습 알고리즘을 적용하여 사전에 분류된 훈련용 데이터 셋을 활용하여 트래픽을 분류하게 되었다[27].

많은 P2P 봇넷 탐지 연구에서는 P2P 봇넷 탐지에 사용되는 대표적인 기계학습 기법은 KNN(K-Nearest Neighbors), ANN(Artificial Neural network), SVM(Support Vector Machine), DT(Decision Tree), RL(Rule Learner), NB(Naive Bayesian) 등을 적용하여 탐지 성능을 비교하였다.

특정한 P2P 봇넷을 탐지하기 위해 기계학습을 적용한 여러 연구가 있었는데, [29]에서는 P2P 봇넷 Peacomm의 탐지를 위해 인터넷 트래픽의 특징을 분석하고 J48(decision tree C4.5의 구현), Naive Bayesian 및 BayesNet의 기계학습을 이용한 데이터마이닝 기반 기법을 적용하였다. 세 가지 기계학습 방법 중에서 정확도는 J48이 가장 우수하였다. 또한, [23]에서는 2-tuple 대화 기반의 기법을 사용하였는데, 두 유형의 P2P 트래픽(eMule, uTorrent)과 2 유형의 P2P봇넷 트래픽(Storm, Waladec)을 세 가지의 기계 학습 기법(bayesian network, J48 Decision Tree, Boosted REPTree)을 적용하여 분류하였다. P2P 트래픽의 탐지는 J48 Decision Tree가 P2P 봇넷 트래픽의 탐지는 bayesian network이 좋은 결과를 보였다. [28]에서는 P2P 봇넷 탐지를 위해 RF(Random Forest), KNN MLP(Multi-Layer Perception)의 알고리즘을 적용하였다. MLP가 정확도와 FP율에서 가장 우수하고, TP율과 precision, F-지수는 KNN이 우수한 것으로 평가되었다.

웹 트래픽 및 P2P 트래픽과 분류하여 P2P 봇넷 트래픽을 탐지하기 위해 기계 학습을 적용한 연구도 있었다. [3]에서는 웹 트래픽에서 P2P 트래픽을 분류하고 P2P 트래픽에서 P2P 봇넷 트래픽을 분류하는 2단계 하이브리드 탐지 시스템을 구현하였는데, 선행 연구인 [34]에서 CART, C4.5보다 우수하게 평가된 REPTree와 휴리스틱을 사용하여 좋은 결과를 얻었다. [30]에서는 트래픽의 특징을 선정하고 기계학습 기법 J48, IBk(Nearest Neighbour), NB를 적용하여 인터넷 트래픽을 비 P2P 트래픽, 정상 P2P 트래픽, 및 P2P 봇넷 트래픽으로 분류하였다.

웹 트래픽에서 P2P 봇넷 트래픽 탐지를 위해 기계 학습을 사용한 연구도 제안되었다. [27]에서는 J48, LSVM (Linear Support Vector Machines), BN(Bayesian Network)의 기계학습 알고리즘들을 이용하여 P2P 봇넷의 C&C 트래픽을 정상 트래픽과 분류하였으며, bayesian network의 성능이 가장 우수하였다. [31]에서는 시간 구간동안 얻어진 트래픽에 근거하여 기계학습 기법인 bayesian network과 REPTree 기법을 적용하여 봇넷 트래픽과 일반 트래픽을 분류하였는데, REPTree 기법이 좋은 성능을 보였다. [19]에서는 감염된 호스트를 생애주기의 초기 감염 단계에서 신속하게 탐지하여 보고하는 P2P 봇넷 탐지 시스템을 제안하였다. 데이터 마이닝 기반의 탐지 시스템은 Bayesian 분류기와 NN(Neural Network) 분류기를 사용하였고, 실험 결과 NN 분류기의 정확도가 높았다.

또한 비슷한 특성을 가진 트래픽들 혹은 유사한 트래픽을 가진 P2P 노드들을 하나의 그룹으로 묶는 클러스터링(clustering)을 이용한 탐지 기법도 데이터 마이닝 기법으로 제안되었다. [35]에서 제안한 Botminer는 다음과 같이 2 단계로 동작한다. 첫 단계에서 유사한 트래픽의 악성 공격 활동을 패킷 내용 분석과 시그니처 기반으로 A-plane으로 클러스터링하고 C&C 통신 트래픽 패턴을 C-plane으로 클러스터링하며, 두 번째 단계에서 이 두 plane을 상호 연계하여 유사한 악성 활동과 통신 패턴을 갖는 호스트를 봇으로 탐지한다. 하지만, 감염된 호스트들의 그룹에만 적용되고, 정상 C&C 트래픽 사용하는 봇은 탐지할 수 없는 단점을 가진다. [36]에서는 HTTP, IRC 및 P2P 봇넷의 탐지를 위해 온라인 트래픽 플로우의 클러스터링 방법을 제안했다. [24]에서는 네트워크 계층과 트랜스퍼 계층에서 일반 네트워크 스트림과 다른 P2P 네트워크 데이터 스트림의 특징들로 P2P 노드들을 클러스터링하여 P2P 응용을 탐지하는 기법을 제안했다. 이 탐지 기법은 P2P 노드 탐지, P2P 노드들의 클러스터링, P2P 봇넷 탐지의 3 단계로 동작한다.

Table 2.에서 보인 바와 같이 선정된 환경에서 정해진 특징의 P2P 봇넷 탐지 시스템에서는 가장 우수한 기계 학습 기법이 정해지지만, 모든 탐지 시스템에서 가장 우수한 기계 학습 기법은 정할 수 없다. 기존 연구에서는 트래픽(플로우 또는 대화)의 선정된 특징과 기계 학습의 탐지 기법을 주로 다루었는데, 이들만이 탐지의 성능을 정하는 것은 아니다. 따라서, 탐지 환경(탐지 단계, 데이터셋 및 탐지 대상)에 따른 탐지 기법의 성능에 대한 분석 연구가 필요하다.

Table 2. Comparison of Machine Learning Schemes for Detecting P2P Botnet

refer.	ML method	detection category	phase	feature, number of features
[28]	RF, KNN, **MLP**	normal, P2P botnet	C&C	not specified
[27]	J48, LSVM, **BN**	normal, P2P botnet	C&C	the largest packet, 10
[23]	**BN,** J48, REPTree	P2P, P2P botnet	conne, C&C	conversation length, 4
[31]	BN, **REPTree**	normal, P2P botnet	C&C, attack	average packet size, 8
[29]	**J48**, NB, BN	normal,	C&C	average packet

		P2P botnet		size, 13
[30]	J48, **IBk**, NB	non P2P, P2P, P2P botnet	C&C	average flow size, 12
[19]	Bayesian, **NN**	normal, P2P botnet	infec-tion	number of UDP packets, 4
[3]	REPTree (2 step)	non P2P, P2P, P2P botnet	C&C, attack	packet size, 5

bold type means the best method in the reference

2.3 Traffic behavior-based

기본 개념은 트래픽의 패턴이나 활동(behavior)을 관측하여 정상적인 응용에 비해 과도한 트래픽 양과 같은 비정상적인 트래픽이나 특정한 패킷의 교환과 같은 다른 응용에는 없는 특별한 트래픽 활동을 찾아내어 P2P 봇넷을 탐지하는 기법이다.

앞에서 소개된 생애주기의 각 단계에서 봇넷이 발생할 수 있는 특성을 감지해 P2P 봇넷을 탐지하는 연구가 제안되었다. [37]에서는 UDP 패킷의 DFE(Data Flow Entropy)과, ICMP, SMTP 및 UDP 패킷의 비율을 이용해 bot initialization 단계 및 secondary injection 단계의 비정상 활동을 표시하고 이런 비정상 활동의 특징과 Multi-chart CUSUM 알고리즘으로 P2P 봇넷을 탐지하였다. [33]에서는 C&C 트래픽의 플로우 의존성(dependency)에 따라 P2P 봇의 통신을 탐지하고 클러스터링을 이용하여 정상 호스트와 봇 호스트를 식별하였다. C&C 단계에서 정상 트래픽은 'stability'를 보이지 않지만, Storm 봇넷은 고도의 'stability'를 가진다는 특성을 이용한 P2P 봇넷을 탐지 기법도 제안되었다[38].

[24]에서는 attack 단계에서 스캔 활동, DDOS 공격, 스팸 전송 등의 유사한 악의적 활동에 기반하여 P2P 봇넷을 탐지 하였다. [39]에서는 봇이 봇넷을 형성하기 위하여 다른 봇의 검색, 다른 봇 정보의 교환, 공격을 위한 검사 등과 같은 단계적 플로우를 생성한다는 관측에 따라 P탐지 기법을 제안하였다. 또한, 앞 절에서 소개된 Botminer는 감염된 봇들이 C&C 단계에서는 동일한 통신 패턴을, 공격 단계에서는 유사한 악성 활동을 보인다는 특성을 기반으로 P2P 봇넷을 탐지하였다[35].

비정상 기반의 탐지 기법은 생애주기의 각 단계에서 발생하는 트래픽 패턴을 활용하는 장점이 있지만, 이러한 비정상 패턴의 발생이 매우 드문 경우에는 탐지에 어려움이 있다. 또한, 대부분의 비정상 패턴은 잘 알려진 P2P 봇넷 트래픽에서만 추출되어 새로운 또는 드문 P2P 봇넷에는 적용하기 어렵다는 단점이 있다. 또한, 새로운 비정상 패턴에 대한 탐지가 계속 필요하다.

2.4 Hybrid

앞에서 소개된 각 탐지 기법은 장점과 제한점을 가지므로, 한 가지 기법의 적용으로는 탐지의 효율성을 올릴 수 없다. 따라서, 2가지 이상의 기법을 적용한 다단계의 하이브리드 기법들이 제안되어 좋은 탐지율을 보이고 있다.

[3]에서는 연결 휴리스틱과 REPTree를 적용한 P2P 트래픽 분류기와 패턴 휴리스틱과 REPTree를 적용한 P2P 봇넷 트래픽 분류기의 2 단계로 구성된 하이브리드 탐지 시스템을 제안하였다. [40]에서는 Storm 봇넷을 탐지하기 위한 2 단계의 하이브리드 기법을 제안하였다. 첫 단계에서는 각 호스트의 트래픽으로부터 휴리스틱과 포트번호를 이용해 P2P와 SMTP 패킷을 분류하였다. 두 번째 단계에서는 유효부하 크기, TCP/UDP 비율, SMTP 패킷수 등의 트래픽 특성을 적용한 SVM을 이용하여 정상 P2P 트래픽으로부터 Storm 트래픽을 탐지하였다.

[41]에서는 P2P 호스트 탐지 모듈과 P2P 트래픽 분류 모듈로 구성된 두 단계 분류 시스템 PeerRush를 제안하였다. PeerRush는 호스트 연관 특징을 이용하여 P2P 호스트를 식별한 후에, 이 호스트들에 의해 생성되는 트래픽을 각 개별 분류기를 통하여 특정 P2P 응용 또는 P2P 봇넷 트래픽으로 분류하였다. [4]에서는 학습과 탐지의 두 단계로 동작하는 하이브리드 P2P 봇넷 탐지 시스템 PeerMinor를 제안하였다.

다단계 하이브리드 기법은 다단계를 수행하기 위한 연산양의 증가로 확장성에 제한이 있으며 탐지 성능도 한계가 있다는 문제점을 가진다. 이러한 문제점을 해결하면서 앞 절에서 소개된 데이터 마이닝 기반과 본 논문에서 제안한 생애주기의 각 단계별로 적용할 수 있는 비정상 기반이 효율적으로 결합된 하이브리드 기반의 탐지 시스템에 관한 더 많은 연구를 제안한다.

3. Data sets and Detection Target

P2P 봇넷의 탐지는 대부분 인터넷 또는 특정 네트워크를 통해 전송되는 트래픽을 분석하여 이루어진다. 분석할 트래픽은 P2P를 제외한 정상 트래픽, 봇넷을 제외한 P2P 트래픽, P2P 봇넷 트래픽 등으로 구성된다. 탐지하려는 대상과 환경에 따라 데이터셋은 다른 구성을 가질 수 있다. 기존 연구에서는 이미 발표된 데이터셋과 자신이 새로 캡쳐한 데이터셋을 혼용하는 방법을 많이 사용한다. 기계 학습의 경우에는 형성된 데이터셋을 훈련과 테스트에 적용하는데, 충분하지 못한 데이터를 보강하기 위해 10-fold cross validation 기법을 사용하여 데이터셋을 10개의 랜덤 셋으로 나누고, 그중의 9개는 훈련에 1개는 검증에 사용하는 과정을 10번 반복한다.

본 절에서는 기존 연구에서 탐지하여 분류하려는 대상과 이를 위해 사용된 데이터셋을 비교하고 분석한다.

[23]에서는 정상 P2P 트래픽과 P2P 봇넷을 분류하였다. 즉, 2가지의 정상 P2P 트래픽(eMule, uTorrent)과 2가지의 P2P 봇넷 트래픽(Storm, Waledac)을 데이터셋으로 사용하여 이들에 대한 식별을 제공하였다. 따라서, 새로운 봇넷에 대한 식별은 불가능하며, P2P가 아닌 일반 정상 트래픽으로부터 P2P 봇넷 트래픽 식별은 제시하지 못하였다.

다음 연구들은 정상 트래픽에서 P2P 봇넷 트래픽을 탐지하였다. [31]에서는 Storm과 Waldedac을 포함하는 악성 트래픽의 두 개의 데이터셋과 헝가리 Ericsson 연구소의 정상 트래픽 데이터셋을 혼합하여 파일을 생성한 후에 이를 다시

LBNL(Lawrence Berkeley National Lab.)의 정상 트래픽 데이터셋에 합하여 데이터셋을 구성하여 악성 트래픽을 탐지하였다. 탐지 성능을 높이기 위해 10-fold cross validation 기법을 사용하였다. [22]에서는 Storm과 Nugache로부터 캡쳐된 봇넷 트래픽을 실제 웹 트래픽 트레이스와 혼합한 데이터셋을 사용하였다. [28]에서는 wireshark을 이용하여 캡쳐한 패킷들과 기존에 발표된 표준 데이터셋을 혼합하여 사용하고, 악성 트래픽을 탐지하였는데, 캡쳐된 패킷 중에서 양방향 플로우 패킷만 사용하고, 단방향 플로우는 제외하였다. 탐지 성능을 위해 10 fold cross validation을 적용하였는데, 구체적인 P2P 봇넷에 대한 정보는 없다. 또한, [43]에서 예측 모델에 대해 좋은 성능을 보인 SMOTE를 이용해 클래스 임밸런스 문제를 해결하였다. [27]에서 사용된 데이터셋은 UT at Dallas에서 수집한 Nugache의 봇넷 데이터셋과 Wireshark을 이용해 수집된 정상 웹 플로우의 패킷들로 구성된다. 단일 패킷의 플로우와 NetBios 서비스, 방송, DHCP의 플로우의 패킷은 데이터셋에서 제외하였고, 봇넷 트래픽 분류를 위해 10 fold cross validation을 적용하였다. [21]에서는 Waledac과 Storm 봇을 포함한 Honeynet project의 악성 트래픽과 Ericsson 연구소와 LBLN의 정상 트래픽으로 구성된 ISOT 데이터셋과 ISCX 데이터셋을 사용하였으며, 정확한 탐지를 위하여 10-fold cross validation 기법을 적용하였다.

다음 연구들에서는 P2P가 아닌 비P2P 트래픽, 정상 P2P 트래픽, P2P 봇넷 트래픽의 데이터 셋을 혼합하여 사용하였다. [3]에서는 비P2P 트래픽, 정상P2P 트래픽, P2P 봇넷 트래픽을 분류하였다. 이를 위하여, 5개의 정상 트래픽 데이터셋(UNIBS, Univ. of Brescia의 트래픽, 헝가리의 Ericcson 연구소의 트래픽, 단국대학교에서 수집한 3개의 트래픽)과 3개의 악성 데이터셋(Storm/Waledac 트래픽, Waledac/Conflicker/Storm 트래픽, Bredolab/Kelihos-hlux/Zeus 트래픽)을 혼합하여 데이터셋을 형성하고 10 fold cross validation을 사용하였다. 또한, [41]에서 제안된 PeerRush는 비P2P, 정상P2P, P2P 봇넷의 세 데이터셋을 사용한다. 즉, 자체 수집한 non-P2P 트래픽의 데이터셋, P2P 응용(Skype eMule, Torrent, Frostwire 및 Vuze)에 의해 생성된 P2P 데이터 셋, 세 가지 P2P 봇넷(Storm, Waledac, Zeus)의 데이터셋에 대해 10 fold cross validation를 수행하였다.

다음의 경우에는 시뮬레이트되는 데이터셋을 활용하였다. [25]에서는 한 PC에 봇 서버를 설치하고, 또 다른 PC에 Peacomm P2P 좀비 바이러스를 설치하여 4 대의 좀비 호스트를 가상머신으로 시뮬레이트하였다. 가상 좀비 호스트들로부터 initial 및 trance 단계의 봇넷 트래픽을 수집하고, 이를 정상 네트워크 트래픽과 혼합하여 오프라인 탐지에 이용하였다. [24]에서는 3 유형의 P2P 응용(Bittorrent, Emule, Kazaa)과 3 유형의 P2P 봇넷(Storm, Nugache, Slapper)을 설정한 랜 환경에서 시뮬레이션을 수행하였으며, 데이터셋에 대한 설명은 없다. [19]에서는 VMware를 사용하여 시뮬레이션 실험을 하였다. 각 컴퓨터에서 P2P 응용 프로그램 (BitTorrent, Foxy, GoGoBox 및 eDunkey)이 실행되었으며 일부 컴퓨터를 의도적으로 봇넷 바이러스 (Trojan.Peacomm, W32.Waledac 및 W32.Pulleuz)로 감염시켰는데, 자세한 설명은 없다.

Table 3.은 앞에서 소개한 기존의 P2P 봇넷 탐지를 위한 데이터셋의 구성을 정리한 것이다.

Table 3. Data Sets in the P2P Detection Schemes

refer.	normal traffic	P2P botnet	phase	remark
[23]	P2P(eMule, uTorrent)	Storm, Waledac	conn, C&C	
[31]	Ericsson, LBNL	Storm, Waledac	C&C, attack	*
[22]	captured normal traffic	Storm, Nugache	C&C	*
[28]	captured/standard traffic	not specified	C&C	*
[27]	captured normal traffic	Nugache	C&C	*,**
[21]	ISOT, ISCX	Storm, Waledac	attack	*
[3]	UNIBS, Ericsson, DKU	Waledac, Conflicker,Storm Bredolab, Kelihos, Zeus	C&C, attack	*
[24]	Bittorrent, Emule, Kazaa	Storm, Nugache, Slapper	conn,C&C, attack	
[41]	non P2P, P2P***	Storm, Waledac, Zeus	C&C	*

*: 10-fold cross validation
**: SMOTE(Synthetic Minority Oversampling TEchniques)
***: skype, eMule, Torrent, Frostwire, Vuze

기존 연구가 갖는 제한점의 분석을 기반으로 다음과 같은 개선안을 고려한 데이터셋의 구성을 제안한다.

1) 각 연구에서 개별적으로 캡쳐하여 구성한 데이터셋의 검증을 수행한다.
2) 새로운 연구에서 사용할 수 있는 공인된 표준 P2P 봇넷 데이터셋을 충분히 확보한다.
3) 데이터셋에 포함된 봇넷 트래픽 데이터는 Storm, Nugache, Waledac가 주를 이루며, 데이터셋을 구성하는 봇넷의 유형과 트래픽 양이 부족하므로 이를 확충한다.
4) 서로 다른 P2P 봇넷이 생애주기의 각 단계에서 생성하는 트래픽의 분석을 수행한다.
5) 동일한 P2P 봇넷이 서로 다른 환경에서 생애주기의 각 단계에서 생성되는 트래픽이 동일한 특성을 가지는 가에 대한 분석을 수행한다.

4. Performance Measures and Evaluation

다음은 봇넷의 탐지 또는 분류의 성능을 표시하는 성능 지표들인데, 많은 연구에서는 이중에서 정확도와 TP율을 선호한다.

1) 정확도(accuracy) = (TP+TN)/(TP+TN+FP+FN)
2) TP율(recall=탐지율=sensitivity) = TP/(TP+FN)
3) F-지수 = (2 × precision × recall)(precision+recall)
4) FP율 = FP/(TN + FP)

5) precision =TP/(TP + FP)

6) ROC(Receiver Operating Characteristics) 커브: 탐지율과 FP율 관계를 표시

7) AUV(Area Ubder Curve); ROC 커브의 하단 면적

TP: True Positive, TN: True Negative,

FP: False Positive, FN: False Negative

위의 지표를 적용하는 단위에 따라, 성능 지표를 플로우의 수에 대해 표현한 플로우 성능과 바이트의 수로 표현한 바이트 성능으로 나눌 수 있다. 최근의 P2P 봇넷 탐지 연구들은 높은 바이트 탐지의 정확도 보다는 높은 플로우 탐지 정확도에 더 초점을 두고 있다.

[3]에서는 일반 트래픽, 정상 P2P 트래픽, P2P 봇넷 트래픽을 분류하는 성능의 분석을 위해 정확도와 F-지수를 사용하여 2단계 탐지 시스템(2단계 모두 REPTree 사용)에 대한 플로우 성능과 바이트 성능을 함께 제시하였다. P2P 봇넷 트래픽에 대한 플로우 정확도는 97.7%, 바이트 정확도는 90.1%를 보였으며, F-지수는 플로우와 바이트에 대해 각각 99%와 85%를 보였다.

[31]에서는 TP율과 FP율을 사용하여 일반 트래픽에서 봇넷 트래픽을 분류하여 탐지하는 성능을 보였다. 우수한 결과를 보인 REPTree 기법은 봇넷 트래픽 탐지에 대해 98.3%의 TP율, 0.01%의 FP율을 보였다. 탐지 시간을 줄이기 위해 4개의 핵심 특징을 사용한 결과는 봇넷 트래픽 탐지에 대해 TP율 98.1%, FP율 2.1%를 보였다.

[22]에서는 일반 트래픽에서 P2P 봇넷 트래픽의 탐지하기 위해 F-지수, 정확도, precision을 성능 지표로 사용하였다. F-지수는 91.8%, 정확도는 100%(Storm 탐지)와 87%(Nugache 탐지), precision은 98.1%를 보였다.

[28]에서는 정상 패킷에서 P2P 봇넷 패킷을 탐지한 결과를 정확도, TP율, Precision, F-지수의 성능 지표로 표시하였다. 제시된 3 알고리듬들(RFt, KNN, MLP) 중에서 MLP가 정확도=91.1%, TP율=0.906로 가장 우수하였다. 하지만, Precision=0.915, F-지수=0.906으로 다른 기법보다 열등한 결과를 보여 다양한 성능 지표들이 일괄적인 결과를 제시하지 못하였으나 이에 대한 설명은 없었다.

[27]은 P2P 봇넷의 C&C 트래픽 분류에 대해 정확도, TP율, FP율, precision, ROC 커브, 소요시간을 사용하여 검증하였다. 정확도(0.997), TP율(0.997), FP율(0.004) 및 precision (0.997)의 모든 성능 지표에서 bayesian network 기법이 가장 좋은 성능을 보였다. 특히, 데이터셋의 class imbalance problem으로 인한 영향을 고려하여 기계학습 알고리즘을 올바르게 평가하기 위한 ROC 커브도 제시하였는데, bayesian network 기법이 평균 AUC 값이 1로 가장 우수하였다. 이 연구에서는 다양한 성능 지표가 일관성 있는 검증 결과를 제시하였다.

[18]에서는 정상 트래픽에서 HTTP 기반 봇넷의 탐지를 위해 naive bayes와 C4.5 알고리즘을 구현하여 봇넷을 탐지하고, 성능 지표로는 정확도, FP율, TP 율, 분류, 해결의 복잡도, 소요 시간을 제시하였다. naive bayes는 C4.5에 비해 봇넷 탐지의 정확도와 TP율은 많이 떨어지고 FP rate는 우수한데, 정상 트래픽을 탐지하는 TP율와 FP율은 우수한 것으로 분석되었다.

[21]에서는 정상 트래픽과 봇넷 악성 트래픽의 분류를 위해 정확도와 TP율, FP율 등의 성능 지표와 특징 선택 시간 및 뉴럴 네트워크 훈련 시간으로 성능 결과를 제시하였다. 3가지의 특징 수를 감소하는 방법들 중에서 CART가 ReliefF나 PCA보다 모든 지표에서 우수한 결과를 보였는데, 정확도와 TP율은 서로 일관적인 성능의 결과를 제시하지 못하였다. 제안 기법은 99.2%의 정확도, 99.08%의 TP율, 98.32%의 precision, 98.69%의 F-지수, 0.75%의 FP율을 보였다.

[25]에서는 시뮬레이트한 4대의 좀비 호스트의 트래픽을 이용해 오프라인 탐지한 후에 온라인 모니터링을 통해 탐지하였는데, 두 간계를 통해 좀비 호스트 4대를 모두 탐지하였다. 검증 환경이 매우 작으므로 별도의 성능 지표는 사용하지 않았다.

[23]에서는 P2P 봇넷 탐지는 bayesian network이 가장 좋은 성능을 보였고, 정상 P2P 탐지는 J48DT가 더 좋은 성능을 보였다.

[19]에서는 데이터 마이닝 기법 NB 및 NN를 비교 평가한 결과 NN의 정확도가 98.71%로 NB의 정확도 95.78%보다 높았다. [41]에서 제안한 P2P 호스트 탐지와 개별 P2P 분류의 2단계 기법에서는 3가지 P2P 봇넷 Storm, Zeus, Waledac에 대해 개별적 탐지를 하여 각각 다른 TP율, FP율, AUC를 제시하였다. Storm은 TP율:100%, FP율:0%, AUC:1.0 으로 완벽한 탐지를 하지만, Zeus와 Waledac은 이에 미치지 못한다.

[36]에서는 클러스터링 기법을 써서 HTTP와 IRC 및 P2P 봇넷을 탐지하였는데 TP율 및 TP율의 두 가지 지표로 제안 시스템의 성능을 평가하였다. testbed network에서 실험해서 P2P 봇넷(Immonia)을 탐지하는 TP율은 91%이고, TP율은 3.7%이다.

Table 4.는 각 탐지 기법의 특성을 성능 결과와 함께 나타낸 표로 각 연구에서 제시한 가장 우수한 봇넷 탐지 기법과 그의 성능을 표시하였는데, 특정한 탐지 기법이 모든 경우에서 최상의 성능을 제공하지는 않는다. 또한, 각 연구에서는 해당 환경에 최적인 탐지 기법을 제시하였으므로, 탐지에 적용된 특징, 탐지 대상과 데이터셋 구성을 고려하지 않고 서로 다른 탐지 기법의 성능 수치를 직접 비교하는 것은 의미가 적다.

특정 탐지 기법에 대해 동일한 데이터셋을 사용하여 다양한 성능 지표의 결과를 구해보면 어떤 성능 지표는 우수한 결과를 보이고 또 어떤 성능 지표는 열등한 결과를 보이는 경우가 있지만, 성능 지표들의 이러한 일관성 없는 결과에 대한 분석 연구는 없었다. 실제 대부분의 연구에서는 비교적 일관성 있는 결과를 보이는 정확도, TP율, FP율이 성능 지표로 많이 사용되고 있다. 성능 지표에 대한 더 많은 분석 연구가 필요하며, 다음과 같은 기존 연구의 제한점과 향후 연구를 위한 개선안을 제안한

다.

1) 선정된 특징, 사용된 데이터셋의 구성과 탐지/분류의 대상을 고려해야만, 여러 기법들에 대한 성능 비교의 의미가 있다.
2) 동일한 기법에 대해 여러 성능 지표들이 일관성 있는 결과를 보이지 않는 경우에 대한 원인 분석이 필요하다.
3) 서로 다른 기법이 서로 다른 환경에서 더 우수한 탐지 성능을 보이는 근거에 대한 분석이 요구된다.

Table 4. Performance of P2P Botnet Detection Schemes

refer	methods	detection category	P2P botnet	performance	remark
[3]	REPTree	normal, P2P, P2P botnet	*	a:97.7% F:99%	flow/byte results
[31]	REPTree	P2P, P2P botnet	Storm, Waledac	TP:98.3% FP:0.01%	reduce features
[22]	graph-based	normal, P2P botnet	Storm, Nugache	F:91.8% p:98.1%	Td=1hour
[28]	MLP	normal, P2P botnet	not specified	a:91.1% TP:90.6% F:90.6% p:91.5%	inconsistent results
[27]	bayesian network	normal, P2P botnet	Nugache	a:99.7% TP:99.7% FP:0.4% p:99.7% AUC:1.0	consistent for SMOTE
[21]	Neural network	normal, P2P, P2P botnet	Waledac, Strom	a:99.2% TP:99.08% FP:0.75% F:98.67% p:98.32%	inconsistent results
[41]	traffic profiling	non P2P, P2P. P2P botnet	Storm, Waledac, Zeus	TP: 94.5~100% FP: 0%~0.99% AUC: 0.976~1.0	detection for each botnet
[23]	bayesian network	P2P(eMule, eTTorent). P2P botnet	Storm, Waledac	TP:98.8% FP:0.9%	different result for normal/ botnet
[29]	J48	internet, game, P2P, P2P botnet	Peacomm	a:98%	only in LAN
[30]	IBk	non P2P, P2P, P2P botnet	not specified	TP:99.9% FP:0.01%	long training time
[19]	neural network	P2P botnet,	Peacomm, Waledac, Pilleuz	a:98.71%	only in LAN
[36]	BotOnus with clustering	HTTP bot, IRC botnet, P2P botnet	Immonia	TP:91% FP:3.7%	only in testbed network

a: accuracy, F: F-measure, p: precision
*: Waledac, Conflicker, Storm, Bredolab, Kelihos, Zeus

IV. Conclusions

중앙집중적 구조의 봇넷보다 위협은 커지고 탐지는 더욱 어려워진 P2P 봇넷이 등장한 이후, 탐지 기법과 생애 주기의 탐지 단계에 기반한 많은 P2P 봇넷 탐지 기법들이 제안되었다. 하지만, 탐지 대상, 데이터셋의 구성, 선정된 특징을 고려하지 않고 탐지 기술이나 성능 지표의 수치만으로 탐지 기법들을 단순 비교하는 것은 의미가 적다. 즉, 탐지 기법의 개선과 개발을 위해서는 기존 탐지 기법들의 비교 분석 및 연구가 필요하다. 본 연구는 P2P 봇넷의 새로운 특징이나 개선된 탐지 기법을 제안하는 대신, P2P 봇넷 탐지 기법들을 여러 관점에서 비교 분석하여 P2P 봇넷 탐지에 대한 향후 연구의 방향을 제시한 첫 시도이다.

본 연구에서는 기존의 연구들을 단순한 나열적 설명이 아닌 생애주기, 탐지 기술, 데이터셋 및 성능 지표의 4 가지 측면에서 비교 분석하여 다음과 같이 P2P 봇넷 탐지 시스템 개발에서 고려해야 할 제한점을 제시하고 향후 개선을 위한 연구 방향을 제안하였다.

1) 기존 연구에서 제시한 다양한 생애주기 모델의 단계별 공통적 특성을 분석하여 봇의 감염 단계, 봇넷 합류 단계, C&C 및 유지 단계, 공격 단계로 구성되는 4 단계의 생애주기를 제안하였다. 선형적 순서 특성을 기반으로 생애주기의 전 과정이 아닌 가장 취약한 단계에서 발생하는 트래픽 또는 호스트의 특성을 활용하는 탐지 기법을 제시하였다.
2) 여러 봇넷 탐지 기법들을 5 유형으로 분류하고, 그 중에서 데이터마이닝 기반의 기법들을 탐지 기술, 선정된 트래픽 특징, 탐지 단계, 탐지 대상을 기준으로 비교하였다. 데이터마이닝 기반과 제안된 생애주기의 각 단계별로 적용할 수 있는 비정상 기반이 효율적으로 결합된 하이브리드 기반의 탐지 시스템에 관한 연구를 제안하였다.
3) 기존 연구에서 사용된 데이터셋의 구성과 성능 지표의 문제점을 분석하고 제한점과 개선점을 제안하였다.

또한, [36]과 [42]에서 제시된 바와 같이, P2P 봇넷의 탐지 기법들에 대해 알려지지 않은 P2P 봇넷의 탐지, 온라인 탐지, 생애 주기의 초기 단계에서 탐지와 같은 구체적인 기능에 대한 가능성과 확장성(scalability), 신뢰성(reliability)과 같은 다양한 측면에 대한 분석도 필요하다.

REFERENCES

[1] W. Ye and K. Cho, “Hybrid P2P Traffic Classification with heuristic rules and machine Learning,” Soft Computing, Vol. 19, No. 9, pp. 1815-1827, Sept. 2014.
[2] M. Feeil and A. Shahrestani, “A survey of Botnet and Botnet Detection,” Procs. of the Third International

Conference on Emerging Security Information, systems and Technologies, pp. 268-273, Athens Greece, Jun. 2009.

[3] W. Ye and K. Cho,"P2P and P2P Botnet Traffic Classification in Two Stages," Soft Computing, Vol. 21, No. 5, pp.1315-1326, Mar. 2017.

[4] N. Kheir, X. Han and C. Wolley, "Behavioral fine-grained detection and classification of P2P bots," Journal of Computer Virology and Hacking Techniques, Vol. 11, No. 4, pp. 217-233, Nov. 2015.

[5] M. Mahmoud, et al.,"A Survey on Botnet Architectures, Detection and Defences," International Journal of Network Security, Vol. 17, No.3, pp. 272-289, May 2015.

[6] S. Silva, et al., "Botnets: A survey," Computer Networks, the International Journal of Computer & Telecommunications Networking, Vol. 57 No. 2, pp.378-403, Feb. 2013.

[7] M. Soysal and E. G. Schmidt, "Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison," Performance Evaluation Vol.67. No.6, pp. 451-467, Jun. 2010.

[8] I. Ghafi, J. Svoboda and V. Přenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security, Vol.5, No,2, pp. 75-80, Apr. 2015.

[9] A. Obeidat and M. Bawaneh, "Survey of the P2P botnet detection methods," International Journal of Emerging Trends of Technology in Computer Science, Vol.5, No.2, pp. 12-23, Apr. 2016.

[10] S. Ghalebandi, R. Noor and A. Lashkari, "A Survey on P2P Botnets Detection," Procs. of International Conference on Communication and Broadband Networking (ICCBN 2011), Kuala Lumlur, Malaysia, Jun. 2011.

[11] M. Elhalabi, et al., "A Review of Peer-to-Peer Botnet Detection Techniques", Journal of Computer Science, Vol. 10, No.1, pp. 169-177, Nov. 2013.

[12] P. Vadivu and K. Karthika, "A Survey on Botnet Dectection Approaches In Peer-To-Peer Network." International Journal of Advances in Computer Science and Technology, Vol 3, No.5, pp. 311-317, May 2014.

[13] P. Wang, B. Aslam and C. Zou, "Peer-to-Peer Botnets," Handbook of Information and Communication Security, pp. 335-350, 2009.

[14] Priyanka and M. Dave, "A review of recent Peer-to-Peer botnet detection techniques," Procs. of International Conference on Electronics and Communication Systems. IEEE, pp. 1312-1317, Coimbatore, India, Feb. 2015

[15] R. Rodriguez-Gomes, G. Macia-Fernandez and P. Garcia-Tedoro, "Analysis of Botnets through Life-Cycle," Procs. of SECRYPT 2011 International Conference on Security and Cryptography, pp. 257-262, Seville, Spain, Jul. 2011.

[16] N. Hachenm, et al., "Botnets: Lifecycle and Taxonomy," Procs. of 2011 Conference on Network and Information Systems Security (SAR-SSI), pp. 1-8, May. 2011.

[17] J.B. Grizzard, et al., "Peer-to-peer botnets: overview and case study," Procs. of USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07), pp. 1-8, Cambridge, USA, Apr. 2007.

[18] J. Leonard, X. Shouhuai and S. Ravi, "A Framework for understanding botnets," Procs. of the international conference on availability, reliability and security, pp. 917-922, Fukuoka, Japan, Mar. 2009.

[19] W. Tarng, C-K. Chou and K-L. Ou, "A P2P Botnet Virus Detection System Based on Data-Mining Algorithms," International Journal of Computer Science & Information Technology, vol. 4, No. 5, pp. 51-65, Oct. 2012.

[20] H. Li, et al., "Modeling to Understand P2P Botnets," Procs. of International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp.75-78, Harbin City, China, Dec. 2012.

[21] M. Alauthaman, "A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks," Neural Computer and Applications(First Online), Oct. 2016.

[22] H. Hang and X. Wei, "Entelecheia: Detecting p2p botnets in their waiting stage," Procs. of IFIP Networking Conference, pp. 1-9, Brooklyn, USA, May 2013.

[23] P. Narang, et al., "Peershark: Detecting Peer-to-Peer Botnets by Tracking Conversions," IEEE Security and Privacy workshop, pp.108-115, SanJose, USA, May 2014.

[24] Y Li, Y H, and Z Liang, "A P2P-Bonet Detection Model and Algorithms Based on Network Streams Analysis", International Conference on Future Information Technology and Management Engineering, Vol.1, pp. 55-58, Changzhou, China, Oct. 2010.

[25] Y. Fan and N. Xu, "A P2P Botnet Detection Method Used On-line Monitoring and Off-line Detection," Int. Journal of Security and Its Applications, Vol.8, No. 3, pp.87-96, May 2014.

[26] C. Sheng, H. Liang and L. Bo, "The P2P Botnet Online Detect Approach Research," Acta Electronica Sinica, Vol.39, No.4, pp. 906-912, Apr. 2011.

[27] P. Barthakur, M. Dahal and M. GHose, "An Efficient Machine Learning Based Classification Scheme for Detecting Distributed Command & Control Traffic of P2P Botnets", International Journal of Modern Education and Computer Science, Vol. 5, No. 10, PP. 9-18, Oct.

2013.
[28] P. Bharathula and N. Menon, “Equitable Machine Learning Algorithms to Probe Over P2P Botnets,” Procs. of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications(FICTA), pp.13-21, Durgapur, India, Nov. 2015.
[29] L H Liao and C. Chang, “Peer to Peer Botnet Detection Using Data Mining Scheme,” Procs. of International Conference on Internet Technology and Applications. IEEE, pp. 1-4, Wuhan, China, Aug. 2010.
[30] S. Garg, et al., “Behaviour analysis of machine learning algorithms for detecting P2P botnets,” Procs. of IEEE 15th International Conference on Advanced Computing Technologies (ICACT): pp. 1-4, Rajampet, India, Sep. 2013.
[31] D. Zhao, et al., “Peer to Peer Botnet Detection Based on Flow Intervals,” Information Security and Privacy Research-27th IFIP TC 11 Information Security and Privacy Conference, pp.87-102, Jun. 2012.
[32] P. Wang, et al., "A Systematic Study on Peer-to-Peer Botnets, " International Conference on Computer Communications and Networks, IEEE ICCCN 2009, pp.1-8, August 2009,
[33] H. Jiang and X. Shao, “Detecting P2P botnets by discovering flow dependency in C&C traffic.” Peer-to-Peer Networking and Applications, pp.320-331, Dec. 2014.
[34] W. Ye and K. Cho, “P2P Traffic classification using Advanced heuristic Rules and Analysis of Decision Tree Algorithms,” Journal of the Korea Society of Computer and Information, Vol. 19, No. 3, pp.45-54, Mar. 2014.
[35] G. Gu, et al.,“BotMiner:clustering analysis of network traffic for protocol and structure independent botnet detection,” SS’08 Procs of the 17th conference on Security Symposium, pp. 139-154, San Jose, USA, Aug. 2008.
[36] M. Yahyazadeh and M. Abadi, "BotOnus: An online unsupervised method for botnet detection," The ISC Int'l Journal of Information Security, Vol.4, No.1, pp. 51-62, Mar. 2012.
[37] J. Kang and J Y Zhang, “Application Entropy Theory to Detect New Peer-to-Peer Botnet with Multi-chart CUSUM,” Procs. of 2009 Second International Symposium on Electronic Commerce and Security, pp.471-475, Nanchang City, China, May 2009.
[38] B. Wang, Z. Li, H. Tu and J. Ma, “Measuring Peer-to-Peer botnets using control flow stability,” Procs. of IEEE International Conference on Availability, Reliability and Security ARES'09, pp. 663-669. Fukuoka, Japan, Mar. 2009.
[39] S. K. Noh, et al.,“Detecting P2P Botnets Using a Multi-phased Flow Model,” Procs. of Third International Conference on Digital Society. IEEE Computer Society, pp. 247-253, Cancun, Mexico, Feb. 2009.
[40] Y. Zeng and K. G. Shin, “On detection of storm botnets. Real-Time Computing Laboratory,” Technical report CSE-TR-560-09, The University of Michigan, pp. 1-7, Dec. 2009.
[41] B. Rahbarinia, R. Perdisci, A. Lanzi and K. Li, “PeerRush: Mining for unwanted p2p traffic,” DIMVA 2013-Detection of Intrusions and Malware, and Vulnerability Assessment. Lecture Notes in Computer Science, Vol. 7967. pp. 62-82, JUL. 2013.
[42] S. Garg, S. K. Peddoju and A. K. Sarje, "Scalable P2P bot detection system based on network data stream," Peer-to-Peer Networking and Applications, Vol.9, No6, pp. 1162-1176, Nov. 2016.
[43] E-S. Hong and M-K. Park, “Severity-based Software Quality Prediction using Class Imbalanced Data,” Journal of the Korea Society of Computer and Information, Vol. 21, N0. 4, pp.73-80, Apr. 2016.

Authors

Kyungsan Cho received his B.Sc. in Electronic Engineering(Seoul National University, 1979), master degree in Electrical and Electronic Engineering (KAIST, 1981), and his Ph.D. Degree in Electrical and Computer Engineering(the University of Texas at Austin, 1988) After served as a senior R&D Engineer at Samsung Electronics Company, Dr. Cho joined Dankook University in March, 1990, where he is currently a professor in the department of Software Science. He authored several books in Computer Architecture and Computer Networks, and published over 40 academic papers. His research interests include mobile networks, network security and traffic analysis.

Wu Jian, Ye received the B.S degree in Computer Science and Technology from GuangDong University of Technology in 2010; then received M.S. and Ph.D. degrees in Computer Science from Dankook University in 2012 and 2015 respectively. Dr. Ye joined the faculty of School of Information Engineering at GuangDong University of Technology, GuangZhou, China, in 2015. He is currently a Lecturer in the School of Information Engineering, He is interested in Internet traffic analysis, network security, machine learning and deep learning.