The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 1, pp.61-68, Feb. 28, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.1.61
JIIBC 2015-1-8

스마트폰에서 효율적인 봇 탐지 기법

An Efficient Bot Detection Mechanism in Smartphones

최우진*, 박지연**, 정진만***, 허준영****, 전광일*****

Ujin Choe*, Jiyeon Park, Jinman Jung***, Junyoung Heo****, Gwangil Jeon*****

요 약 최근 스마트폰의 급속한 확대로 다양한 형태의 보안 위협이 증가하고 있다. 그 중 감염된 스마트폰은 개인정보 유출뿐만 아니라 사이버 테러와 같은 DDOS 공격에도 악용될 수 있어 매우 위험하다. 하지만 기존 기법들은 배터리를 사용하는 스마트폰에서는 적합하지 않거나 별도의 저장소를 필요로 하는 문제점이 있다. 본 논문에서는 스마트폰에서 효율적인 봇 탐지 기법을 제안한다. 제안 기법은 수신 트래픽을 대상으로 탐지하는 기존 기법과 다르게 제안 기법은 송신 트래픽만을 대상으로 탐지하므로 수신 트래픽보다 송신 트래픽이 적은 스마트폰에서 더욱 에너지 효율적이다. 또한 의도하지 않은 트래픽을 유발하는 로그 정보들을 외부 통합 서버에 수집하여 봇뿐만 아니라 봇넷을 탐지할 수 있다. 제안 기법을 안드로이드 스마트폰에서 구현하고 성능 평가를 한 결과 효과적으로 봇을 탐지할 수 있음을 확인하였다.

Abstract Recently, with increasing use of smartphones, the security threats also have increased rapidly. Especially, the compromised smartphone is very dangerous because it could be exploited in a DDOS attacks such as cyberterrorism as well as in the leakage of personal information. However, most bot detection mechanisms are still unsuitable for smartphone with its lower computing capability and limited battery capacity because they incur additional computational overheads or require pre-defined signatures. In this paper, we present an efficient bot detection mechanism in smartphones. Our mechanism detects effectively bots in outgoing traffic by using a correlation between user events and network traffic. We have implemented its prototype in Android smartphone and measured its performance. The evaluation results show that our mechanism provides low overhead to detect bots in smartphones.

Key Words : Security, Smartphone, Android, Bot Detection, Botnet Detection

I. 서 론

최근 스마트폰의 보급 확대로 인하여 악성 코드에 감염되는 사례가 증가하고 있다. 악성앱이나 악성웹페이지를 다운로드받아 감염되는 전통적인 방식뿐만 아니라 블루투스[1], SMS[2], QR 코드[3] 등의 다양한 경로로부터 스마트폰은 악성코드의 보안 위협에 노출되어 있다. 감염되는 경우 스마트폰 성능 저하, 개인정보 파괴/유출 및

*준회원, 한국산업기술대학교 컴퓨터공학부
**정회원, LG전자 SW엔지니어
***정회원, 한남대학교 정보통신공학과(교신저자)
****정회원, 한성대학교 컴퓨터공학과
*****정회원, 한국산업기술대학교 컴퓨터공학부
접수일 : 2015년 1월 17일, 수정완료 : 2015년 2월 4일
게재확정일자 : 2015년 2월 13일

Received: 17 January, 2015 / Revised: 4 February, 2015
Accepted: 13 February, 2015
***Corresponding Author: jmjung@hnu.kr
Department of Information and communication engineering, Hannam University, Korea

과금 발생 등 심각한 문제를 일으킬 수 있다. 특히 감염된 스마트폰이 공격자의 명령에 제어되는 경우에는 DDOS 공격에 악용될 수 있다. 일반적으로 봇마스터(botmaster)는 메시징 서비스와 같은 특별한 프로토콜을 통해 감염된 스마트폰에 명령을 전달하고 제어한다. 이때 명령 및 제어 (Command and Control; C&C) 메시지를 전달하는 봇마스터와 조종되는 봇(bot)들로 연결된 네트워크를 봇넷(botnets)이라고 한다. 또한 특정한 절차 없이 앱을 개발하거나 등록이 가능하기 때문에 봇(Bot)[4]을 비롯하여 다양한 공격기법에 의해 스마트폰이 악성코드에 감염되는 사례가 나타나고 있다. 대부분 스마트폰 고유의 특성을 악용하여 봇넷을 구성하는데 대표적인 방법이 SMS(Short Message Service)을 이용하는 방법이다. SMSC(Short Message Service Center)에서 메시지 전달을 보장하고, 전화번호를 식별 번호로 활용하면 확장성이 높기 때문에 많이 사용된다 [5, 6]. 최근에는 SMS와 HTTP가 결합된 형태의 봇넷도 등장하였고 [7], 대부분의 스마트폰에 탑재된 블루투스도 봇넷을 구성하는데 악용될 수 있다 [8]. 하지만 PC 기반의 기존 기법들은 오버헤드가 크기때문에 배터리를 사용하는 스마트폰에서는 적합하지 않거나 많은 트래픽을 유발하는 문제점이 있다. 본 논문에서는 스마트폰에서 효율적인 봇 탐지 기법을 제안한다. 제안 기법은 사용자가 의도하지 않은 트래픽을 유발하는 로그 정보들을 외부 통합 서버에 수집하여 봇뿐만 아니라 봇넷을 탐지하는 기법이다. 제안 기법에서 트래픽의 악의성 여부는 사용자 이벤트와 트래픽의 상관관계를 이용하며 로그 정보들의 분석을 통해 봇들을 탐지 할 수 있다. 수신 트래픽을 대상으로 탐지하는 기존 기법과 다르게 제안 기법은 송신 트래픽만을 대상으로 탐지하므로 수신 트래픽보다 송신 트래픽이 적은 스마트폰에서 더욱 에너지 효율적이다.

본 논문의 구성은 다음과 같다. II장에서 기존 스마트폰 기반 DDOS 탐지 기법들을 알아보고, III장에서 스마트폰에서 효율적인 봇 탐지 기법을 제안한다. IV장에서는 제안 기법의 구현 이슈를 논의하고 실험 결과를 설명한 후 V장에서 결론을 맺는다.

II. 관련 연구

대부분의 스마트폰 기반 봇 탐지 기법은 배터리 기반의 스마트폰에서 효율적으로 동작하도록 연구되어 왔으나 그 기본 원리는 기존 PC 기반 침입 기반 탐지 기법과 유사하다.

1. 시그니처 탐지 기법

시그니처 기반 탐지 기법(Signature based Detection)은 알려진 공격 또는 봇들의 규칙 패턴들을 시그니처 저장소에 저장하고 수신 트래픽들을 비교하여 탐지하는 기법이다. 이 탐지 기법은 트래픽을 수신할 때마다 저장소의 봇 시그니처들과 비교하는 패턴 매칭 알고리즘을 수행해야 하므로 많은 오버헤드를 발생한다. [9]에서는 자원 제약적인 환경을 고려하여 기존 시그니처 기반 탐지 기법을 경량화 시킨 Lightweight IDS 기법이 연구되었다. 이 기법은 알려진 봇들의 시그니처 저장소가 필요하므로 저장 공간이 제약적인 스마트폰에서는 확장성이 떨어질 수 있다.

2. 이상 행위 기반 탐지 기법

이상 행위 기반 탐지 기법(Anomaly based Detection)은 네트워크 또는 호스트의 일반적인 상태를 정의하고 그 정의된 상태와 시스템의 상태를 비교하여 이상 행위를 탐지한다. 시그니처에 비해 변종 악성 코드에 비교적 높은 내성을 보이지만 시스템 콜을 모니터링하거나 메모리, 파일 시스템 상태를 추적하여 시스템의 동작과 비교해야 하기 때문에 기본적으로 상당한 오버헤드를 요구한다. MADAM[10]은 단말기 사용자의 특성을 분석하여 정보를 벡터로 저장 후 상태나 시스템 콜의 횟수 등이 패턴과 다른 경우 악성앱으로 분류하여 탐지한다. SmartSiren[11]에서는 스마트폰 내부에 경량 에이전트를 탑재하고 스마트폰의 SMS와 블루투스 등의 로그 정보만을 외부 서버에 주기적으로 전송하여 배터리 소모량을 줄이는 방법을 사용하였다. 이 기법은 외부 서버에 수집된 로그들의 통계적 분석을 통해 악성코드를 탐지한다. Paranoid Android[12]에서도 단말기의 실행 중 발생되는 정보들을 분산된 다른 노드들에게 전송하고 협업하여 악성코드를 탐지한다. 하지만 이 방법들은 스마트폰 내의 오버헤드는 줄일 수 있으나 주기적인 로그 전송으로 인해 큰 네트워크 트래픽을 유발시키며 새로운 프라이버시 문제를 발생시킨다. TaintDroid[13]에서도 안드로이드 기반 스마트폰에 동적 분석을 적용하여 지역 변수, 인자 등의 태그 전파 과정을 추적하여 외부 유출을 탐지하는 기법을 제안하였다. 달빅 가상머신을 이용해 실시간으로

모니터링하여 민감한 정보의 유출을 차단할 수 있지만 높은 오버헤드가 발생한다. 또한 VirusMeter[14]에서는 모바일 기기의 배터리 소모량을 실시간으로 모니터링하여 임계치 이상의 배터리 소모가 발생하는 경우 악성코드를 탐지한다. 시그니처 기반 탐지 기법과 이상 행위 기반 탐지 기법은 자원 제약적인 모바일 기기의 환경을 고려하여 최적화 하였지만 시그니처 저장소가 필요하거나 패턴 매칭 알고리즘이 필요하다. 또한 데이터를 수집하고 외부 서버에 전송하는 과정에서 모니터링 오버헤드, 트래픽 발생 및 프라이버시 문제를 유발한다. 제안 기법은 스마트폰에서 트래픽과 사용자 이벤트의 관계적인 특성을 이용하여 정상적인 트래픽 전송인지 여부를 확인하므로 이상 행위 기반 탐지 기법에 속할 수 있다. 또한 사용자 이벤트와 트래픽의 관계의 통계적 분석 내용을 바탕으로 탐지하므로 변종 악성 코드에도 강하다. 더욱이 외부 통합 서버로 전송하는 데이터는 모든 로그 정보가 아니라 의심스러운 후보 봇의 정보만 전송하므로 유발되는 트래픽의 양이 적고 프라이버시 문제도 발생시키지 않는다.

Ⅲ. 스마트폰에서 효율적인 봇 탐지 기법

1. 봇 탐지 개요

봇넷은 봇마스터와 봇으로 이루어진 그래프 G(V, E)로 표현 가능하다. 점들의 집합 V는 봇마스터와 봇으로 구성되고 이들은 식별 가능한 IP 주소로 나타낸다. 간선들의 집합 E는 봇들의 송신 IP 주소와 수신 IP 주소의 순서쌍으로 구분할 수 있다. 봇 탐지는 전체 네트워크에서 V를 찾는 것이 목표이다. 먼저 제안 기법은 봇마스터를 포함한 봇들의 집합 V를 탐지하기 위해 간선들을 수집한다. 봇들은 사용자의 의도와 무관하게 봇마스터에 의해 명령을 받고 제어되므로 사용자 이벤트와 독립적으로 발생하는 특성을 가지는 것으로 가정한다. 그러므로 스마트폰에서 발생한 송신 트래픽이 사용자 이벤트와 무관하게 발생하는 경우 의도하지 않은 트래픽으로 간주하고 이 간선들을 후보 집합 E'에 추가하고 수집된 간선 집합 E'를 통해 V'를 예측한다. 축적된 간선 집합 E'의 빈도를 가중치로 사용할 수도 있다.

2. 사용자 이벤트와 트래픽 상관 관계

제안 기법은 먼저 사용자 이벤트와 송신 트래픽의 발생 시간과 횟수에 대한 통계적인 분석을 바탕으로 임계치를 정의한다. 외부로 나가는 트래픽이 발생할 때 이벤트 발생 시간과 비교하여 봇을 탐지한다. 이 때, 봇이 보내려는 송수신 IP 주소를 외부 통합 서버에 전송하여 다른 봇과 봇마스터도 탐지할 수 있다. 봇은 사용자의 의도와 무관하게 봇마스터에 의해 명령을 받고 제어된다. 이는 감염된 스마트폰의 송수신 트래픽이 사용자 이벤트와 독립적으로 발생하는 특성을 갖는다는 것을 의미한다. 스마트폰 내의 앱들에 대한 송신 트래픽 발생 시간과 사용자 이벤트간의 상호 연관성을 살펴보기 위해 다양한 앱을 대상으로 이벤트 발생 후 경과 시간에 따른 트래픽 발생 횟수를 관찰하였다.

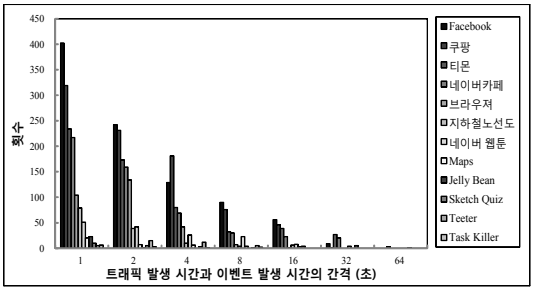

그림 1. 이벤트 후 짧은 시간 내에 트래픽을 발생시키는 앱
Fig. 1. Apps that generate outgoing traffics within a short time after being triggered by user event

그림 1은 사용자 이벤트와 트래픽 발생 시간의 관계를 알기 위해 48시간 동안 12개의 정상앱 대한 이벤트 발생 후 네트워크 트래픽 발생 시간을 관찰하였다. 이 그림에서 x축은 이벤트 발생 후 몇 초 후에 트래픽이 발생한 지를 나타내고, y축은 트래픽 발생 빈도를 나타낸다. 대부분의 정상앱은 사용자의 이벤트 발생 후 일정 시간 내에 네트워크 트래픽을 발생시키는 것을 확인하였다.

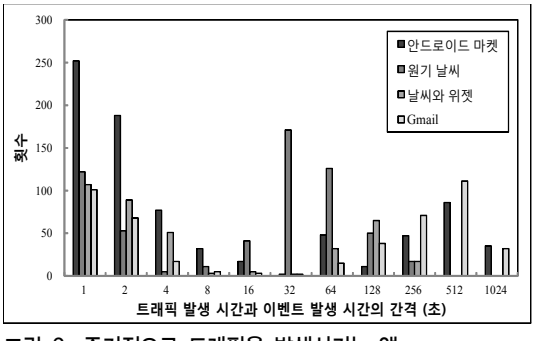

그림 2. 주기적으로 트래픽을 발생시키는 앱
Fig. 2. Apps that periodically generate network traffics

날씨 정보나 이메일과 같이 데이터를 주기적으로 서버에서 서비스 받거나 동기화하기 위한 앱들도 존재하였다. 이 경우에는 그림 2와 같이 사용자 이벤트와 무관하게 주기적으로 트래픽을 발생시키므로 봇과 같이 단순히 임계치 만으로 탐지한다면 오탐율을 증가시킬 수 있는 요인이 된다. 제안 기법에서는 화이트 리스트를 통해 이러한 종류의 앱들을 오탐하지 않도록 하였다.

마지막으로 이벤트와 무관하게 트래픽을 발생시키는 악성앱을 분석하였다. 악성앱은 백그라운드에서 동작하여 외부 서버와 통신하거나 사용자의 정보를 송신하는 등의 악성 행동을 한다. 그림 3과 같이 악성앱들은 이벤트와 무관하게 발생하거나 정상앱에 비해 이벤트 발생 후 상대적으로 긴 시간 후에 네트워크 트래픽을 발생시키는 것을 알 수 있다.

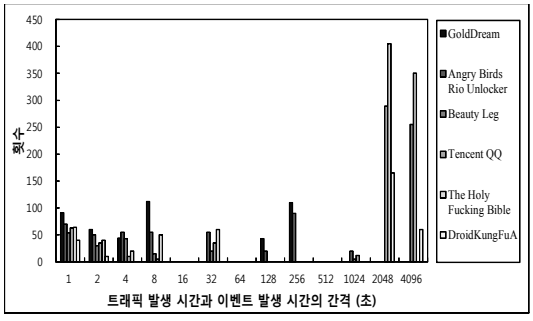

그림 3. 이벤트와 독립적으로 트래픽을 발생시키는 악성앱
Fig. 3. Apps that generate traffics regardless of events

사전 실험 결과, 송신 트래픽의 사용자 의도성 유무를 판단하는 방법으로 사용자 이벤트와 트래픽 발생 시간을 사용하는 것은 합리적이라고 할 수 있다. 제안하는 기법은 사용자 이벤트와 외부로 나가는 네트워크 트래픽의 발생 시간과 횟수에 대한 임계치를 정의하여 봇을 탐지하는 것이다. 이벤트 발생시간과 트래픽의 변화량에 대한 모니터링만을 이용하기 때문에 기존의 기법보다 오버헤드가 적고 외부 서버에 통신하는 악성앱을 효율적으로 탐지할 수 있다.

3. 효율적인 봇 탐지 기법

제안 기법은 이벤트 관리 모듈, 트래픽 감시 모듈, 봇 처리 모듈 3가지 모듈로 구성된다. 그림 4는 봇 탐지를 위한 내부 구조를 보여준다. 이벤트 관리 모듈은 사용자 이벤트 발생 시 앱 별로 이벤트 발생 정보를 이벤트 엔트리 테이블에 저장하여 관리한다. 이벤트가 발생하면 이벤트 로거는 이벤트 타입의 종류에 따라 터치, 키 이벤트로 분류하고 이벤트 발생 시간, 임계치 시간 등의 이벤트 엔트리를 생성한다. 또한 이 생성된 엔트리를 전면(foreground) 상태에 있는 앱과 일치하는 이벤트 엔트리 테이블에 저장한다. 이벤트와 트래픽이 동일한 앱에서 발생된 것인지를 구분하기 위함이다.

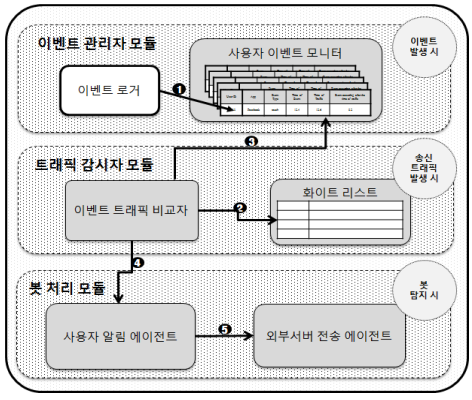

그림 4. 봇 탐지를 위한 내부 구조
Fig. 4. The structure for bot detection

트래픽 감시 모듈은 송신 트래픽 발생 시 호출된다. 먼저 화이트 리스트에서 트래픽을 발생 시킨 앱 ID의 존재 여부를 확인 후, 존재한다면 정상적인 트래픽으로 처리하고 존재하지 않는다면 이벤트 엔트리 테이블에 접근한다. 이벤트 트래픽 비교자는 이벤트 엔트리 테이블로부터 이벤트 발생 시간과 현재 트래픽 발생 시간의 차가 임계치 이내인지를 확인한다. 이벤트 발생 이후 임계치 이상의 시간이 지났으면 사용자가 의도하지 않은 트래픽을 발생한 것으로 판단한다.

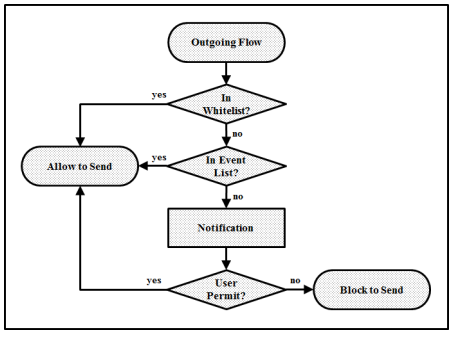

그림 5. 제안된 봇 탐지 과정
Fig. 5. The proposed bot detection procedure

봇 처리 모듈은 사용자 알림 에이전트와 외부 서버 전송 에이전트로 구성된다. 먼저 사용자 알림 에이전트는 송수신 IP 주소, 탐지 시간, 트래픽 정보 및 그 트래픽을 유발한 앱 정보를 저장하고 사용자에게 알린다. 사용자로부터 봇 유무 여부를 확인 받을 수 있도록 하고 오탐인 경우 화이트 리스트에 추가하여 향후 정확도를 높일 수 있다. 또한 외부 서버 전송 에이전트는 외부 통합 서버로 전송한다. 그림 6과 같이 통합 서버에서는 수집된 송수신 IP 주소 즉 간선들의 집합으로부터 봇들의 집합을 예측한다. 간단하게는 간선의 출현 빈도를 통해 예측할 수 있다. 제안 기법이 적용된 노드가 대규모로 참여한 네트워크에서는 수집된 로그 정보로부터 패킷당 바이트 수(bytes per packet), 초당 바이트 수(bytes per sencod) 등의 특성의 유사도를 비교하여 봇넷을 더 정교하게 탐지할 수 있다.

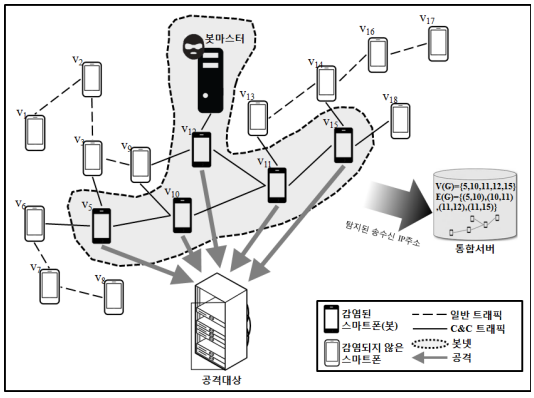

그림 6. 외부 통합 서버를 이용한 봇넷 탐지 예
Fig. 6. An Example of botnets detection using the integrated server

Ⅳ. 구현 및 실험결과

제안 기법의 프로토타입은 안드로이드 4.1버전(Jelly bean)과 리눅스 커널 3.0.31버전의 환경에서 설계되었다. 앞서 설명한 3가지 모듈은 input_allocate_device 커널 함수에서 초기화된다. 이벤트 관리 모듈은 스마트폰 사용자의 이벤트가 발생할 때마다 커널 내부의 input_handle_event 함수에서 스마트폰 상의 발생된 이벤트와 앱의 정보를 수집한다. 이 정보들은 커널 상에서 전역 변수로서 앱 별로 연결 리스트를 이용하여 관리된다. 또한, 트래픽 감시 모듈은 커널 내 TCP/IP 프로토콜 스택을 거치고 네트워크 카드로 전송되기 전인 dev_queue_xmit 함수에서 구현되었다. 패킷이 발생할 때마다 트래픽 감시 모듈이 호출되고 봇을 탐지하는 경우 탐지된 트래픽과 앱 정보들은 봇 처리 모듈에 저장되어 사용자에게 콜백되며 연결된 통합 서버로 전송한다.

본 장에서는 안드로이트 스마트폰 상에서 제안 기법의 탐지율과 효율성을 평가한다. 실험을 위해 표 1과 같이 Cortex-A9이 탑재된 갤럭시 넥서스가 사용되었다. 봇 탐지율 평가를 위해 Y.Zhou[15] 등이 조사한 49개의 안드로이드 악성 코드 중에서 트래픽을 발생시키는 27개의 악성 코드가 사용되었다. 각 탐지 기법의 효율성 평가를 위해 Quadrant벤치 마크 앱을 사용하여 CPU와 메모리 효율성을 측정하였다.

표 1. 실험 환경
Table 1. The experimental environment

Feature	Specification	
Galaxy Nexus (SHW-M402S)	CPU	TI OMAP 4460(Cortex-A9)
	RAM	1GB

표 2는 실험을 위해 단말기에 설치된 27개 악성코드의 특징과 제안된 기법의 탐지결과이다. 27개의 악성 코드 중 이벤트와 동시에 반응하는 KMin, CruseWin와 SMS 기반의 DogWars, GGTracker 악성코드를 제외한 23개의 악성코드를 탐지하였다.

표 2. 악성코드 탐지결과
Table 2. The detection result

Malware	Remote Control		Financial Charges		Personal Information Stealing			Detection
	NET	SMS	Phone Call	SMS	SMS	Phone number	User Account	
ADRD	√							O
anserverBot	√			√				O
BaseBridge	√		√	√				O
BeanBot	√		√	√		√		O
BgServ	√			√		√		O
CoinPirate	√			√				O
Crusewin	√			√	√			X
DogWars				√				X
DroidCoupon	√							O
DroidDream	√							O
DroidDreamLight	√						√	O
DroidKungFu1	√					√		O
DroidKungFu2	√					√		O
DroidKungFu3	√					√		O
DroidKungFu4	√							O
DroidKungFuUpdate	√					√		O
Endofday	√			√		√		O
Gginimi	√		√	√	√	√		O
GGTracker				√	√	√	√	X
GoldDream	√		√	√	√	√		O
JSMSHider	√			√		√		O
KMin	√			√				X
Nickyspy	√			√	√			O
Pjapps	√			√		√		O
Plankton	√							O
RogueLemon	√			√	√			O
YZHC	√			√		√		O

제안 기법의 오버헤드를 확인하기 위해 안드로이드 벤치마크 앱인 Quadrant를 사용하였고 점수가 높을수록 성능 또한 우수하다는 것을 의미한다. 그림 7은 Quadrant 앱을 20회 실행하여 기존 안드로이드 스마트폰에서 제안 기법을 적용하기 전과 후의 평균 성능을 비교한 것이다. Quadrant앱 에서 CPU의 오버헤드는 제안 기법을 적용 후 5% 증가하였다. 또한 메모리 오버헤드는 적용 전후 약 9% 성능 차이를 보였다.

제안 기법은 트래픽이 발생할 때만 봇 탐지를 위한 트래픽 감시를 하기 때문에 낮은 CPU사용률을 보인다. 또한 이벤트 엔트리 테이블을 관리를 위한 공간 비용도 크지 않았다. 이와 같은 실험 결과를 바탕으로 제안된 기법은 적은 오버헤드로 높은 탐지율을 보임을 확인하였다. 또한 제안 기법은 사용자의 이벤트 없이 발생되는 송신 트래픽을 탐지하므로 DDOS에 악용될 수 있는 봇 탐지뿐만 아니라 개인 정보 불법 유출 피해를 줄이는데 효과적이라고 할 수 있다.

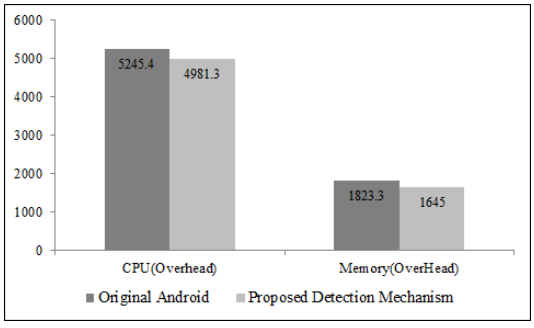

그림 7. Quadrant앱을 이용한 성능측정 결과
Fig. 7. The result of performance evaluation with Quadrant

V. 결 론

본 논문에서는 스마트폰에서 효율적인 봇 탐지 기법을 제안하였다. 제안 기법은 송신 트래픽을 대상으로 탐지하여 스마트폰에 더 효율적으로 동작하도록 설계되었다. 또한 사용자 이벤트와 트래픽의 관계의 통계적 분석 내용을 바탕으로 탐지하므로 변종 악성 코드에도 강하다. 더욱이 외부 통합 서버로 전송하는 데이터는 모든 로그 정보가 아니라 의심스러운 후보 봇들의 정보만 전송하므로 발생되는 트래픽의 양이 적고 프라이버시 문제도 유발시키지 않는다. 통합 서버에 수집된 데이터들의 통계 정보를 통해 봇뿐만 아니라 봇넷을 탐지하는데도 활용할 수 있다. 제안 기법을 안드로이드에서 구현하고 벤치마크 앱으로 실험 분석한 결과에서 기존 안드로이드에 비해 5%의 CPU 오버헤드와 9%의 메모리 오버헤드로 85.2%를 탐지율을 보였다.

References

[1] J. Baek and J. Park, "A study of analysis and improvement of security vulnerability in Bluetooth for data transfer", Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 12, No. 6, pp. 2801-2806, 2011.

[2] K. Shin, U. Park and M. Jun, "A Design of SMS DDoS Detection and Defense Method using Counting Bloom Filter", In Proceedings of the KAIS Fall Conference, Vol. 1, pp. 53-56, 2011.

[3] H. Yang, "A Study of Security Weaknesses of QR Codes and Its Countermeasures", The journal of the Institute of Internet Broadcasting and Communication (JIIBC), vol. 12, no. 1, pp. 83-89, 2012.

[4] S. Kim, D. Choi and B. An, "Detection and Prevention Method by Analyzing Malignant Code of Malignant Bot", The journal of the Institute of Internet Broadcasting and Communication (JIIBC), Vol. 13, No. 2, pp. 199-207, 2013.

[5] G. Geng, G. Xu, M. Zhang, Y. Guo, G. Yang, and C. Wei. "The design of sms based heterogeneous mobile botnet", Journal of Computers, Vol. 7, No. 1, pp. 235-243, 2012.

[6] G. Weidman. "Transparent botnet command and control for smartphones over sms", In Proceedings of Shmoocon, 2011.

[7] C. Mulliner and J. Seifert, "Rise of the ibots: Owning a telco network", In Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware), pp. 19-20, 2010.

[8] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating bluetooth as a medium for botnet command and control", Detection of Intrusions and Malware, and Vulnerability Assessment, Vol. 6201,

pp. 61-80, 2010.

[9] X. Kou and Q. Wen, “Intrusion detection model based on android”, Broadband Network and Multimedia Technology (IC-BNMT), pp. 624-628, 2011.

[10] G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, "MADAM: A Multi-level Anomaly Detector for Android Malware", In Proceedings of the 6th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS'12), pp. 240-253, 2012.

[11]J. Cheng, S.H.Y. Wong, H. Yang, and S. Lu, "SmartSiren: virus detection and alert for smartphones", In Proceedings of the 5th international conference on Mobile systems, applications and services (MobiSys'07), pp. 258-271, 2007.

[12]G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: versatile protection for smartphones", In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC'10), pp. 347-356, 2010.

[13]W. Enck, P. Gilbert, B. Chun, L. Cox, J. Jung, P. McDaniel and A. Sheth, "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones", In Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation, pp. 1-6, 2010.

[14]L. Liu, G. Yan, X. Zhang, and S. Chen, "VirusMeter: Preventing Your Cellphone from Spies", In Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID'09), pp. 244-264, 2009.

[15]Y. Zhou and X.Jiang, "Dissecting Android Malware: Characterization and Evolution", In Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP'12), pp. 95-109, 2012.

저자 소개

최 우 진(준회원)

- 2009년 : 한국산업기술대학교 컴퓨터공학과 졸업(학사)
- 2012년 : 한국산업기술대학교 컴퓨터공학과 졸업(석사)
- 2012 ~ 현재 : 한국산업기술대학교 컴퓨터공학부 박사과정

<관심 분야 : 시스템 소프트웨어, 임베디드 시스템, 시스템 보안>

박 지 연(정회원)

- 2010년 : 성신여자대학교 컴퓨터공학부 졸업(학사)
- 2013년 : 서울대학교 컴퓨터공학부 졸업(석사)
- 2013년 ~ 현재 : LG전자 SW엔지니어

<관심 분야 : 운영체제, 임베디드 시스템, 시스템 보안>

정 진 만(정회원)

- 2008년 : 서울대학교 컴퓨터공학과 졸업(학사)
- 2014년 : 서울대학교 전기컴퓨터공학과 졸업(박사)
- 2014년 ~ 현재 : 한남대학교 정보통신공학과 조교수

<관심 분야 : 운영체제, 임베디드 시스템, 시스템 보안>

허 준 영(정회원)

- 1998년 : 서울대학교 컴퓨터공학과 졸업(학사)
- 2009년 : 서울대학교 컴퓨터공학과 졸업(박사)
- 2009년 ~ 현재 : 한성대학교 컴퓨터공학과 조교수

<관심 분야 : 운영체제, 무선 센서 네트워크, 임베디드 시스템, 결함허용 시스템>

※ 이 논문은 2014년도 한남대학교 학술연구 조성비 지원에 의하여 연구되었음

전 광 일(정회원)

- 1986년 : 서강대학교 컴퓨터공학과 졸업(학사)
- 1988년 : 서울대학교 컴퓨터공학과 졸업(석사)
- 2002년 : 서울대학교 컴퓨터공학과 졸업(박사)
- 1988 ~ 1994년 : 한국전자통신연구원 선임연구원
- 2001년 ~ 2003년 : 유비쿼스(주) 연구소장
- 2003년 ~ 현재 : 한국산업기술대학교 컴퓨터공학부 교수

<관심 분야 : 운영체제, 임베디드 시스템, 고신뢰컴퓨팅시스템>