Journal of Computer Science 10 (1): 169-177, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.169.177 Published Online 10 (1) 2014 (http://www.thescipub.com/jcs.toc)

A REVIEW OF PEER-TO-PEER BOTNET DETECTION TECHNIQUES

Mohammed Jamil Elhalabi, Selvakumar Manickam, Loai Bani Melhim, Mohammed Anbar and Huda Alhalabi

National Advanced IPv6 Center of Excellence (NAv6), Universiti Sains Malaysia, Malaysia

Received 2013-04-22; Revised 2013-09-13; Accepted 2013-11-13

ABSTRACT

In recent years, Peer-to-Peer technology has an extensive use. Botnets have exploited this technology efficiently and introduced the P2P botnet, which uses P2P network for remote control of its bots and become one of the most significant threats to computer networks. They are used to make DDOS attacks, generate spam, click fraud and steal sensitive information. Compared with traditional botnets, P2P botnets are harder to be defended and hijacked. In this study we discuss various P2P botnet detection approaches and evaluate their effectiveness. We identify the advantages and shortcomings of each of the discussed techniques. This can guide the researchers to a better understanding of P2P botnets and easier for them developing more sufficient detection techniques. Our evaluation shows that each technique has its own advantages and limitations. Two or more detection techniques might be used together, in order to have a robust P2P botent detection.

Keywords: Peer to Peer, Botnet, P2P Botnet

1. INTRODUCTION

Botnet is a network of infected computers (bots) running malicious software, usually installed by different attacking techniques such as worms, Trojan horses and viruses. Each bot is remotely controlled by an attacker (botmaster). They responds to the botmaster orders and initiate several malicious activities, such as email spam, key loggin, password cracking and Distributed Denial of Service (DDOS) attack.

Botnet is a network of compromised computers connected to the Internet, which were commanded and controlled by the botmaster. Botent in general, are formed in a centralized architecture and has a central point of failure which is the C&C server. That is, if the C&C server is tracked, the entire botent will be easily detected and shut down.

To avoid the weakness of centralized architecture, botnet imitate Peer to Peer (P2P) networks architecture and design a botnet of a P2P control mechanism, in order to increase its stability. In P2P networks there is no centralized node for command and control. Each node acts as a client and a server, even if a node is taken offline by the defenders, the botnet will remain under other nodes control (Ping *et al*., 2010). Compared with traditional botnets, P2P botnets are harder to be hijacked and defended. **Figure 1** shows how P2P botent works.

1.1. P2P Botnet Operation

1.1.1. P2P Botnet Analysis

Botnet lifecycle has four phases: Formation, C&C, attack and post attack (Leonard *et al*., 2009). In the first phase, formation; the botmaster infects other computers on the Internet to form a botnet. One way of forming P2P botnets is using the indexes of P2P file sharing system to connect to each other, this enables nodes to know IP addresses and port numbers of other nodes. A new bot receives an index from the spreading nodes, then it will try to contact to bots whose IP address included in the index. Building a P2P botnet is called bootstrap and botnets built by this method are called index-based botnet.

Corresponding Author: Mohammed Jamil Elhalabi, National Advanced IPv6 Center of Excellence (NAv6), Universiti Sains Malaysia, Malaysia

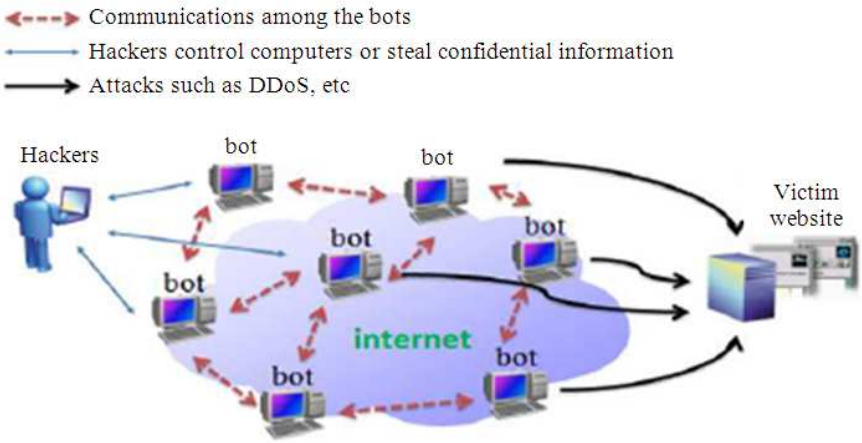

Fig. 1. P2P botnet operation

After building the botnet, all bots should be ready to communicate with their botmaster for more instructions, as starting an attack or making update. That will be in the C&C phase, which is the most important part for the botnet; because it defines its network topology and its strength against defenses. P2P botnets also uses the P2P traffic indexes to send commands. C&C phase include two mechanisms; pull mechanism and push mechanism. During the Pull mechanism, bots retrieve commands from the botmaster. This commonly used in centralized botnets, but in P2P, a peer can send a query message for the needed file and based on the routing algorithm of the system, the message will be passed around. The search for the desired file will be continued until peers receive the query message and return it with command encoded, or the query message will expire. Push mechanism means the bots are passively waiting for commands and resend them to other bots.

According to the instructions, bots will carry malicious activities during the attack phase. After attack, if some bots are detected and stopped, the botmaster will plan to build a new botnet.

P2P bots can spread very fast in P2P network; due to the huge popularity of P2P file sharing systems; Moreover, their traffic can be completely integrated with regular P2P traffic, which makes them more difficult to be detected.

1.2. P2P Botnet Detection

In order to protect networks against bots, bots should be stopped from spreading. But this process is not easy with P2P botnet, since there is no central point to detect and stop it. The researchers are working on methods to detect the communication of botnets, in order to prevent the bots from forming new botnet, or launching an attack.

There are two main approaches for botnet defense, the first one is analyzing the network traffic the second approach is using honeypots (Zhaosheng *et al*., 2008).

Analyzing the network traffic can be useful to identify the existing botnet in the networks and collecting its characteristics and behaviors and build a common model for it. So the defenders can use this model to detect botnets. Botnet in this model based on the existence of many network anomalies such as high volumes of traffic, high network latency and traffic on unusual ports. Using the common model, the hosts that share similar communication and similar malicious activity pattern can be identified. Although this approach is effective for detecting known botnets, it is not such powerful in detecting new botnets. In the other hand, honeypots is useful in analyzing characteristics of new botnets, but it is not effective in detecting infected programs. Therefore, defenders tend to use both approaches together to detect botnets and identify their C&C mechanisms (Li *et al*., 2011).

1.3. P2P Botnet Detection Techniques

P2P botnet is still an emerging technology; therefore most of the literature is about the centralized botnet. Recently, researchers have focused on analyzing and modeling P2P botnet (Grizzard *et al*., 2007). There are some efforts on detecting P2P botnet, but it still the great challenge.

The following subsections discuss most of the P2P botnet detection approaches proposed by the researchers around the world in recent years.

1.4. Botminer

Proposed a general botnet detection framework, named BotMiner. This framework is proposed for both centralized IRC and P2P botnets. BotMiner suppose that bots are coordinated malware and shows the same communication patterns and malicious activities. The first stage in the proposed framework is clustering hosts with similar malicious activities and communication patterns from a network traffic and the resulted clusters are named A-Plane and C-plane for activity traffic and C&C communication traffic, respectively. The second stage is applying a cross correlation between A-plane and C-plane clusters. As a result from the correlation process, hosts that show both kinds of behaviors are detected as bots.

Real network traffic was used to evaluate the proposed framework. The results show relatively high detection efficiency, with low numbers of false positives and false negatives. Furthermore, reasonable time and resources have been employed.

BotMiner has two main limitations, the first one that it targets a group of infected computers within a monitored network, but in fact in a monitored network there is only a single compromised host and this single host may belong to a larger botnet. Therefore, BotMiner is not effective in detecting compromised hosts. The second limitation of BotMiner is its assumption of the systematic classification of any infected hosts. In case of P2P botnet, the bot may have malicious behaviors but still exchange normal C&C messages, so that bot will not be considered as a bot for the BotMiner. Under such scenario, BotMiner may not detect bots that exchange covert C&C messages (Gu *et al*., 2008).

1.5. Network Streams Analysis

As shown in **Fig. 2**, they present a general P2P botnet detection framework, which includes three main algorithms.

P2P nodes detection algorithm: Filtering can be applied on the P2P botnet, according to its features of paroxysm and distribution of the network streams.

P2P nodes clustering algorithm: Clustering is proposed based on the connection characteristics of the nodes. The research uses K-mean clustering algorithm which based on the connection degree between the pair of nodes.

Botnet behaviors detection algorithm: By extracting the similarities of the malicious behaviors of the bots, which may occur several times a day, the algorithm can detect if the P2P network is infected by bots.

Unlike other detection models, the testing characteristics of this model taken from net stream macroscopical statistic, so it can be used to detect unknown protocol P2P botnets effectively.

They ran a simulation of the three model algorithms in LAN circumstances and have goocd results of extracting the P2P stream, clustering and detecting botnets from normal network (Liu *et al*., 2010).

1.6. Multi-Phased Flow Model

P2P bots generate phased flows to connect with outside peers in order to construct the botnet. Based on this, the researcher proposed a multi-phased flow model to detect malicious traffic. The proposed model identifies P2P botnet by observing similar flows between network hosts. The proposed system consists of three stages, shown in **Fig. 3**.

Flow grouping: Where the system group huge volume of traffic generated by P2P botnets and make clustering of TCP/UDP connections.

Flow Compression: Extract information from each flow group value.

Flow Modeling: Modeling the P2P flows using a constructed matrix based on the transition information.

Finally, the likelihood ratio is computed based on the probability-based models and used in detecting bots.

The experimental evaluation was carried on Storm, Nugache and Spam Thru botnets. The detection rates ware 100, 95, 96% respectively (Noh *et al*., 2009).

1.7. Node Behavior Detection

This research proposed a new method to detect the P2P bots inside the LAN. It uses correlation between the Process name and both ports and network traffic (the protocols). To evaluate the system on real network, a storm bot infected dataset has been used. The research was conducted in University Technology Malaysia (UTM), which has a UTM-AntiBot to monitor the input and output flows and the network communication. In this research UTM-Antibot has been used to observe the network traffic between the internet and the internal host. After filtering out all the processes of the network traffic, PPNT correlates each process with its associated port and the connected IP. A behavior of a normal user under a controlled LAN has been examined. The research resulted that it is impossible to send thousands of SMTP packets in less than 10 minutes and considering UDP packets with fixed port, SMTP packets confirm that this user is a part of Storm Botnet. Acceptable but not high rate of detection has been shown in their experimental results (Rostami *et al*., 2011).

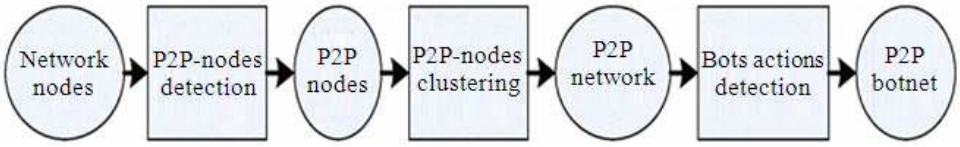

Fig. 2. P2P Botnet detection model

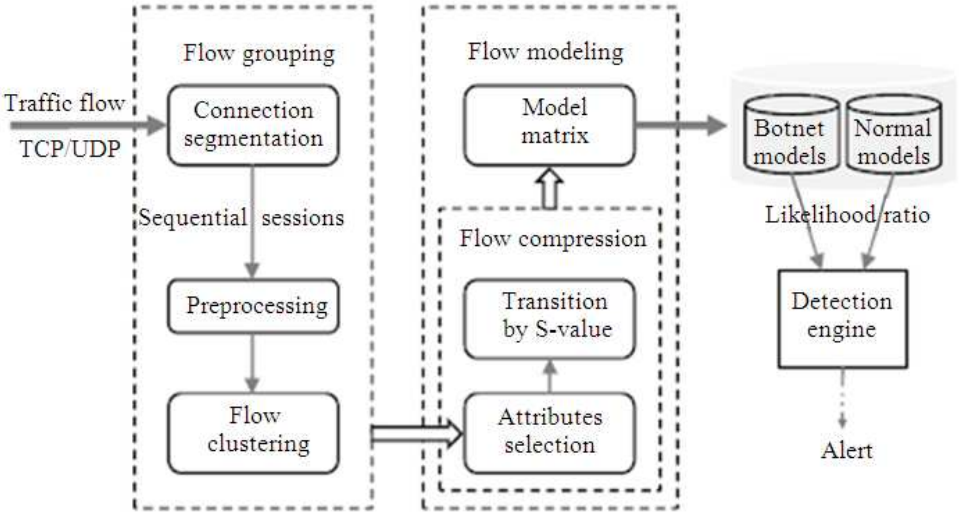

Fig. 3. Multi-Phased flow model architecture

1.8. Entropy Theory Detection

Propose a new detecting method that applies the Information Entropy theory in the Detection Multi-chart CUSUM.

Storm botnet malicious activities appear as abnormities in network flows on the CUSUM chart. The researcher collected these abnormities and transformed it into proportion, then integrated the UDP packets characteristics to data flow entropy. Then, the resulted data will be the detecting input factors of multi-chart non parametric CUSUM algorithm.

The algorithm steps are as following:

- Take the data from monitoring device and turn it into the proportion CUDP, CICMP, CSMTP.
- Compute the data flow entropy-Ei
- Put the resulted data on the multi-chart CUSUM as an input and output d(Si(UDP)), d(Si(ICMP)), d(Si(SMTP)), d(Ei)
- Use those outputs and do the judgment by this integration method

$$D_t = \alpha_t * d(S_n(UDP)) + \beta_t * d(S_n(ICMP)) + \gamma_t d(S_n(SMTP)) + \eta_t d(E_i)$$

$$\alpha_t + \beta_t + \gamma_t + \eta_t = 1$$

α, β, γ are the weight values. If D>K (K is a network constant), it is judged as abnormity and consider that botnet exists, otherwise not.

Evaluation of the proposed method was carried on an experiment network platform consists of a protected internet network; include several computers connected to a firewall through a hub. One of the logging hosts to the network traffic was with Wireshark and some of the hosts work as storm botnet. Results show that using entropy theory has its own advantages in detecting P2P botnets (Kang and Zhang, 2009).

1.9. Behavioral Correlation

They developed an algorithm to detect P2P bots by correlating their behavioral attributes. They use a Peacomm (Storm P2P bot) as a case study. They collect their data by assuming the bot to be already installed on the victim host, so they used extrusion detection in order

to limit the bot activities. They developed an interception program (APITrace) to record behavioral attributes and capture some function calls done by the monitored processes. These function calls were used as input to the developed algorithm.

The state of the system was defined by three signal categories namely S1, S2 and S3 collected by the interception program APITrace. S1 derived from the change rate of three fields, which are Failed Connection Attempts (FCA), Destination Unreachable (DU) and Reset connections (RST). S2 is derived from the change rate of number of packets send per second. S3 represents the time difference between two outgoing successive communication functions.

The algorithm was developed to find the correlation between S1, S2 and S3, by setting a Sensitivity Value (SV) and check each value of the three signals. If it exceeds SV, the value of one will be assigned to the signal records; otherwise, zero will be assigned. Then, the signal records will be examined to check if they have same values, the value of one will be assigned, which represents the correlation between the three signals. After repeating the process for all the signals of the data (log files), the anomaly factor and the correlation values were calculated.

The evaluation shows that correlating different activities can enhance the detection process of P2P bots. The main disadvantage of this algorithm is that the threshold value is not defined. In addition, evaluation was examined only on one type of bots (Peacomm) (Al-Hammadi and Aickelin, 2010).

1.10. Network Behavior Analysis and Machine Learning

This research proposes a new method for detecting botnets through identifying the network behavior characteristics. This approach aimed to detect P2Pbotnet Command and Control (C&C) phase, which allows detecting the bots before attacking their victims. In addition, this study discussed the requirements of online botnet detection framework and investigates the ability of five Machine Learning (ML) techniques to meet these requirements. The evaluation results show the promising performance of ML techniques, but none of them satisfy all the requirements of the online botnet detection framework (Sherif *et al*., 2011).

1.11. Association between Common Network Behaviors and Host Behaviors

This research proposed a new P2P Botnet detection approach relying on the association between common host and network behaviors.

The proposed framework consists of six stages as following:

- Detected system: To distinguish between the single and communication program, since the main characteristic of the bots is communication with other bots on other computers
- Filtering: To reduce traffic load, so the system can work more efficiently
- Extract features from P2P data: Detect the more relevant features to make a subset of features that describe properly the P2P data
- Botnet detection: Based on the data source this stage includes host data detection and network data detection. The objective is to detect the known botnet and the unknown malware
- Report: If the detected behavior is known, the system report, if not the system will detect the bot behavior by correlating host and network behaviors
- Solution: After finding out the botnet, the system can either fire it back or take it down
- This method has some limitations such as, bots that using encryption algorithms cannot be detected (Yin and Ghorbani, 2011)

1.12. User Behavior Sociality and Traffic Entropy Function

Based on the user behavior and the social action of Botnet nodes that differ from normal nodes, this research proposed a new structure to identify P2P Botnet and consider it as a key basis for P2P Botnet detection. The proposed structure of P2P Botnet includes:

- Analyzing sociality characteristics as centrality from the original network data, by making too high centrality nodes as suspicious ones
- Finding out data packet size characteristic cand use the entropy concept to make model for the data packet of the suspicious node
- Make deep data packet detection, with improved entropy

After doing experimental evaluations of the proposed structure, the results show that this structure can identify the P2P botnet with high accuracy. However, the identification accuracy reduces when the download rate of net traffic is very high, or the user video streaming is too big (Zhigang *et al*., 2012).

1.13. Data Mining

This research proposed a P2P botnet detection approach which relies on monitoring gateway traffic and analyze network behavior using data mining techniques. To evaluate the proposed method, they used a freeware WEKA and three popular algorithms J48, Naïve Bayes and Bayesian networks for data mining. The resulted accuracy rates were 98, 89 and 87%, respectively for the three algorithms. Based on the results, the proposed method can used in distinguishing infected bots flows from other bots and the most appropriate algorithm among the three algorithms was J48 (Liao and Chang, 2010).

1.14. TCP Distinctive Behavior

This study presents a new approach to recognize P2P botnets, through its Transmission Control Protocol (TCP) connections. They focus on analyzing the abnormal characteristics in the network traffic behavior of P2P botnet. This approach can be used for early detection and warning of any P2P botnet activities in the network; since the P2P Botnets initialize its activities by the TCP connections. The proposed framework includes filtering, detecting malicious activity and analyzing. The study also uses the general P2P botnet detection framework with the P2P botnet detection model proposed by Dan *et al.* (2010). The model involved three steps: Detection of the P2P-nodes, clustering of P2P-nodes and detection of the botnets.

The proposed framework was implemented on both normal P2P network test-bed and abnormal P2P traffic which has been infected by the P2P botnet. The captured dataset in each case is analyzed based on TCP protocols using network analysis tools. At the end of the framework, comparison is done to classifies and detect the P2P botnet characteristics (Syahirah *et al*., 2011). **Figure 4** shows proposed TCP framework.

1.15. Behavior Clustering and Statistical Tests

Su & Thomas present two detection schemes to detect P2P botnet C&C behaviors. Based on the observation of node behaviors correlations at different times, they design algorithms using formal statistical tests on popular behavior clusters in the network, to see if there are undetectable activities from C&C in P2P botnets using non-P2P protocols, in order to measure the impact of P2P botnet C&C behaviors on normal behavior clusters. They evaluate this approach in both simple and realistic cases and achieve an encouraging good detection rate of C&C channel (Chang and Daniels, 2009).

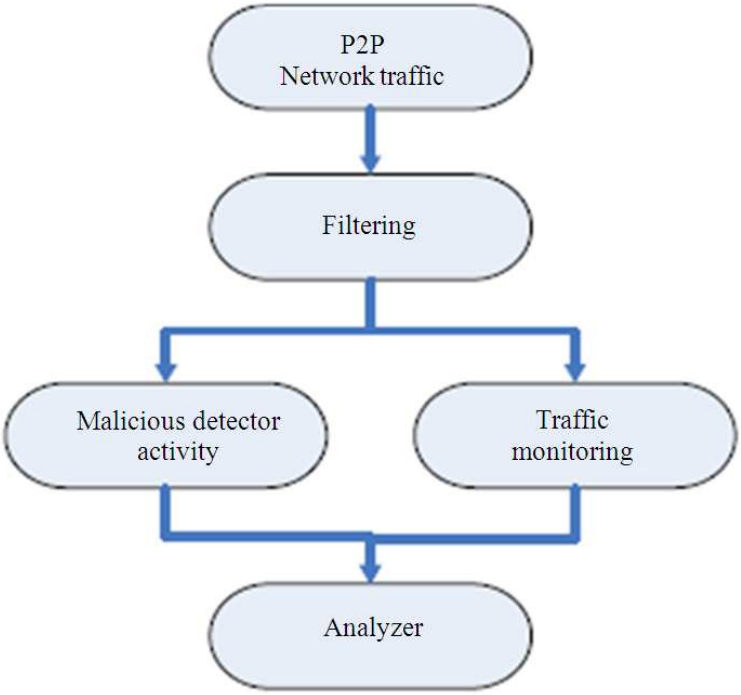

Fig. 4. TCP Framework for P2P botnet detection

Table 1. Summerized Table of the discussed detection approaches

Researcher	Proposed detection approach	Features
Gu *et al*. (2008)	Proposed a general botnet detection framework named BotMiner, based on clustering analysis of network traffic	BotMiner can be useful for detecting IRC botnet, but it is not effective for detecting P2P botnet
Masud *et al*. (2008)	Proposed a general botnet detection framework named BotMiner, based on clustering analysis of network traffic	BotMiner can be useful for detecting botnet, but it is not effective for detecting P2P botnet
Noh *et al*. (2009)	They consider the network traffic as infinite data stream and use data mining techniques to detect P2P botnet	They have better detection accuracy than other data stream classification techniques
Kang and Zhang (2009)	Propose using a multi-phased flow model to detect malicious traffic	The proposed system shows the efficiency with the SpamThru, Storm and Nugache botnets
Kang and Zhang (2009)	Applying the information entropy theory In the detection Multi-chart CUS UM to detect new P2P botnets	The results show that the entropy theory has its own advantages in detecting P2P botnets
Chang and Daniels (2009)	Present two detection schemes using behavior clustering and statistical tests clustering and statistical tests	The proposed algorithms achieve an encouraging good detection rate of C&C channel
Chen *et al*. (2009)	Propose a detection method of P2P controlled bots on the hosts, using API function calls and algorithms to process APIs	Effective in detecting the controlled bots on the host, but has few limitations as the large training set required to improve the detection accuracy
Hangxia (2010)	They propose mitigating P2P botnets using Two Sybil attacks, based on analyzing botnets' weaknesses	The results show that sybil attack technique can be quite effective to defend against P2P botnets
Liu *et al*. (2010)	Present a general P2P detection model and algorithms based on network stream analysis	It can be used to detect unknown protocol P2P botnets effectively
Al-Hammadi and Aickelin (2010)	Developed an algorithm to detect P2P bots by correlating their behavioral attributes	The proposed correlation method can enhance the detection process of P2P bots The key limitation is that the threshold value is not defined
Liao and Chang (2010)	Propose a detection approach relies on monitoring traffic at the gateway and using data mining to analyze network behavior	The proposed method can used in distinguishing infected bots flows from other bots
Rostami *et al*. (2011)	Propose detecting P2P botnets connections on node behavior, by using correlation between processes with the associated ports and traffic protocols	Acceptable but not high rate of detection has been shown in the experimental results
Syahirah *et al*. (2011)	Propose recognizing P2P botnets through its TCP connections, by analyzing the abnormal characteristics in the network traffic behavior	Can be used for early detection and warning of P2P botnet activities in the network
Sherif *et al*. (2011)	Detecting P2P botnets through identifying the network behavior characteristics and using Machine Learning techniques	The results show the promising performance of ML techniques but none of them can satisfy all the requirements of the online botnet detection framework
Yin and Ghorbani (2011)	Their detection is relying on the association between common host and network behaviors	The main disadvantage is that bots using encryption algorithms cannot be detected
Zhigang *et al*. (2012)	Proposed a new structure to identifyP2P botnet, based on the user behavior and the social action of botnet nodes	The proposed structure can identify the P2P botnet with high accuracy. However, the identification accuracy reduces when the download rate of net traffic is very high

1.16. Cyber-Security: A Data Mining Approach

They follow the approach of considering the network traffic as infinite data stream and classify it into equal size of chunks. However, they propose a new technique in storing the data. They divide the chunks into several classifiers and introduce multi-chunk, multi-level ensemble for data stream classification. This technique reduces the expected error of single chunk, single-level ensemble method. They evaluate their proposed technique theoretically and empirically and have better detection accuracy than other data stream classifications techniques (Masud *et al*., 2008).

1.17. Controlled Bots on the Host

Proposed a general approach to detect P2P-controlled bots on the host. They aim to detect malicious behaviors and P2P communication simultaneously. They use API function calls and N-gram algorithm to process API sequence and utilize a static signature to detect P2P communication traffic. The advantage of this method is detecting the bots on the host. There are few shortcomings in this approach, such as the large training set required to improve the detection accuracy and other limitation is the usage of signature based technique (Chen *et al*., 2009).

1.18. Mitigating Peer-to-Peer Botnets by Sybil Attacks

They proposed a new detection technique, include mitigating P2P bots behaviour. Based on analysing botnets' weaknesses, they present two Sybil attacks methods; d-choice sybil attack and random Sybil attack. They also study the effect of the sybil nodes sizes in attacking P2P botnet. Their proposed method has been evaluated by simulation and theoretically (Hangxia, 2010).

The **Table 1** below summarizes the P2P botnet detection approaches that have been discussed in this previously.

3. CONCLUSION

P2P Botnet is the most critical issue in Network security to be detected since it based on non-centralized command and control (C&C) communication, In this study we present most of the P2P detection techniques proposed by researchers. In addition, we identify advantages and shortcomings of each of the discussed techniques, which can guide the researchers to a better understanding of P2P botnets and easier for them developing more sufficient detection techniques.

From the detection approaches discussed in this study, we can notice that:

- Most of studied approaches rely on one technique in detecting the bots, which may cause less detection accuracy
- Many techniques focus on detecting the bots after the attacking process; this cannot stop bots from spreading, since the remaining bots will build a newborn botnet
- Most of them evaluate their proposed methods only theoretically or simulation with non-real P2P botnet environment

4. ACKNOWLEDGEMENT

This research is supported by National Advanced IPv6 Centre of Excellence (NAV6), Universiti Sains Malaysia (USM).Grant title: "A comprehensive botnet mitigation Ecosystem".Acc.No:1001/PNAV/857001.

5. REFERENCES

Al-Hammadi, Y. and U. Aickelin, 2010. Behavioural correlation for detecting P2P bots. Proceedings of the 2nd International Conference on Future Networks, Jan. 22-24, IEEE Xplore Press, Sanya, Hainan, pp: 323-327. DOI: 10.1109/ICFN.2010.72

Chang, S. and T.E. Daniels, 2009. P2P botnet detection using behavior clustering and statistical tests. Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence, (AI '09), ACM Press, New York, USA., pp: 23-30. DOI: 10.1145/1654988.1654996

Chen, F., M. Wang, Y. Fu and J. Zeng, 2009. New detection of peer-to-peer controlled bots on the host. Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, Sept. 24-26, IEEE Xplore Press, Beijing, pp: 1-4. DOI: 10.1109/WICOM.2009.5302674

Dan, L., Y. Li, Y. Hu and Z. Liang, 2010. A P2P-botnet detection model and algorithms based on network streams analysis. Proceedings of the International Conference on Future Information Technology and Management Engineering, Oct. 9-10, IEEE Xplore Press, Changzhou, pp: 55-58. DOI: 10.1109/FITME.2010.5655788

Grizzard, J.B., V. Sharma, C. Nunnery, B.B. Kang and D. Dagon, 2007. Peer-to-peer botnets: Overview and case study. The Johns Hopkins University.

Gu, G., R. Perdisci, J. Zhang and W. Lee, 2008. BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection. Proceedings of the 17th Conference on Security Symposium, (CSS' 08), USENIX Association Berkeley, CA, USA., pp: 139-154.

Hangxia, Z., 2010. Mitigating peer-to-peer botnets by sybil attacks. Proceedingsd of the International Conference on and Information Technology and Ocean Engineering, Jan. 30-31, IEEE Xplore Press, Macao, pp: 241-243. DOI: 10.1109/CICC-ITOE.2010.67

Kang, J. and J.Y. Zhang, 2009. Application entropy theory to detect new peer-to-peer botnet with multi-chart CUSUM. Proceedings of the 2nd International Symposium on Electronic Commerce and Security, May 22-24, IEEE Xplore Press, Nanchang, pp: 470-474. DOI: 10.1109/ISECS.2009.61

Leonard, J., X. Shouhuai and S. Ravi, 2009. A framework for understanding botnets. Proceedings of the International Conference on Availability, Reliability and Security, Mar. 16-19, IEEE Xplore Press, Fukuoka, pp: 917-922. DOI: 10.1109/ARES.2009.65

Li, X.N., L. Yang and Z. Hua, 2011. Peer-to-Peer botnets: Analysis and defense. Proceedings of the 3rd International Conference on Communication Software and Networks, May, 27-29, IEEE Xplore Press, Xian, pp: 140-143. DOI: 10.1109/ICCSN.2011.6013561

Liao, W.H. and C.C. Chang, 2010. Peer to peer botnet detection using data mining scheme. Proceedings fo the International Conference on Internet Technology and Applications, Aug. 20-22, IEEE Xplore Press, Wuhan, pp: 1-4. DOI: 10.1109/ITAPP.2010.5566407

Liu, D., Y. Li, Y. Hu and Z. Liang, 2010. A P2P-botnet detection model and algorithms based on network streams analysis. Proceedings of the International Conference on Future Information Technology and Management Engineering, Oct. 9-10, IEEE Xplore Press, Changzhou, pp: 55-58. DOI: 10.1109/FITME.2010.5655788

Masud, M.M., J. Gao, L. Khan, J. Han and B. Thuraisingham, 2008. Peer to peer botnet detection for cyber-security: A data mining approach. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, May 12-14, ACM Press, Oak Ridge, TN, USA., pp: 39. DOI: 10.1145/1413140.1413185

Noh, S.K., J.H. Oh, J.S. Lee, B.N. Noh and H.C. Jeong, 2009. Detecting P2P botnets using a multi-phased flow model. Proceedings of the Third International Conference on Digital Society, Feb. 1-7, IEEE Xplore Press, Cancun, pp: 247-253. DOI: 10.1109/ICDS.2009.37

Ping, W., S. Sparks and C.C. Zou, 2010. An advanced hybrid peer-to-peer botnet. IEEE Trans. Dependable Secure Comput., 7: 113-127. DOI: 10.1109/TDSC.2008.35

Rostami, M., B.S. Reza and N.B. Idris, 2011. Analysis and detection of P2P Botnet connections based on node behaviour. Proceedigns of the Information and Communication Technologies, Dec. 11-14 IEEE Xplore Press, Mumbai, pp: 928-933. DOI: 10.1109/WICT.2011.6141372

Sherif, S., I. Traore, A. Ghorbani, B. Sayed and D. Zhao *et al*., 2011. Detecting P2P botnets through network behavior analysis and machine learning. Proceedings of the 9th Annual International Conference on Privacy, Security and Trust, Jul. 19-21, IEEE Xplore Press, Montreal, QC, pp: 174-180. DOI: 10.1109/PST.2011.5971980

Syahirah, A.R., M.Z. Masud, M.F. Abdollah, S. Sahib and R. Yusof, 2011. Recognizing P2P botnets characteristic through TCP distinctive behaviour. Int. J. Comput. Sci. Inform. Security, 9: 7-11.

Yin, C. and A.A. Ghorbani, 2011. P2P botnet detection based on association between common network behaviors and host behaviors. Proceedings of the International Conference on Multimedia Technology, Jul. 26-28, IEEE Xplore Press, Hangzhou, pp: 5010-5012. DOI: 10.1109/ICMT.2011.6001651

Zhaosheng, Z., G. Lu, Y. Chen, Z.J. Fu and P. Roberts *et al*., 2008. Botnet research survey. Proceedings of the 32nd Annual IEEE International, Computer Software and Applications, Jul. 28-Aug. 1, IEEE Xploer Press, Turku, pp: 967-972. DOI: 10.1109/COMPSAC.2008.205

Zhigang, J., W. Ying and B. Wei, 2012. P2P Botnets detection based on user behavior sociality and traffic entropy function. Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks, Apr. 21-23, IEEE Xplore Press, Yichang, pp: 1953-1955. DOI: 10.1109/CECNet.2012.6202113