e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:05/May-2020 www.irjmets.com

DISTRIBUTED THREAT INTELLIGENCE SYSTEM: A NEW SIGHT OF P2P BOTNET DETECTION

Puja Sunil Erande[*1], Monika Dhananjay Rokade[*2]

[*1,2]Sharadchandra Pawar College Of Engineering, Dumbarwadi (Otur),India.

ABSTRACT

Botnet evolution affects most of cyber space security. Now days Botnet has become most important threat in cyberspace security. Because of its feature like strong concealment and easy expansibility, Detection of botnets done through analysis of network traffic. Most of researchers uses this technique.

For Peer -to-Peer (P2P) botnet detection method, distributed threat intelligence system is used. To fufill the botnet detection main important parts are: the threat intelligence sharing and evaluating system, the BAV quantitative model, the AHP and HMM based analysis algorithm.

KEYWORDS: Threat intelligence ;Threat intelligence sharing ;P2P Botnet Detection.

I. INTRODUCTION

Botnet is set of number of Internet-connected devices each of which is running one or more bots. Botnets usally combines various malwares such as worm, Trojan, backdoor toolkit and so on.

The first Botnet **PrettyPark ,** a malicious code created in 1999 with botnet features ,and botnet is now most widely used as **cyber attack weapon**.

With development of of IT technology, botnet has evolved from centralized structured system distributed system . With the number of IoT devices exploding, cyber attackers starts to turn IoT devices into the bots ,and that enriches cyber attacks pattern.

Main example of Botnet is Mirai ,this ever largest IoT botnet out break in 2016 launched a DDOS attacks on 20th September with maximum speed of 1.5 Tbps on OVH , a web host in France and launched another DDoS attack on the DNS management system service provider in America.

II. METHODOLOGY

a) What is P2P Botnet?

Subheading should be 10pt It is used to make a whole botnet paralyzed once the master node is found and shut down, which is known as single point of failure. To avoid weakness of traditional centralized structure, most of botnets uses decentralized Peer- to -Peer structure. That is each bot act as a separate server.

b) Existing P2P Botnet Detection methods:

Based on Reverse Engineering Analysis

P2P botnet analysis and tracking technique is based on reverse analysis. After getting copy of binary bots it is necessary to dissemble the binary code.

Based on Network Data Analysis

P2P botnet analysis and tracking is based on data flow .This method identify the existence of bot by filtering the network data flow and then filter illegal data before attack.

Based on TI analysis

The concept of TI analysis was around near 2010 but actually implemented in 2015. Threat-Intelligence is evidence based knowledge including context, mechanisms, indicators ,implications and actionable advice about existence data.

III. MODELING AND ANALYSIS

P2p Botnet Dettection Method Based On Distributed Threat Intelligence System

Following are the main P2P Botnet detection methods :

1) Threat Intelligence Sharing and evaluating system:

What is STIX?

STIX stands for "Structured Threat Information expression". Is a language and serialization format used to exchange Cyber Threat Intelligence(CTI). STIX is open source and free allowing interested to ask questions freely.

Distributed Threat Intelligence Sharing System:

STIX contains threat information sharing policies and standards. The segment frequency of STIX is reflected by sighting community.

Detailed detection is as following:

A) System Structure Design :

The distributed structure design consists of Botnet and APT detection system connected to each other based on distributed threat intelligence system. As shown in Fig. 1 system is mainly composed of community cluster and honeypot cluster. In community cluster users can set their evaluation indices according to their respective conditions and give ranking to importance of threat intelligence. The ranking results also distributed to other members of the same cluster.

The main purpose of honeypot cluster is to gather the threat intelligence data.

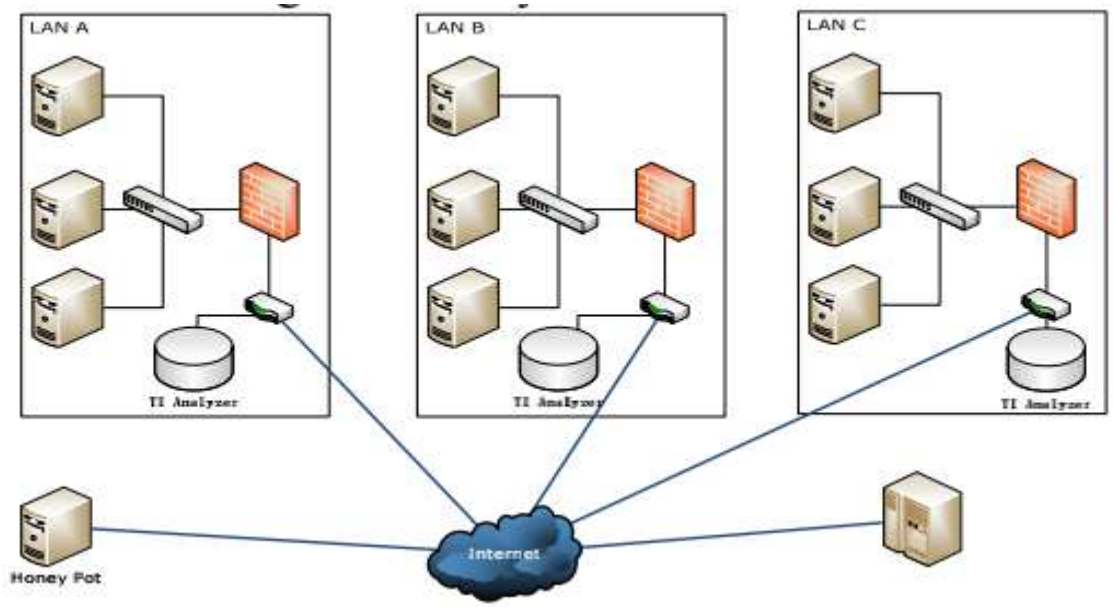

Fig-1: Distributed TI Sharing based Botnet detection system

B) Sharing Mechanism:

The Threat intelligence system are based on STIX and TAXII which are popular sharing modules established by OASIS. Threat events are recorded according to STIX standard and distribute through TAXII standards.

There are 3 types of threat intelligence sharing system:

1) Peer -to -Peer(P2P)
2) Source and Subscriber

3) Hub and Spoke

All sharing models are described in figure 2.

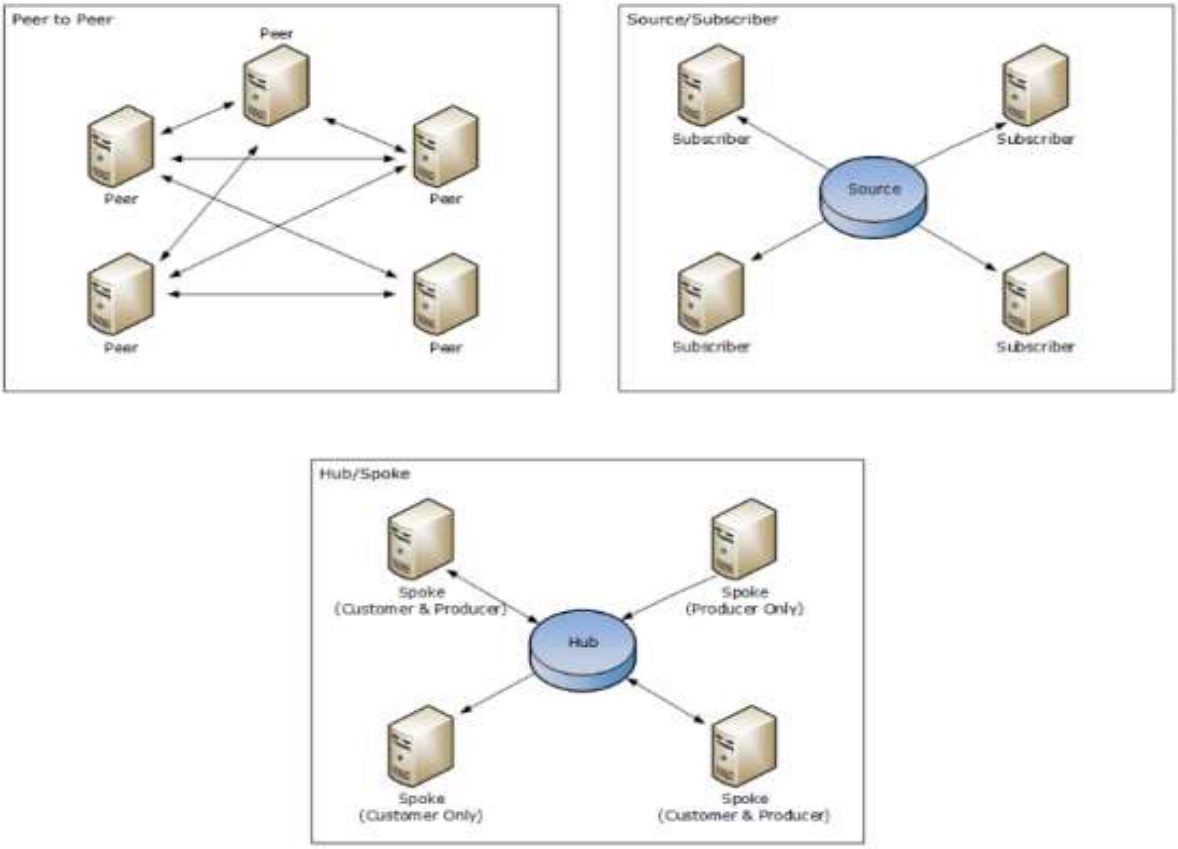

Fig-2 : Three types of sharing models

C) Sharing Strategy:

Below steps are used for describing process flow of scoring Intelligence system:.

1) Deployment and setting :

This step consists of deployment of clients to each community cluster . Key indicators are used for clusters according to their community type

2) Collection:

In this step main task of clients to collect and analyze threats events occurring in the cluster.

3) Report:

Each system gathered and scores the threat intelligence data and reports the analysis to main cluster according to their situation.

4) Push:

The center or main system tests the received threat intelligence .If the threat intelligence data is correct and true ,centers will decide to push it according to the community.

5) Measurement

Central system is responsible for collection and analysis of threat intelligence . After analysis done its very easy to find out where the APT attack take place.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:02/Issue:05/May-2020 www.irjmets.com

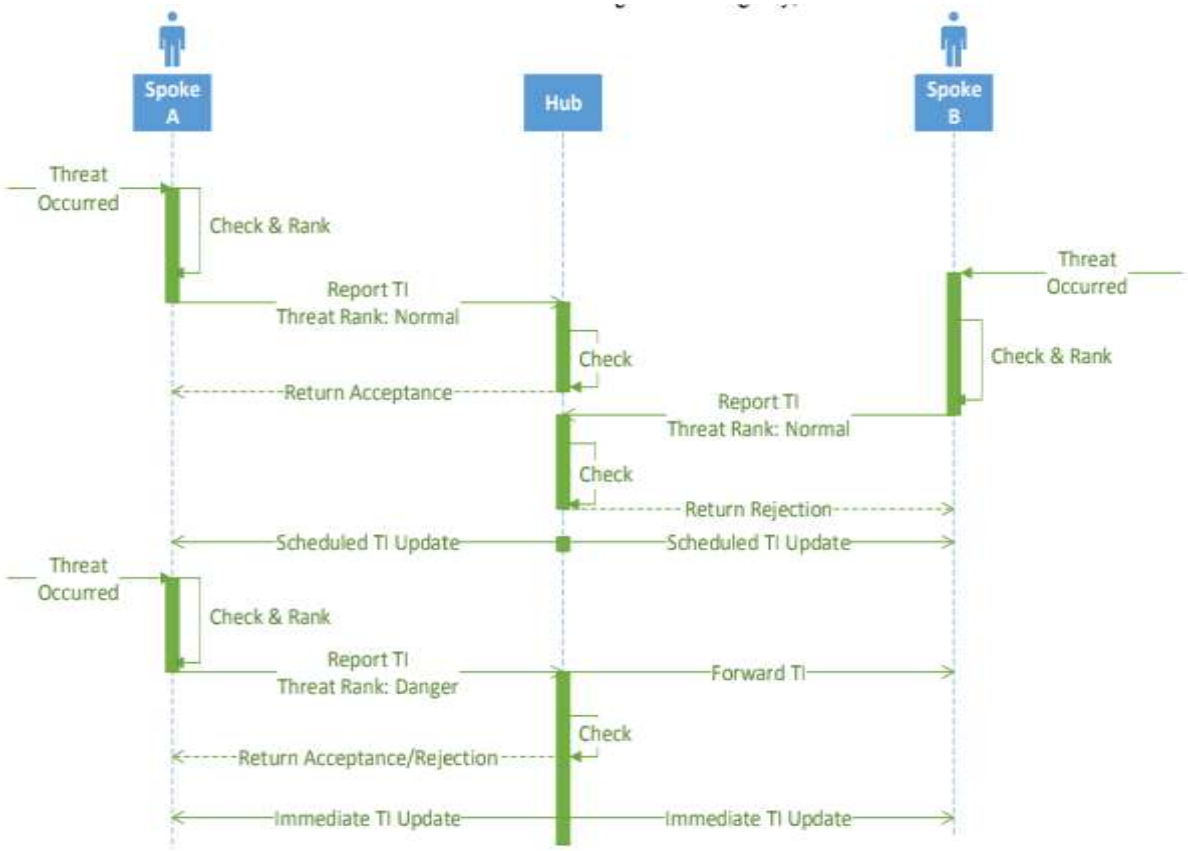

Fig-3: Process Flow of Scoring Intelligence Sharing System

2) BAV Quantitative model:

BAV is the "Botnet Active Vector" ,in this model system runs continuously on main server, community clusters and calculates the Botnet Active Vector(BAV) in each predefined time intervals. BAV model is based on quantification and measurement methods. Research on policy assessment of Cyberspace security status, based on AHP and optimized ERM mix algorithm.

The proposed system described each threat intelligence report into 3 level collection segments.

1) BAV Degree

2) Tag

3) Sub Cluster

BAV degree	Tag	Sub Cluster	Imp	Freq
Attack	Attack Pattern Name[] Malware Name[] Intrusion-Name []	Name_1 ..Name_n Name_1....Name_n Name_1....Name_n	....	....
Clue	Indicator_label [] Course-of-Action.Name[]	Label_1.....Label_n Name_1.....Name_n	....	....
Weakness	Vulnerability.name[] Threat-actor-target []	Label_1.....Name_n Target_1.....Target_n	....	....

Table-1: BAV Structure

3) AHP and HMM based analysis algorithm:

This is advance model for detection of threat intelligence which uses input as a BAV tables.Since BAV model is only working on the current situation. HMM is used for training normal samples and finding abnormal behavior.

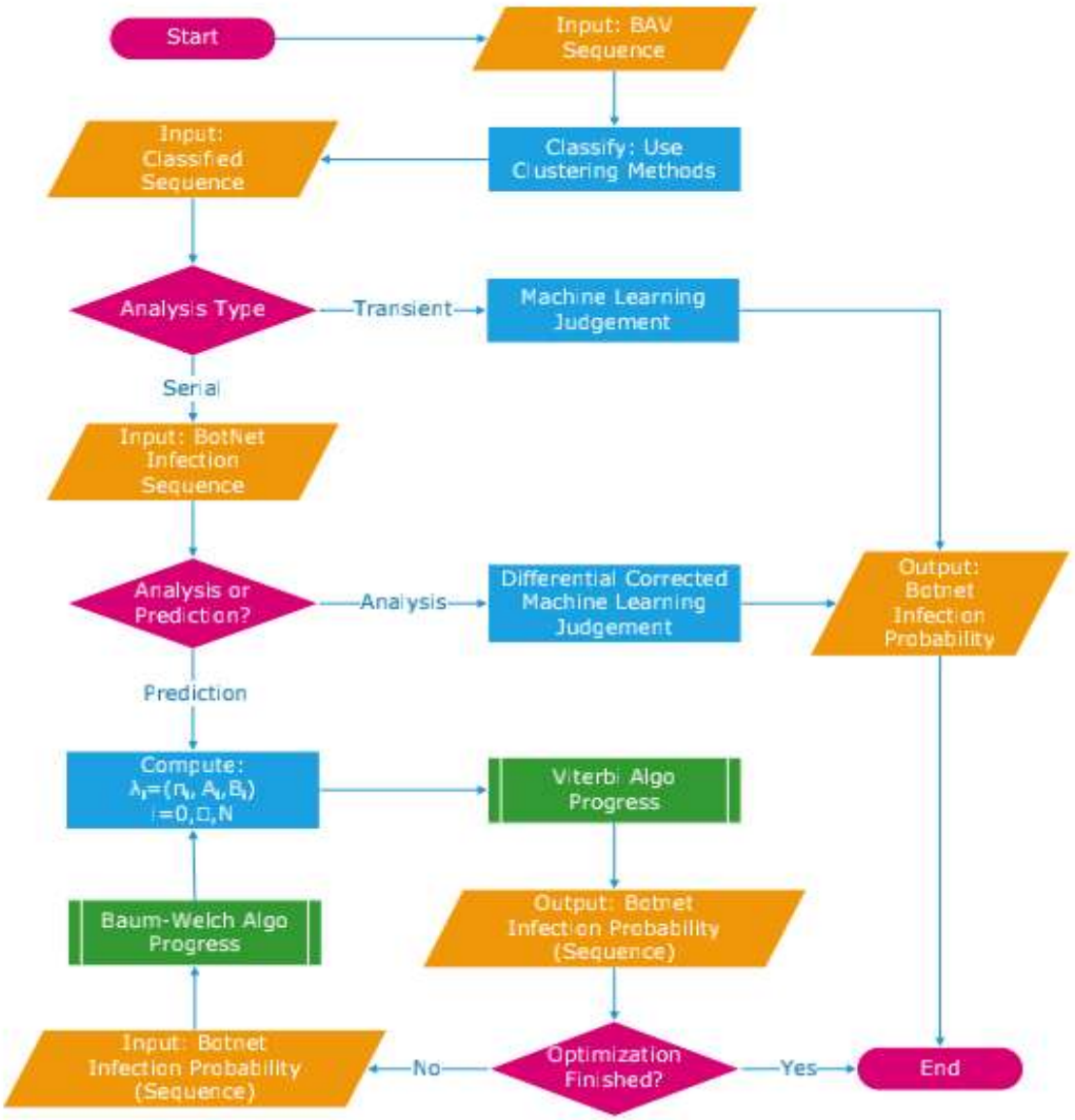

Fig-3: HMM Process

IV. RESULTS AND DISCUSSION

Peer -to -Peer(P2P) Botnet detection is become great challenge in now days. Most of the researchers are uses this types of distributed Threat intelligence structures for designing P2P botnet detection systems.

Main important parts from this paper :

1) Threat intelligence sharing and evaluating mechanism

2) BAV Quantitative model

3) AHP and HMM model

V. CONCLUSION

All the main points of the research work are in this paper consists of use of new threat intelligence system. Researchers aware about how to design and develop the distributed threat intelligence structures based on various models.

VI. REFERENCES

[1] Geer D. Malicious bots threaten network security. Computer. 2005. 38(1): 18-20

[2] Cui Lijuan, Ma Wei guo ,Zhao Wei, Jing Qiushi. A Survey of Botnet. Journal of Information Security Research, 2017. 3(7):589-600.

[3] Li Ming. Botnet Evolution and Defense. Computer Security. 2010(2):81-83.

[4] Canavan, J. (2005, October). The evolution of malicious IRC bots. In Virus Bulletin Conference (pp. 104-114).

[5] Dave McMillen, Michelle Alvarez. 2017-04-10. Mirai IoT Botnet: Mining for Bitcoins? https://securityintelligence.com/mirai-iot-botnet-miningfor-bitcoins.

[6] Zhang Xi, Tang Heping. Study on Botnet Based on P2P. Computer & Digital Engineering. 2009. 37(2):94-97.

[7] Dittrich, D., & Dietrich, S. (2008, October). P2P as botnet command and control: a deeper insight. In 2008 3rd International Conference on Malicious and Unwanted Software (MALWARE) (pp. 41-48). IEEE

[8] Rossow, C., Andriesse, D., Werner, T., Stone-Gross, B., Plohmann, D., Dietrich, C. J., & Bos, H. (2013, May). Sok: P2pwned-modeling and evaluating the resilience of peer-to-peer botnets. In 2013 IEEE Symposium on Security and Privacy (pp. 97-111). IEEE

[9] Holz, T., Steiner, M., Dahl, F., Biersack, E., & Freiling, F. C. (2008). Measurements and Mitigation of Peer-toPeer-based Botnets: A Case Study on Storm Worm. LEET, 8(1), 1-9.

[10] Li, K., Wen, H., Li, H., Zhu, H., & Sun, L. (2018, October). Security OSIF: Toward Automatic Discovery and Analysis of Event Based Cyber Threat Intelligence. In 2018 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. (Smart World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 741-747). IEEE.

[11] MacDonald, I. L., & Zucchini, W. (1997). Hidden Markov and other models for discrete-valued time series (Vol. 110). CRC Press.