# *PTP Approach in Network Security for Misbehavior Detection*

Neha Pathak
*Department of Information Technology, SKNCOE Pune, India*
*Email: neha.pathak59@gmail.com*

R. S. Apare
*Assistant Professor in Department of Information Technology, SKNCOE Pune, India*
*Email: ravi.apare@gmail.com*

***Abstract*—A PTP approach in network security for misbehavior detection system present a method for detecting malicious misbehavior activity within networks. Along with the detection, it also blocks the malicious system within the network and adds it to Blacklist. Malicious node defined as a compromised machine within the network that performs the task provided by bot server i.e. it does not forward the legitimate message to another node in the network or send some other message to a neighbor node. This system is based on Probabilistic threat propagation. This scheme is used in graph analysis for community detection. The proposed system enhances the prior community detection work by propagating threat probabilities across graph nodes. To demonstrate Probabilistic Threat Propagation (PTP) paper considers the task of detecting malicious node in the network. Proposed System also shows the relationship between PTP and loopy belief propagation.**

***Keywords*-blacklist, botnet, community detection, graph algorithms, Network security.**

## I. INTRODUCTION

Network Security is an important field of computer networking. It secures a computer network infrastructure. In Network security administrator or system administrator, handles the network operation. They are also responsible for implementations of the security policy for network software and hardware.They protect a network and the resources accessed from unauthorized access. So it secures the network by protecting and overseeing the operation. Network inference is a topology that shows the wiring diagram of the network. Community detection is an important application in the field of network inference. It explores the structure of static association between entities. Example of community- based system is email traffic between employees of a company, vehicle traffic between physical locations.

In network security, it is critical for the defender to analysis and detection of malicious node activity. Methods for detecting unwanted network traffic can be categorized as signature-based intrusion detection system [9] or anomaly-based detection system [3]. Both of the systems are based to analyze the activity of the individual network node rather than the interaction between nodes. Due to the increase of botnets a newer detection technique have developed which view the network host activity to detect the infective activity of nodes. The behaviors of multiple nodes can be aggregate to perform spatial anomaly [3] detection that considers the relationship between nodes with another node.

Some time network defenders not able to identify known malicious nodes, either the use of previous detection methods in the internal network or from blacklists in external nodes [6]. Using these methods an analysis can be performed to identify host communication with the known malicious nodes on network traffic. Existing work has proposed that malicious node activity is local in the network space and form communities of maliciousness. Method for the detection of malicious nodes on a network, independent of their activities, shows the fact that malicious activity tries to be localized. If a tip node of known maliciousness or their collection is given then proposed system perform graph analysis to compute the threat probability of neighboring nodes. Method work iterative until a Statistical probability is not compute for each node of a network. In the probabilistic threat propagation, [1] the probability of a node being malicious is proportional to the level of maliciousness of its neighbor nodes.

This paper is organized as: In Section 2 Related work is described in detail. Section 3 introduces proposed work.Section 4 describes the working of PTP on graph. Section 5 gives the mathematical model of proposed system. Section6 conclude the paper.

## II. RELATED WORK

Paper [2] shows that by using a single peer to peer method if a bot is detected then it is possible to detect another member of the same network. In a paper, a simple method is presented to identify member host from known peer nodes, of an unstructured P2P botnet in a network. Method provides a list of hosts ordered by a degree of certainty that belong to the same P2P botnet as discovered node belong. Method represents that peers of a P2P botnet communicate with other peers to receive command and update. In spite of some different bots can communicate with another peer bot. Paper shows that for P2P botnets is an unstructured topology where bots randomly select peers for communication it is rarely high probability that bots communicate with external bot though a given time window. There is a probability pair of malicious within a network has a mutual contact.

In this Paper [3] a Botnet Sniffer method is given to detect botnet C&C problem. A proposed approach uses network-based anomaly detection to identify botnet C&C channels in a local area network (LAN) without the knowledge of signature or C&C server addresses. This method can identify both the C&C servers and infected hosts or bots present in the network. This approach based the observation of the pre-programmed activities related to C&C. A bot node within the same botnet will likely show the spatial-temporal correlation and similarity.

Paper [4] presents conditional random fields method to build probabilistic models to segment and label sequence data. Methods provide several advantages over Markov models and stochastic grammars for such tasks. Conditional random fields also avoid a limitation of the label biased problem present in maximum entropy Markov models (MEMMs) and other Markov models using directed graphical models. Paper used iterative estimation algorithms for conditional random fields.

In the paper [5] a novel approach is present to detect activity based communities by propagating membership in between the neighboring nodes. To represent utility of a method, a local implementation is the use. These local are checked for community detection by given starting node and then apply it to on two varied data set. There are two methods were used for membership propagation: Static and dynamic. Static membership utilizes information of tip node into a community that demonstrates the improvement over a baseline method. In Dynamic propagation method nodes membership probability varies over time.

In this Paper [6] a method is used which constructs the blacklists for large scale security log sharing infrastructure. Method Used in this paper uses Page ranking scheme. The ranking method measures how closely related an attack source is to a contributor. This is using the attacker's history and the contributor's recent log production patterns. This method works in three stages. First stage that is called pre-filtering preprocesses the security alerts supplied by sensors across the Internet. This method removes known noises in the alert collection. The preprocessed data are then fed into two parallel engines. The second stage scores the sources using a severity that measures their maliciousness. The relevance ranking and the severity score are combined at the last stage to generate a final blacklist for each contributor.

In Paper [7] an Intrusion Detection System is presented for a network. Using this method, the problem of IDS can be determined by scanning and harvesting attack. A harvesting attack is exploitation where an attacker initiates communications with multiple hosts to control and reconfigure them. While in a scanning, the attacker's communication with multiple hosts is an attempt to determine what services they are running. This paper method evaluates IDS focus to frustrate the attacker goals. In order to do this, model captures the attacker's payoff over an observable attack space.

In this Paper [9] a Snort system is presented which is used to detect Network Intrusion Detection in small and large network system. This tool can be deploying to monitor small TCP/IP networks and detect suspicious network traffic attacks present in a network. It can also provide administrators with enough data to make decisions on the action of suspicious activity. Snort is a cost efficient tool.

In this Paper [10] a Probabilistic Misbehavior Detection Scheme (I trust) were presented which could reduce the detection overhead effectively. Method firstly introduced data forwarding evidences for general misbehavior detection. The proposed framework is not only detect various misbehaviors But also a compatible with other routing protocols. Secondly it introduced a probabilistic misbehavior detection scheme by adopting the Inspection Game.

TABLE I ANALYSIS OF EXISTING SYSTEM

| ***Sr. No.*** | ***Method Name*** | ***Attack Type Addressed*** | ***Advantage*** | ***Disadvantage*** |
|---|---|---|---|---|
| 1. | Probabilistic Threat Propagation[1] | Malicious and infected node | 1) Useful to solve graphical model. | 1) Does not consider weight matrix. |
| 2. | local members of peer-to-peer botnets using mutual contacts[2] | Botnet | 1)It uses advantage of pairwise mutual-contact relationships Between pairs of bot peers. | 1) Identifying only local member of a botnet present in the network. |
| 3. | BotSniffer: Detecting Botnet Command and Control[3] | Botnet C&C | 1) Network-based anomaly detection is possible. 2)Work with IRC and HTTP | 1) Does not detect P2P botnets. |
| 4. | Conditional random fields[4] | Label bias problem | 1) CRF-based prediction model achieves better performance. | 1) Training of CRF model is expensive. 2) Training process is also slow. |
| 5. | Dynamic membership Propagation[5] | Activity based Community detection | 1) Give better performance when weight from tip node to a neighbor is given. | 1) Fail to describe different edge weighting function. |
| 6. | Highly Predictive Blacklisting[6] | Blacklist Communication in the Internet community | 1) Better attacker prediction quality. 2) Long term performance stability. | 1) Threshold adaptation is difficult because small changes require unpredictable effects. |
| 7. | Payload-Oblivious[7] | Intrusion Detection System | 1) By incorporating payoffs, it's better to characterize the deterrence offered by IDS. | 1)focus the activity of the individual network Nodes rather than the interaction between nodes. |
| 8. | Weighted Graph Clustering[12] | Malicious misbehavior | 1) Better time complexity. 2) Does not require specifying number of clusters. | Ineffective where weight is different or not given in the graph. |
| 9. | Snort[9] | Intrusion Detection | 1) Cost-effective tool for detection of Intrusion. 2) Flexible for the small network. | 1) Only detect a Known attack. 2) Signature must be created for every attack. |

## III. PROPOSED SYSTEM

The proposed system will help to system administrators in automatically identifying the compromised machines in their networks. The proposed system will work as router in the network as LAN. Whenever any node wants to send the message to another node then first the shortest path between them is calculated. Our algorithm will check the entire node and detect if any malicious node is present on the selected path if it present then our system will block that malicious node and add their IP addresses into Blacklist. Now system will select another path for transfer and finally messages will be forwarded to their destinations. The architecture of the proposed system works with the help of following parts:

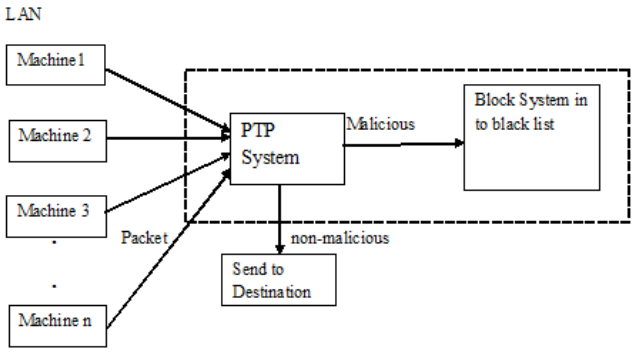


Fig 1 System Architecture

### A. PTP System

In Probabilistic Threat Propagation (PTP), system the threat level calculates at each node is equal to the sum of weight of neighboring nodes from the level of a source to receiver nodes.The weight matrix W is computed as the function $w_{ij} = f(x_i; x_j)$. It measures the interaction between Nodes $x_i$ and $x_j$. PTP detect malicious node and generate very low false positives.

### B. Blacklisting System

The goal of malicious behavior detection in a proposed system is to determine given partial blacklist and recovers full blacklist while keeping false alarms low.

During a malicious detection using PTP system the following steps follows,

1. Initially sender sends a packet to the receiver.
2. Shortest path select between sources to a receiver.
3. IF (receiver ! receive packet)
4. PTP detect the malicious node present in the path between sources to the receiver.
5. IF (malicious node = present) then
6. This system Block that node and add to it in Blacklist.
7. Select another short path and forward packet from this new path to the receiver.
8. Receiver receives the packet.

Here we are using the algorithm threat which is having following steps.

1. Creation of a factor graph from general graph.
2. Given set of Nodes we define the node threat probability vector.
3. Initialize PTP with set {tips} - IP address of a node which are Known if detected earlier otherwise select source neighbor node if it is a first time.
4. Assign priori probabilities $P(x \in \{tips\}) = \gamma$.
5. Here $\gamma \in [0, 1]$.
6. Other nodes initialized to priors of $P(x \notin \{tips\}) = 0$;
7. Weight matrix W can be computed via $w_{ij} = f(x_i, x_j)$.
8. Compute Probabilities at iteration for each node.
9. Reassign $P(x \in \{tips\}) = \gamma$.

## IV. THREAT PROPAGATION IN GRAPH

Graphs are the best way to represents the network architecture and the relationship between node. We Consider a graph G (X, E) here X shows the set of nodes present in the graph and E shows the set of edges of nodes. Now If there exists an edge $e_{ij} \in E$ then we can say that there exists some quantifiable *direct* relationship between nodes $x_i$ and $x_j$ in G. The relationship strength can be described by the weighting $w_{ij}$ on given $e_{ij}$. If there exist an $x_k$ in the graph for which $e_{ik} \notin E$ and has consequences on a node $x_i$. Then this type of relationship called indirect relationship[11].

For our purposes of this paper, we consider two communities for the detection problem: malicious and benign. We consider the probability of being present in the malicious community as $P(x)$ and the probability of being in the benign community is $1-P(x)$. Or simply we can say that $P(x) = P(x; G)$ all probabilities are recursively calculated through the parameterized graph $G$ and with weightings wij Here this can be interpreted as the "threat level" of a particular node be calculated.

## V. MATHEMATICAL MODEL

Set Theory Analysis
A] Identify Nodes:-
N is the set of each user
N= {S, D, M,Nr}
S= Source Node
D= Destination Node
M= Malicious Node
Nr= Neighborhood node

B] Identify the malicious node
M= {m1, m2, m3……}
Where m1, m2, m3…..arethe malicious node

C] Identify the neighborhood node of a malicious node
Nr= {n1, n2, n3…….}
Where n1, n2, n3 are neighbor node of a malicious node

D] Evaluate the Algorithm
A= {a1,a2, a3…}

Where A is the main set of algorithm
r = {PTP}
Let G= (X, E) where X represents the set of nodes and E- represents the set of edges.
Threat level calculates on node $x_i$ as the probability of maliciousness is as:-

$$P(xi, G) = \sum_{j \in N(xi)} Wij\, P\left(xj \mid xi = 0; G\right)$$

Where N ($x_i$) = Neighborhood of $x_i$, eij € E and wij = weight of the edge $e_{ij}$.

## VI. CONCLUSION

A novel method for the malicious detection is introduced in this paper. Probabilistic Threat Propagation is an iterative approach for graph analytic. It determines malicious node in a network by statistical probability. It is hard to find a threat cause to avoid node threat levels being increased uniquely depend on their network presence. PTP outputs approximations of statistical probabilities that are interpretable by an analyst. PTP can use in network security for botnet detection and prediction of malicious domains.

## ACKNOWLEDGMENT

I would like to thank my guide Prof. R. S. Apare for his guidance, constant encouragement and valuable feedback throughout the duration of the paperwork. His valuable suggestions were of immense help throughout this paper. I am also thankful for the concern members of iPGCON2015 to their constant guidelines and support.

## REFERENCES

[1] Kevin M. Carter, NwokediIdika, and William W. Streilein "Probabilistic Threat Propagation for Network Security", IEEE Transactions on Information Forensics and Security, Sep 2014.
[2] B. Coskun, S. Dietrich, and N. Memon, "Friends of an enemy: Identifying local members of peer-to-peer botnets using mutual contacts," in Proc. 26th Annu. Comput. Security Appl. Conf., Dec. 2010.
[3] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting botnet command and control channels in network traffic," in Proc. 15th Annu. Network.Distributed.System.Security. (NDSS), Feb. 2008.
[4] J. D. Lafferty, A. McCallum, and F. C. N. Pereira, "Conditional random fields: Probabilistic models for segmenting and labeling sequence data," in Proc. 8th Int. Conf. Mach. Learn. (ICML), 2001.
[5] S. Philips, E. Kao, M. Yee, and C. Anderson, "Detecting activity-based communities using dynamic membership propagation," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Mar. 2012.
[6] J. Zhang, P. Porras, and J. Ullrich, "Highly predictive blacklisting," in *Proc. 17th Conf. Security Symp.*, 2008
[7] M. P. Collins and M. K. Reiter, "On the limits of payload-oblivious network attack detection," in Proc. 11th Int. Symp.Recent Adv. IntrusionDetection (RAID), 2008.
[8] M. Roesch, "SNORT—Lightweight intrusion detection for networks," in Proc. 13th LISA Conf., 1999.
[9] Haojin Zhu, Suguo Du, ZhaoyuGao, Mianxiong Dong and Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, JANUARY 2014.
[10] K. M. Carter, N. Idika, and W. W. Streilein, "Probabilistic threat propagation for malicious activity detection," in Proc. IEEE Int. Conf.Acoust., Speech Signal Process., May 2013.
[11] RuifangLiua, Shan Fenga, RuishengShib,, WenbinGuoa, "Weighted graph clustering for community detection of large social networks," in 2nd International Conference on Information Technology and Quantitative Management, ITQM 2014.