International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

PTP Method in Network Security for Misbehavior Detection Using Entropy

Neha Pathak[1], R. S. Apare[2]

[1]Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

[2]Professor, Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

Abstract: ***A PTP method in network security for misbehavior detection system is a method of detecting malicious misbehavior activity within networks. The System detects the malicious node and blocks them by adding into Blacklist. Malicious nodes are the compromised machine present in the network, which performs the task given by bot server i.e. it does not forward the legitimate message to another node in network or send some other message to neighbor node. This system is based on Probabilistic threat propagation and Entropy. When the monitored network runs in normal way, the entropy values are relatively smooth. Otherwise, the entropy value of one or more features would changes. This proposed scheme is use 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) we consider the task of detecting malicious node in network.***

Keywords: Botnet, Blacklist, Community Detection, Graph Algorithms, Network Security.

1. Introduction

Network detection is the main objective in many graphs applications like graph partitioning, mesh segmentation and community detection [3], network anomaly detection [10]. The Malicious or bot system is responsible for many attacks on the networks security. A week system is always vulnerable to all kinds of attacks. Such malicious or compromised system within the network is a bot system, the network of bot system is also known as a botnet. These botnets system performs the task assigned by the bot server and fluctuate the normal working of the system. Because of the increase of botnets, a newer detection technique has developed which view the host network activity to detect the infective behaviour of nodes. The behaviours or activity of multiple nodes can be aggregate to perform spatial anomaly [6] detection which considers the relationship between nodes with other nodes.

To detect the known malicious nodes, there are some methods which use either internal network detection or blacklist system in the external network [14]. By using these methods, an analysis can be performed to identify host communication with the known malicious nodes on network traffic. The existing system has shown that malicious node activity can be determined and then block them. But some time a malicious node can modify their pattern and can fool the system but proposed system has administrator which block the system permanently so that malicious node cannot perform any other task only legitimate user can recover the system by some registered key which known by only him. A method for the detection of malicious nodes on a network, independent of their activities, shows the fact that malicious activity tries to be localized. Suppose for any tip graph 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 [11] is not compute for each node of a network. In the probabilistic threat propagation [12] (PTP) the probability of a node being malicious is proportional to the level of maliciousness of its neighbor nodes and by applying entropy [2] we can calculate the randomness of a system.

2. Related Work

Paper [2] has showed the use of entropy to detect the DDOS attack using IP Trace back scheme against DDOS attacks based on entropy variations. This scheme is implemented by storing the information of network flow between systems at the routers. After this step, it performs pushback tracing procedure. The Trace back algorithm first identifies its upstream router where the attack flows comes from and then submits the Trace back request to the related next neighboring router. This procedure continues the process until the most far away zombies, or malicious are found.

Paper [3] uses Bayesian framework for network detection, which detection algorithm is based on random walks on graphs. The system detects the threat present in network using partial observations of their activity. To define the algorithm a graph is used in this paper, here a link is provided for well-known spectral detection then the equivalent of the random walk and harmonic solutions is applied to prove the Bayesian formulation.

In paper [4] an iTrust system represents which use to detect malicious and selfish behaviors in delay tolerant networks (DTNs). iTrust is a probabilistic misbehavior detection scheme, which uses a Trust Authority(TA) to judge the node behavior. Schemes (iTrust) reduced the detection overhead effectively. Method firstly introduced data forwarding evidences for general misbehavior detection. The proposed

framework is not only detected various misbehaviors But also a compatible to other routing protocols.

In the paper [5] an effective approach is presented to detect activity based communities by propagating membership in between the neighboring nodes. To show the utility of a method, a local implementation is use. These local implementations are checked for community detection by given starting node and then apply it to on two varied data set.

In this Paper [6] a method is represented which constructs the blacklists for large scale network security log sharing infrastructure. This method 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 prefiltering preprocesses the security alerts supplied by sensors across the Internet. The processed data were then fed into two parallel engines, and the second stage finds the malicious sources using a severity that measures their actual maliciousness. The related ranking scheme is used to severity score are combined at the last step to generate a final blacklist for each contributor.

In Paper [7] a low rate distributed denial of service attack has presented. In this system, a probability distribution is used to quantify the differences of network traffic. The paper has used two new information metric as generalized entropy metric and information distance metrics. Generalized entropy metric detects an attack by measure the difference between legitimate traffic and attack traffic. Information distance metric uses Kullback-Leibler approach to enlarge the distance and then find the optimal detection.

In Paper [9] a spam detection method has presented. This paper scheme presents that mail servers were not made with spam email message. The paper has argued that the architecture of email server design optimize the performance. It represents that to increase the performance of server three major component i.e.,, the concurrency architecture, the disk I/O, and DNSBL lookups, can be optimized by exploiting the new –ecommon case" workload.

In this Paper [13] 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 the network. It can also provide administrators with enough data to make decisions on the action of suspicious activity. Snort is a cost efficient tool.

3. Proposed Work

The proposed system will help to system administrators in automatically identifying the compromised machines in their networks. The proposed system will work as the 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 the system will select another path for transfer and finally messages will be forwarded to their destinations. As shown in figure 1. The architecture of the proposed system works with the help of following parts:

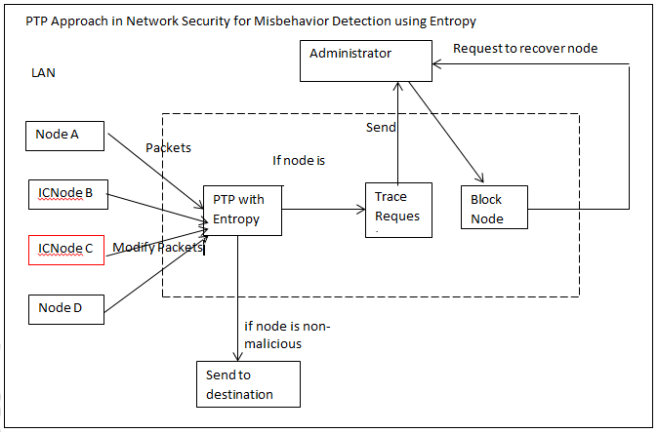

Figure 1: System Architecture of Proposed System

3.1 Network Initialization module

In this module network is initialized to show the result where an administrator can add the nodes and remove the nodes. This module is basically to create the network for the determination of malicious behavior attack detection.

3.2 PTP Algorithm For Malicious Detection:

In this module, a PTP method employed, which detect the present malicious node by calculating the threat level and also their neighborhood node. Then Entropy variance calculates which analyzes the distribution characteristics of alert. Here PTP system creates probability of each node and the possibility of them being benign or maliciousness

3.3 File Scanner System

The trace back algorithm first identifies its upstream routers where the attack flows came from, and then submits the trace back requests to the related upstream routers. This procedure continues until the most far away malicious are identified. Then system identifies source attacker and blocks the source attacker from the current network access.

3.4 Blocking System

The trace back algorithm first identifies its upstream routers where the attack flows came from, and then submits the trace back requests to the related upstream routers. This procedure continues until the most far away malicious are identified. Then system identifies source attacker and blocks the source attacker from the current network access.

3.5 Recovery System

The only legitimate user can recover the node by authentication; the node need to send its key value to verify

the admin then admin validate key by matching it to present in the database for respective node.
During malicious detection using PTP system the following steps are followed,

1) Initially sender send packet to the receiver.
2) Shortest path select between source to receiver.
3) IF (receiver ! receive packet)
4) PTP detect the malicious node present in the path between source to 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 receiver.
8) Receiver receives the packet.

4. Mathematical Model

Set Theory Analysis

A] Identify Nodes:-
N is the main 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,_,_ are malicious node

C] Identify the neighborhood node of malicious node
Nr= {n1,n2,n3…….}
Where n1, n2, n3 are neighbor node of 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 on node x_i as the probability of maliciousness is as:-

$$P(xi, G) = \sum_{j \in N(xi)} wijP(xj|xi = 0; G)$$

Where $N(x_i)$ = Neighborhood of x_i , $e_{ij} \in E$ and w_{ij} = weight of the edge e_{ij}
Initially current node = 0
Initialization of PTP with the set {M} – Known to be malicious

Apply priori probabilities P (x € {M}) = γ
γ € [0,1]

Other node initialized to P(x €/ {M}) =0 at each iteration
Weight matrix W can be computed via $w_{ij} = f(x_i , x_j)$.

Entropy Variation Can be calculated by :-

$$H(F)=H(p_1, p_2, \ldots, p_N)=-\sum_{i=1}^{N} p_i \log p_i.$$

In this formula H(f) is the entropy variance , Pi is the probability.

5. Result and Discussion

Table 1: comparisons of existing system and proposed system with respect to malicious message forwarded

System	Total Node	Non malicious msg forwarded in network	Malicious msg forwarded in network	No. of malicious detected	Exact block Node
PTP	4	4	6	1	0
PTP using Entropy	4	3	0	1	1
PTP	6	6	7	1	0
PTP using Entropy	6	6	0	1	2

As shown in table1 comparison of system in terms of malicious and non-malicious messages forwarded into the system. PTP system allow node to forward the malicious message to their neighbor while PTP system using Entropy does not allow any node to send malicious message.

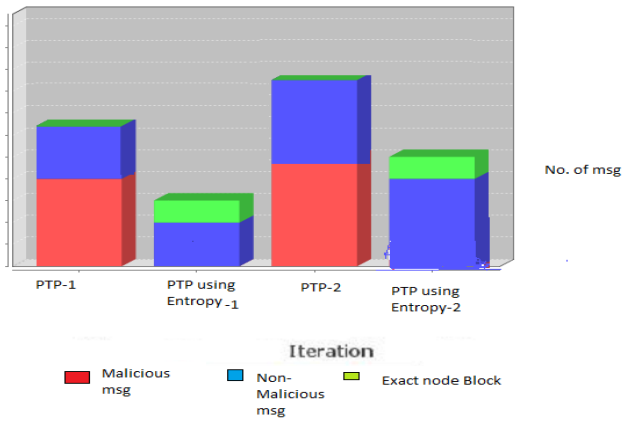

Figure 2: Comparison with existing system and proposed system.

As shown in Fig 2 comparison between existing system and proposed system. Existing system will allow malicious node to send malicious message and also it does not block the exact node while proposed system will not allowed sending malicious or infected message and also blocking network to perform any activity

Table 2: flow calculation when no malicious node present at ICNode.

Node	Packet	TimeStamp	TimeInterval	Entropy
NodeA	2	2	3	3.29583686600433
ICNodeB	2	2	3	3.29583686600433
ICNodeC	2	2	3	3.29583686600433
Node D	2	2	3	3.29583686600433

Table 2 show the calculation of flow when no malicious nodes were present. Table shows the entropy value calculated

at nodes. When no malicious nodes were present then the value of entropy would be 3.2958368660433.

As shown in figure 3. at normal condition when no malicious node were present then for a particular time interval the value of Entropy is 3.29583686600433 approx. in the figure up cylinder shows that the value of entropy is the same at all the node.

Table 3: Flow Calculation when malicious node present

Node	Packet	TimeStamp	Time Interval	Entropy
NodeA	2	2	3	3.29583686600433
ICNodeB	2	2	3	3.29583686600433
ICNodeC	2	9	9	19.775021196026
Node D				

Table 3 show the calculation of flow when a malicious node was present at ICNodeC. When malicious nodes were present then the value of entropy would be 19.775021196026.

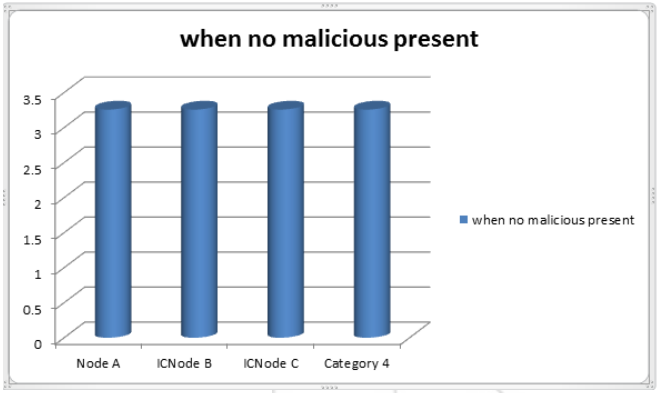

Figure 3: Entropy Value at nodes when no malicious present

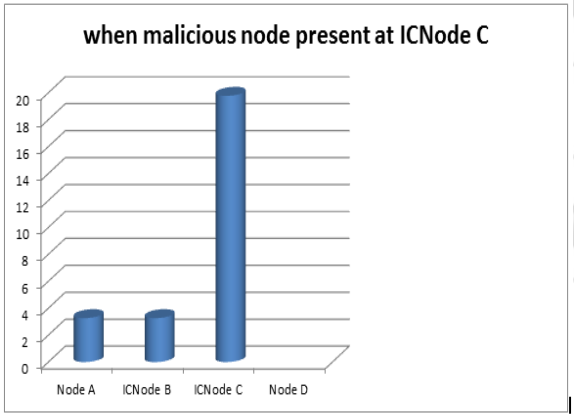

Figure 4: Entropy value at ICNodeC due to malicious present at ICNodeC**.**

After estimating the first task now, to find out the fluctuation for normal situations by adding an attacker at any one of the node. As shown in figure 4 entropy values is increase at the ICNodeC so the Up cylinder at ICNode C shows the entropy rise.

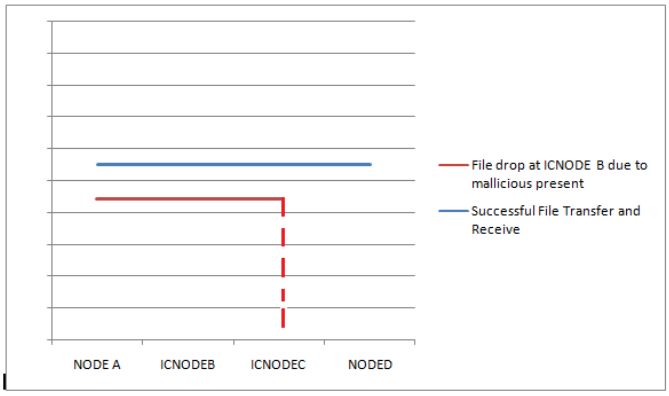

Figure 5: File transmits and receive.

In fig 5 straight line shows successfully file send by nodeA and received by nodeD while red line shows file drop at node C due to presence of malicious node.

6. Conclusion

A effective method for malicious detection was presented in the paper. Probabilistic Threat Propagation is an iterative approach for graph analytic. It determines malicious node in network by statistical probability and entropy. It is difficult to find threat origin to avoid node threat levels being increased uniquely depend on their network presence. PTP outputs approximations of true statistical probabilities that are easily interpretable by an analyst. PTP can use in network security for botnet detection and prediction of malicious domains.

7. Acknowledgment

I would like to thank my guide Prof. R. S. Apare for his valuable feedback, constant encouragement and exemplary guidance throughout the duration of the paper. His suggestions were of immense help throughout this paper.

References

[1] V . Sushma Reddy, K.Damodar Rao, SowmyLakshmi, ―Efficient Detection of DDOS Attacks by Entropy Variation,‖ in IOSR Journal of Computer Engineering (IOSRJCE) Volume 7, Issue 1 NOV-DEC 2012.

[2] Steven Thomas Smith, Edward K. Kao, ―Bayesian Discovery of Threat Networks,‖ in IEEE Transaction on Signal Processing, Sep. 2014.

[3] D.Suguna Kuamari, Bala Veeravatnam, P.Sowmya ,―Efficient Trust Establishment in Delay Tolerant Networks by Misbehavior Detection Scheme,‖ in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 11,November 2015.

[4] Haojin Zhu, Suguo Du, Zhaoyu Gao, 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.

[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] S. Philips, E. Kao, M. Yee, and C. Anderson, "Low-Rate DDoS Attacks Detection and Trace back by Using New Information Metrics," in IEEE Transactions on Information Forensics and Security, VOL 6, June 2011.
[8] 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.
[9] Abhinav Pathak, Syed Ali Raza Jafri and Y. Charlie Hu, "The Case for Spam-Aware High Performance Mail Server Architecture," in 2nd International Conference on Information Technology and Quantitative Management, ITQM 2014.
[10] 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.
[11] 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.
[12] Kevin M. Carter, Nwokedi Idika, and William W. Streilein "Probabilistic Threat Propagation for Network Security", IEEE Transactions on Information Forensics and Security, Sep 2014.
[13] M. Roesch, "SNORT—Lightweight intrusion detection for networks," in Proc. 13th LISA Conf., 1999.
[14] Neha Pathak, R.S.Apare, "PTP Approach in Network Security for Misbehavior Detection," in iPGCON-2015.