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

PTP Approach in Network Security for Misbehavior Detection Using Entropy

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

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

[2]Assistant Professor in Dept. of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

Abstract: ***A PTP approach 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 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 Security is a special field of computer networking. It secures a computer network infrastructure. In Network security network 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 categorize 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 behavior of nodes. The behaviors of multiple nodes can be aggregate to perform spatial anomaly [3] detection which considers the relationship between a node with other nodes.

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 localize. 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] (PTP) the probability of a node being malicious is proportional to the level of maliciousness of its neighbor nodes.

2. 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 may communicate with other 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 during a given time window. There is a probability pair of bots 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 bots 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 show 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. There are two methods were used for membership propagation: Static and dynamic membership. 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 prefiltering, 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 attack, the attacker's communication with multiple hosts is an attempt to determine what services they are running. In this paper a method is used to evaluate 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 an attacks present in 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 (iTrust) 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 to other routing protocols. Secondly it introduced a probabilistic misbehavior detection scheme by adopting the Inspection Game.

3. 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 on the graph and *E* shows the set of edges between nodes. Now If there exists an edge *ei j* ∈ *E* then we can say that there exists some quantifiable *direct* relationship between nodes *xi* and *x j* in *G*. The relationship strength can be represented by the weighting *wi j* on given *ei j*. If there exist a *xk* in the graph for which *eik* /∈*E* and has consequences on a node *xi*. Then this type of relationship called indirect relationship.

For our purposes of this paper we consider two communities for the detection problem: malicious and benign. We considers 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.

4. 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 router in the network as LAN. Whenever any node wants to send message to other 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 those 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:

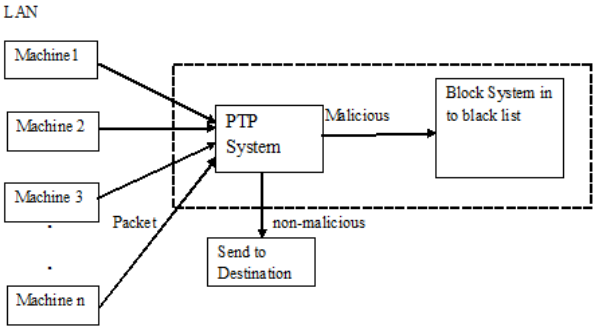

Figure 1: System Architecture

4.1 Network Initialization module

In this module network is initialized to show the result where administrator can add the nodes and remove the nodes. This

module is basically to create network for the determination of malicious behavior attack detection.

4.2 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

4.3 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 block the source attacker from the current network access.

4.4 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 block the source attacker from the current network access.

4.5 Recovery System

Only legitimate user can recover the node by authentication, node need to send its key value to verify the admin then admin validate key by matching it to present in 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.

5. 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.

6. Result and Discussion

In this section the performance is evaluate the effectiveness and efficiency of the entropy variation based on IP Trace back mechanism here the First task is to show that the flow entropy variation is stable for non –attack.

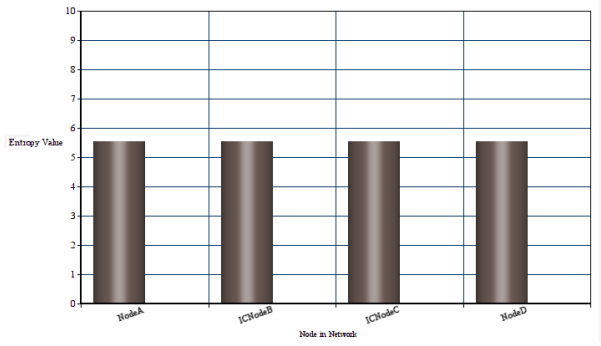

Figure 2: Entropy Value at nodes when no malicious present

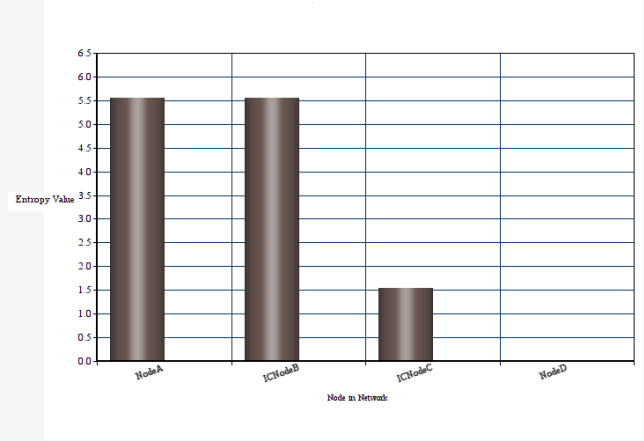

Figure 3: Entropy drop at ICNodeC due to malicious present at ICNodeC**.**

After estimating the first task now, to find out the fluctuation for normal situations by adding an attacker at any one of the node, there by the second task is to demonstrate the relationship between the drop of flow entropy variation and the increase of attack strength, entropy rate due to the attacker at ICNodeC.

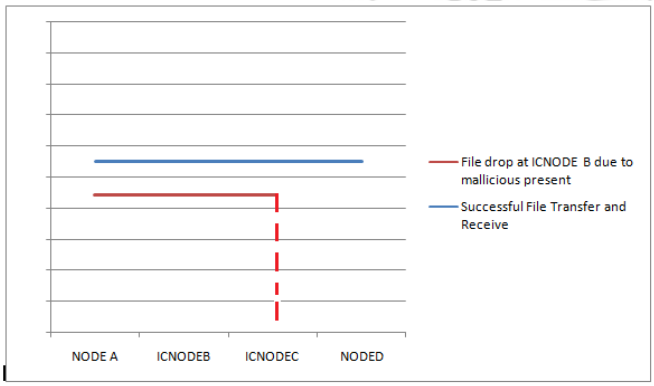

Figure 6: File transmit and receive.

In fig 4 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.

7. Conclusion

A novel method for malicious detection was introduced in this 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.

8. 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] Kevin M. Carter, Nwokedi Idika, 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. Intrusion Detection (RAID)*, 2008.
[8] T. Yu, R. Lippmann, J. Riordan, and S. Boyer, “EMBER: A global perspective on extreme malicious behavior,” in *Proc. 7th Int. Symp. Vis. Cyber Security*, 2010.
[9] M. Roesch, “SNORT—Lightweight intrusion detection for networks,” in *Proc. 13th LISA Conf.*, 1999.
[10] 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.
[11] 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.
[12] Ruifang Liua, Shan Fenga, Ruisheng Shib,, Wenbin Guoa, “Weighted graph clustering for community detection of large social networks,” in *2nd International Conference on Information Technology and Quantitative Management, ITQM* 2014.