NSME: A NETWORK SAFETY MANAGEMENT ENGINE TO SPOT AND FILTER MALICIOUS IP CLUSTERS

[1]S.KIRUTHIKA SRI, [2]S.C.PUNITHA

[1]RESEARCH SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE, PSGR KRISHNAMMAL COLLEGE OF ARTS & SCIENCE FOR WOMEN, COIMBATORE, INDIA
[2]ASSOCIATE PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, PSGR KRISHNAMMAL COLLEGE OF ARTS & SCIENCE FOR WOMEN, COIMBATORE, INDIA

Abstract - Detecting and discriminating malicious and gentle nodes in the network is the most convolute task, which has undistinguishable behaviors, and a set of nodes which has different behavior is often possible to be in a same cluster. Finding the node behavior and clustering them in a malicious cluster based on the behavior analysis is a major research to enhance the network security. We demonstrate that it is often possible to discover such clusters and finding optimal response to thwart the further interruption by processing network logs collected at various network configurations. Obviously, not every node and clusters exposed as malicious. Yet, we show that malicious clusters can accurately be distinguished from benign ones by simply using episode segmentation and a predictive IP blacklist. In this paper, we first propose a novel network safety management engine to spot and filter such malicious behavioral IP and IP clusters in the network. In this paper, we concentrated on different types of malicious behaviors like service interruption, spreading spam, spoofing and misusing data in the network etc., Based on the behavior analysis, behavior score is calculated and the score threshold determines the predictive black list. Later the highly predictive blacklists are used to find the malicious cluster. Additionally, we performed the counter measure selection for the node behavior and its behavioral score. We significantly get better results in terms of precision and recall. Furthermore, we produced an episode detection process with event id and its sequence for fast behavior analysis. The proposed malicious detection process and clustering process improves the precision and recall. Finally, we demonstrate the efficacy of the proposed scheme using network log events which are captured from the trace files using the NS2 tool.

Keywords - Malicious IP Cluster, Network Security, Botnet, DOS attack, Countermeasure, Behavior Analysis.

I. INTRODUCTION

Numerous malicious activities on Computer networks have grown tremendously with complex operations. These activities are carried out by the set of IP addresses, which may spread spam, malicious code, and performing different types of attacks [1]. This kind of malicious behavior can be performed individually or by group of IP addresses, which is called as botnet [2]. This malicious behavior leaves some noticeable traces or issues at assorted network nodes. So, defender uses simple and effective data analysis methods to group such IP addresses. In this case, the attacker often utilizes the group of nodes with its IP addresses to log into the compromised online accounts to perform the illegal tasks [3]. Analyzing the login events for a specific account, which have performed from several IP addresses are then clustered. This process allows the defender to identify the set of nodes, which are involved with the malicious activity in the network. In some scenario, the analyzed and clustered IP addresses are non-malicious. Thus, it may contain non-malicious IP addresses and gateways. This case can be illustrated with the mobile network or a corporate network, where the same set of users allowed to login to their accounts. In reality, there are huge other cases contains the nodes in the malicious IP cluster. In network, malicious activity can be referred by many ways, and these are known by several attack names such as Denial of Service (DOS) [4], spamming [5], spoofing [6], replay attacks [7] and data modification attacks [8]. So, spotting malicious node and clusters with complete behavioral analysis is much important. However, the behavior analysis with attack intension is always a complex task and it needs many log and training data.

In this paper, we concentrated on spotting malicious node and malicious cluster by analyzing the IP blacklists and processed network logs. But, sometimes the blacklist IP list is invalid and inaccurate. Finding malicious node from potentially collected network log and restoring the IP black list with optimal counter measure selection is the ultimate aim of this work. Based on this perception, we developed a novel Network Security Engine (NSE), which contains a set of schemes to thwart, detect, and cluster malicious node with selecting optimal countermeasures. The scheme identifies malicious cluster by analyzing the network interactions like network flow records, communication records. We initially crawls the node activity from the network log, and clusters the node by its behavioral score. Then the blacklist and white list aware re-clustering is performed. Finally, for new node or dynamic node in the network will be analyzed with the interaction between blacklist nodes. We demonstrated the NSF result in terms of accuracy and time. Instead of random guessing and statistical analysis, the work utilized complete behavioral analysis and similarity finding functions for better result. We have the following contributions:

- We developed a novel Network Safety Management Engine (NSME) for detecting malicious node, malicious IP cluster from network flow logs. This also validates the nodes before re-clustering from the black list and white list.
- We theoretically analyzed the node behavior analysis strategy and developed a new network flow analysis technique to accurately determine the node behavior using **Optimal Rule Precedence (ORP) algorithm**. From the node behavior the black and white lists are created. The malicious behaviors are inserted in to the Black list (BL) array and legitimate nodes are moved to white List (WL) array. To perform the BL process, we used **highly predictive blacklist (HPB) algorithm**.
- We developed a list of countermeasures to handle such malicious IP and cluster and to reduce the further malicious behavior.
- The countermeasure part includes a service restriction mechanism after detecting the malicious activity score by using **ACL (Appropriate Countermeasure List) algorithm** for effective access limiting process.
- Finally the simulation is carried out to spot and response malicious node using NS2 simulation tool.
- The rest of the paper is organized as follows. In Sections II, we give a brief outline of the existing works related to the malicious node detection in computer networks. In Section III, we give the details about the NSE with the list of algorithms. In Section IV, we demonstrate the proposed scheme working procedure in a simulation tool. In Section V we discuss the performance of the proposed scheme. We present conclusions and future work in Sections VI.

II. MALICIOUS IP CLUSTER DETECTION METHODS

Numerous studies in the literature have proposed to spot malicious node and IP. Malicious node is termed with different types of attacks. The most common and frequent attack in the wireless network is DOS attack, DOS attacks are detected using Activity monitoring and Change-point detection techniques. Authors in [9] presented a simple and robust mechanism which is named as change-point monitoring (CPM) to detect denial of service (DoS) attacks in the network. The main idea of the CPM technique is acquiring traffic patterns to perform the detection mechanism. Instead of every feature, it uses only a few variables at the time of behavioral tracking. This feature incurs low computation overhead.

Behavior Similarity has considered as the main point to address the malicious IP in the literature, so based such assumption, authors in [10] [11], presented a technique to find malicious IP group. And the author proved that the compromised web accounts are utilized by similar sets of IP addresses. Authors in [12] demonstrated the malicious IP spot techniques by the transaction similarity, where the spamming IP addresses often send data to the similar domains. Various detection methods are used in the literature based on the similar network behavior which is explored in several other networks.

Authors in [13] show that when a node affected by the command and control activity by the Botnet, that has a strong communication with each other. This makes the different malicious activity in the network, so author captured the network flow records at the routers and analyzed the malicious cluster. Botnet members may always have a similar network behavior and this can be compared by analyzing the features of the others [14]. This scheme has several limitations like it does need the extended and detailed observation technique for web application service providers. A new detection scheme is designed for web application service providers in [10]. But, the scheme detects the group of users instead of the group of IP addresses. The behavior analysis was performed in this scheme to detect the malicious user group. But due to its individual detection, it is treated as much costlier.

In the proposed scheme, we detect malicious clusters of IP addresses in the network by utilizing simple behavior analysis techniques and black list and white list analysis.

Similarly, in [15], authors focused on detecting malicious IP cluster rather than the malicious user detection. However, the scheme only performs the detection strategy rather than the response system. So the further attacks and vulnerabilities can be avoided. While considering this scenario, authors in [16] proposed a novel intrusion prevention, detection and response system for secure content delivery networks. In this scheme, the author suggested several countermeasures for the intrusion by using game theory concepts.

However, as mentioned before, our focus in the proposed work is on both malicious user and IP address detection with the optimal counter measure selection process. Our concentration on wireless networks, so, additionally other sets of issues and restriction arises based on the energy and resource restrictions. Even though there are huge restrictions on resource utilization, we are still able to present high detection and response accuracy in the proposed work.

In this work, we developed a network security engine which not only detects the malicious IP cluster; it also performs necessary response on them. We also present a mathematical analysis and simulation results to understand the proposed work.

III. PROPOSED SYSTEM

Severe network security threats are carried out by group of IP addresses. It has several reasons behind this, DOS attacks and spamming require several hosts to perform the attack and that can be effectively improved by dividing the load over several hosts. Utilizing numerous hosts to perform the desired attack has some limitations like it can be detected easily. The group of IP addresses is used as a source for attack in the botnet to perform the malicious activity, these bots are compromised and later the identities are spoofed to perform such attack. Like this scenario, every attack is made on the network. In this section, we first present three samples in Table 1 to understand the attacks, to discuss how IP addresses utilized by a malicious activity leave traces at various vantage points in the network and hence can be clustered together. After that, we present a novel clustering scheme which can be used under various scenarios.

Malicious Activity type	Dataset Observed In	Similarity Measure Between IPs
DOS attacks	Network Events observed at the router	Number of common transaction performed
Botnet command and control	Network flow records captured at edge routers of a network	Number of common IPs or domains communicated with
Backdooor attacks	The back door can either recognize some special sequence of input, or is triggered by being run from a certain user ID which is then granted special access rights accordingly.	Similar behavior from other nodes.
Replay attacks	Network log helps to detect the Delay in data transmission and finds delayed response.	Number of packets delayed.

Table 1.Example Cases of Malicious IP Clusters Along With behavior that they can be observed in and potential similarity measure that can be used in work

The above examples on similarity analysis are generated with different types of attack scenario. This clearly shows, the list of nodes collectively carry out same type of task can be easily recognized. But this is not always happen in all types of malicious behavior. The authors in [17], represents the blacklist aware clustering technique to detect the malicious IP addresses. However, the other type of attacks may not participate with huge set of nodes rather it compromise a single heterogeneous node. In the proposed work, we concentrated on several security related vulnerabilities and malicious behavior. So an effective network security management engine is created. This section initially defines the overall architecture and flow of the NSME then each technique discussed in the sub section.

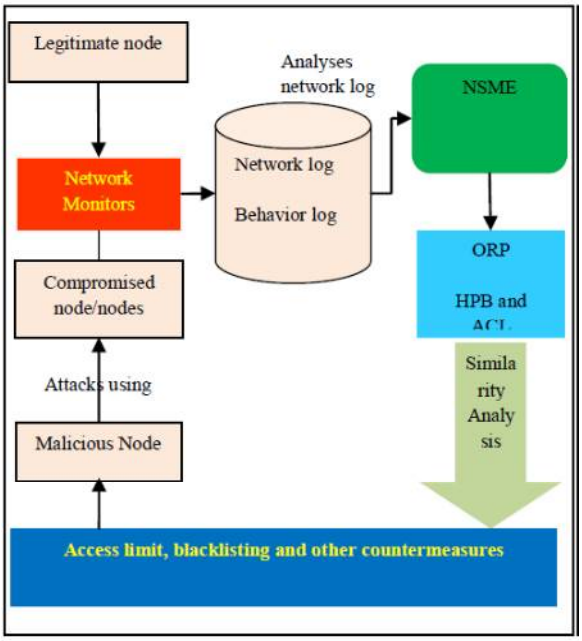


Fig 1. NSME architecture

The fig1.0 shows the architecture of our proposed system. The nodes and its behaviors are analyzed from the network monitor process, by using the optimal rule precedence algorithm; the attacks will be identified by its behavioral data. Then an optimal countermeasure will be selected to the malicious node.

A. Malicious_IP Behavior Analysis (MBA):

The behavior analysis is performed from the transaction log. Network monitoring techniques are used here. In this process, the network events are collected and stored in the log. The events are set of actions, which collected from the NSME. The followings are the list of events with described with the event id. Instead of storing every transaction, the network monitoring system stores with the event id.

Event Id	Event Name
C	Server connection establishment
S	Session creation
N	Node initialization process
L	Authentication process
B	Authentication success and RREQ (Route Request)

A	Authentication failed process
R	Route selection process
D	Network discovery process
M	Acknowledgements
N	Compromised
W	Message sending process
J	Message Receiving process

Table 2. Event Description Table

The table 2 shows the events and its identification number used in the implementation. This contains a set of events and its id. The every event is created to find the node action at every point. The system monitors every event and converts into the event id and stores in the database log. After that this performs the correlation process, which helps to aggregate the events and finds the association between events. This process is necessary to find the malicious sequence events from the log. So, initially we correlate and prune the frequent and non-malicious events and converts into the priority based episodes. The episodes are the collection of events, which has been collected at every specific epoch.

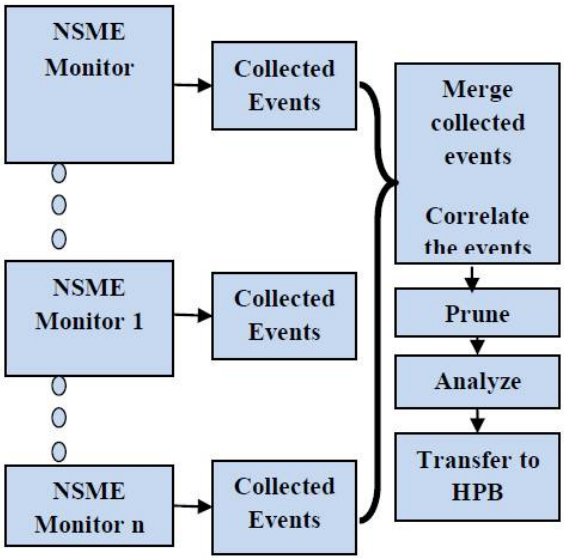


Fig 2.0 over All Process of the Proposed System

The fig 2.0 represents the event collection, correlation and analysis process to detect the malicious node M. Here correlation and aggregation functions are used, the **correlation function** gives the statistical correlation between random variables, contingent on the spatial or temporal distance between those events. If one considers the correlation function between events representing the same quantity measured at two different points then this is often referred to as an autocorrelation function, which is made up of autocorrelations. For possibly distinct two events E(*x*) and E(*y*) at different point's x and *y* of some space, the correlation function is

C(x,y)=corr(E(x),E(y)),

{\displaystyle C(s,t)=\operatorname {corr} (X(s),Y(t)Where, {\displaystyle \operatorname {corr} }corr is described in the above formula is represents the process of correlation. In this definition, it has been assumed that the stochastic variables are scalar-valued. After correlating the infrequent and non-malicious events are eliminated, the filtered events are transmitted to the HPB process. The collection of events are listed based on the epoch is called as an episode. The serial process of every node in the network is analyzed to detect malicious event and similar events by more nodes.

Epoch→	1	2	3
Node 1	CSNLA	CSNLBN	CSNLBNW
Node 2	CSNLB	CSNLBR	CSNLBRW
Node 3	CSNLA	CSNLBN	CSNLBNW
Node 4	CSNLA	CSNLBM	CSNLBNJ

Table 3 Serial episodes

From the collected and potential episodes from network log files, the analysis is performed. This is very difficult to analyze the whole network log file. So, effective epoch analysis techniques are used. Here the table 3.0 shows the episodes and event id collected for four nodes. The events occurred in the first episode for node 1 is CSNLA, which means the node 1 is successfully authenticated. The event id can be refereed in the table 2.0. So in every time interval, the episodes are mined and this implies the activities of the node. Using the episodes, we can find the malicious event and malicious events which are similar among nodes. From the table 3.0, the events of node 2 is legitimate, but the node1,2, and 3 have some misbehaves in every episode. The similarity between the nodes can be used to detect malicious cluster. From the example, the node 1and node 3 are having similar activities so, the both comes under a same cluster.

B. Highly Predictive Blacklist (HPB) algorithm using Behavioral score:

The system receives the initial cluster from the malicious event mining process which further incorporates with an automated re-clustering phase to remove unreliable event contents, later a source ranking phase is used in which node are prioritized on episodes, and finally a severity analysis process is performed in which attacker priorities are adjusted to favor attackers whose alerts mirror known malware propagation patterns. The system constructs final blacklists after every set of episodes. These black lists are used at the time of service discovery.

Algorithm: MBA+HPB+ORP

The NSME contains three different types of algorithms, where the three algorithms are performed iteratively to produce the final result, so this section shows the overall process and steps included in the security engine. The notations are given below.

Notations: Tp- Threshold point for behavior analysis, Bs-Behavioral score, Ts-Total score, N-node, n-number of nodes, Ts-total score.

Step 1: node initialization, n is the total number of nodes and N is the Node id.

Step 2: collect node events from the network monitor phase and convert into episodes with epoch using the following function. Here "x" is episodes and "a" is the events of every node.

$$Episodes\ (x, a) = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

Step 3: read event description list E_d. and match the collected node's event for every node N.

Step 4: calculate the behavior score from the malicious event list by

(a) For ever node N in n do
{
(b) For every node Ni assign score level=100
(c) Ni(Ts=100)→Ts total score
(d) Rs=number of malicious events Mi* Score per event Si
(e) Behavioral score Bs=(total score Ts(Ni)-Rs
(f) If (Bs<Tp)
Add to black list (Bl[i]=Ni)
Else
Add to white list (Wl[i]=Ni)
i=i+1
}

Step 5: calculate similarity between an IP with existing BL cluster.

Step 6: select counter measure C from the list L using ORP

Counter measure list includes L[n]={access limit, service time limit, transaction priority, resource allocation tc}

Step 7: update cluster

Step 8: end.

From the node initialization process to cluster updating process is performed in the above algorithm. Our work has three major phases, but the simple algorithm proves the overall three phases in a single format. From the algorithm, ORP processes are described briefly. But the process of ORP selects optimal countermeasure based on the predefined rules.

IV. EXPERIMENTS

In this section we demonstrate how the proposed system can be used to identify malicious clusters of IP addresses from the behavioral and network log analysis. The experiments utilized the network log, which has been collected from the simulation process using NS2. The log which has been collected is converted into the episodes with event id. This contains the legitimate and malicious node transactions. The malicious behavior such as DOS, spamming, spoofing, data modification and replay attacks are demonstrated and the relevant network log is generated with the attacks. Our main focus is on three phases such as malicious behavior analysis, effective Black listing and white listing and malicious IP clustering with counter measure selection. Unlike the previous work [base paper], we are not particularly falls on only finding malicious IP clustering process, but finding optimal counter measure is also performed. While the proposed scheme can potentially identify malicious IP clusters and suggest optimal response using ORP algorithm, there is a huge responsibility to gather necessary dataset. Such process is domain specific, based on the application the response may vary, which is considered as outside the scope of our experiments presented in this work.

RESULTS AND ANALYSIS

In proposed system, the comparison process consists with two performance metrics: detection accuracy and Latency. Latency is the time taken for every process in the NSME such as event collection time, malicious event detection, BL time and counter measure selection time. This section performs the comparative study between existing system and the proposed system. This has two types of existing system based on the performance. One is based on the behavior analysis with blacklist technique another one is the black list aware clustering algorithm to cluster malicious IP addresses. The following section shows the summary about the existing work and the proposed work.

Existing Black list aware clustering algorithm (BAC): The existing black list aware clustering algorithm performs the malicious IP clustering process from the black list verification. The scheme used mediocre blacklists to make accurate decisions on clusters of IP addresses. The major drawback of this work is the accuracy level is low. The calculation from the blacklist may obviously affect when the node has wrongly blacklisted. The work is not used the behavioral analysis and blacklisting process. So selection of effective black list is the challenging part. When performing transaction similarities between an IP and malicious cluster, it reveals there is only least and few features are matched with one another, the second issue is, there should be at least some of the IP addresses in a malicious cluster are blacklisted. So due to these issues the detection performance would suffer from any effort by an attacker to break any of these assumptions.

Highly Predictive Blacklist (HPB) algorithm for Malicious IP clustering: the proposed HPB clustering along with the other set of algorithm improves the clustering accuracy. The proposed work eliminates the problem due to the wrong and improper blacklisting.

The comparison between the above two techniques are compared by the following section. To investigate the performance of the proposed scheme with a set of network nodes for the simulation period 300 ms, we repeat each of the above steps with transactions. Based on the traffic and number of nodes the detection time varies. The time analysis is performed only for the proposed system. The precision and recall are calculated and then compared with the existing system. Depending on the traffic and the simulation scenario, on each transaction we end up having a different optimal score threshold ranging from 60 to 100. After performing malicious IP detection and clustering using these scores, we declare the clusters whose standardized score is lesser than 60 as malicious. Recall that, with this threshold, our false positive rate is less than in 30% since the probability of standardized score for gentle IP clusters being less than 60 just by chance is less than 25%.

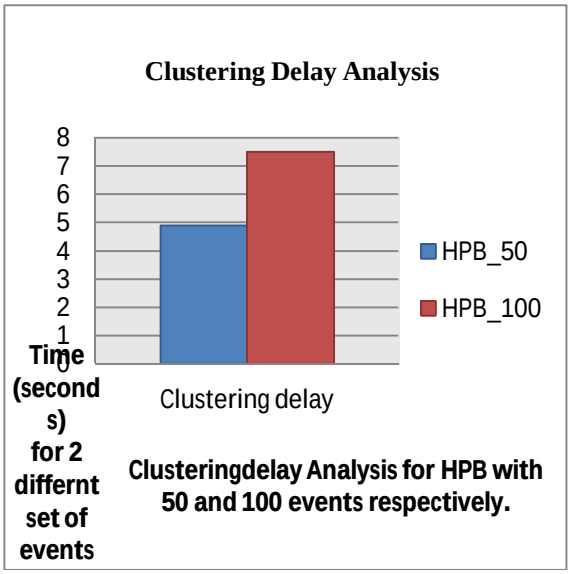


Fig 4 Clustering delay analysis chart

The fig 4.0 shows the clustering time difference between the two set of events techniques. The delay gradually increases when the event counts are huge. The clustering delay includes the event collection delay, pruning delay and clustering delay. In addition, in order to assess the effect of the proposed NSME, we experimented the existing blacklist-aware clustering (BAC) algorithm at the time of clustering. In this scheme we first extract IP clusters using our proposed MBA Method and then deem the resulting clusters with standardized score is less than 60 as malicious. Here we use the same threshold for the proposed HPB scheme, therefore the only difference between BAC and the proposed scheme is the choice of blacklist and clustering method.

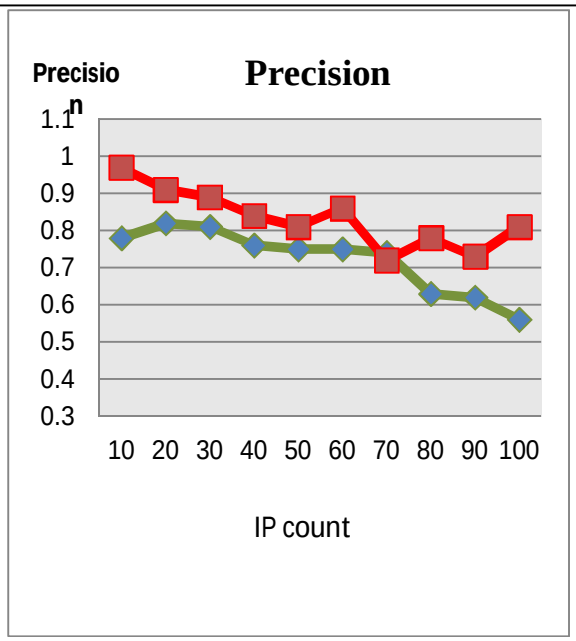


Fig 5 (a) Precision comparison chart

After identifying malicious clusters with both the proposed scheme and the BAC methods, we compute precision and recall values for every event set using trace file reading process. We plot the results in Figure 5(a) and (b). We observe that the proposed scheme performs consistently and significantly better than the BAC method in terms of precision and recall. Also the results the proposed scheme significantly outperforms than the BAC method.

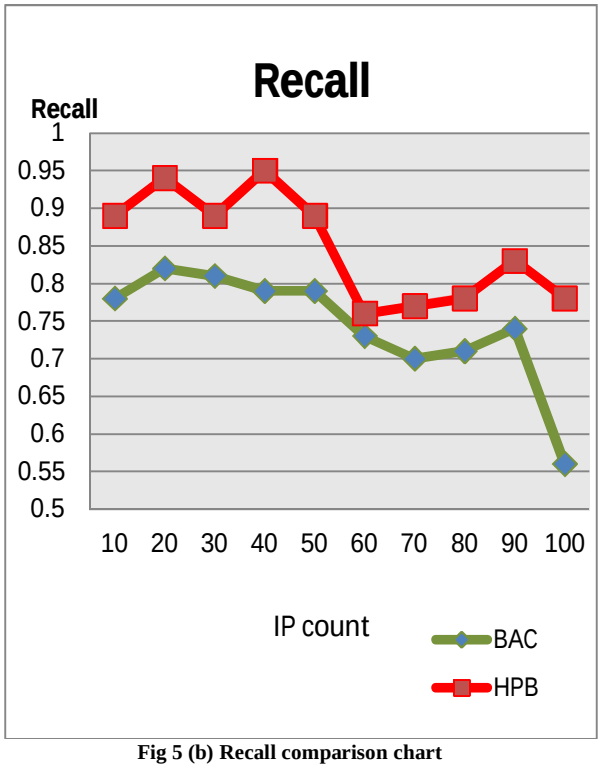


Fig 5 (b) Recall comparison chart

When we closely look at the detected clusters, we observe that the proposed scheme produces much smaller clusters than BAC method does. This is somewhat expected since the proposed scheme ignores the non-malicious and high reputation score nodes to the clusters. In a sense, the proposed scheme prunes non malicious events and IP clusters and outputs the core structures which are highly correlated with the episodes. On the other hand, BAC method involves no such pruning and predictive process, so producing much larger clusters with many more IP addresses several of which are rather loosely connected.

CONCLUSION

Network security becomes one of the major aims in the current scenario due to its immense security threats, which always denies and interrupts the access of the legitimate users. This kind of network threats are categorized into several types of attacks such as DOS, spoofing, spamming etc., in this paper we explored a novel attack protection and response engine for network safety. Initially, we performed smart behavior analysis from the transaction log using episode analysis with event id. This helps to detect whether the specific event or set of events are malicious, and using this event id sequence analysis the similar malicious events can be detected and grouped. After the initial clustering process, the nodes are categorized into Black list or white list. Based on the behavioral score the cluster process is frequently updated. The final process of this work is selects optimal countermeasure for the node based on its malicious score. The response for every malicious activity by individual IP or IP cluster is limiting services, resources, limiting transaction priority etc. In addition, we demonstrated the episodes and its similarity detection process, so the detection of malicious activity became very easy and effective. The basic idea is that, if the true positive rate increases and that are greater than the false positive rate, then the detection accuracy is sufficient. We demonstrated the overall process of the proposed system using trace files of 35 nodes from network simulator. Our results show the proposed system is effective than the existing baseline schemes and blacklist aware clustering scheme. And the main advantage of the proposed system is it supports different types of network vulnerabilities along with the appropriate countermeasures.

REFERENCES

[1] Hansman, Simon, and Ray Hunt. "A taxonomy of network and computer attacks." *Computers & Security* 24.1 (2005): 31-43.

[2] Gu, Guofei, Roberto Perdisci, Junjie Zhang, and Wenke Lee. "BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection." In *USENIX security symposium*, vol. 5, no. 2, pp. 139-154. 2008.

[3] Y. Zhao, Y. Xie, F. Yu, Q. Ke, Y. Yu, Y. Chen, and E. Gillum, "Botgraph: Large scale spamming botnet detection," in Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2009, April 22-24, 2009, Boston, MA, USA, 2009, pp. 321–334.

[4] Carl, Glenn, George Kesidis, Richard R. Brooks, and Suresh Rai. "Denial-of-service attack-detection techniques." *IEEE Internet computing* 10, no. 1 (2006): 82-89.

[5] Sancak, Serdar, Erdal Cayirci, Vedat Coskun, and Albert Levi. "Sensor wars: detecting and defending against spam attacks in wireless sensor networks." In *Communications, 2004 IEEE International Conference on*, vol. 6, pp. 3668-3672. IEEE, 2004.

[6] Duan, Zhenhai, Xin Yuan, and Jaideep Chandrashekar. "Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates." *INFOCOM*. 2006

[7] Syverson, Paul. "A taxonomy of replay attacks [cryptographic protocols]." *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*. IEEE, 1994.

[8] Brachtl, Bruno O., Don Coppersmith, Myrna M. Hyden, Stephen M. Matyas Jr, Carl HW Meyer, Jonathan Oseas, Shaiy Pilpel, and Michael Schilling. "Data authentication using modification detection codes based on a public one way encryption function." U.S. Patent 4,908,861, issued March 13, 1990.

[9] Wang, Haining, Danlu Zhang, and Kang G. Shin. "Change-point monitoring for the detection of DoS attacks." *IEEE Transactions on dependable and secure computing* 1.4 (2004): 193-208.

[10] K. Thomas, C. Grier, and V. Paxson, "Adapting social spam infrastructure for political censorship," in Presented as part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2012.

[11] G. Stringhini, P. Mourlanne, G. Jacob, M. Egele, C. Kruegel, and G. Vigna, "Evilcohort: Detecting communities of malicious accounts on online services," in 24th USENIX Security Symposium (USENIX Security 15), 2015.

[12] A. Ramachandran, N. Feamster, and S. Vempala, "Filtering spam with behavioral blacklisting," in Proceedings of the 14th ACM conference on Computer and communications security, 2007.

[13] S. Nagaraja, P. Mittal, C. yao Hong, M. Caesar, and N. Borisov, "Botgrep: Finding p2p bots with structured graph analysis," 2010.

[14] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection," in Proceedings of the 17th USENIX Security Symposium (Security'08), 2008.

[15] B. Coskun and P. Giura, "Mitigating sms spam by online detection of repetitive near-duplicate messages," in in IEEE International Conference on Communications (ICC), 2012.

[16] Resmi, A. M., and R. Manicka Chezian.;An extension of intrusion prevention, detection and response system for secure content delivery networks." Advances in Computer Applications (ICACA), IEEE International Conference on. IEEE, 2016.

[17] Coskun, Baris. "(Un) wisdom of Crowds: Accurately Spotting Malicious IP Clusters Using Not-So-Accurate IP Blacklists." *IEEE Transactions on Information Forensics and Security* 12.6 (2017): 1406-1417.

★★★