Real Time Attacker Behavior Pattern Discovery and Profiling Using Fuzzy Rules

K. Narasimha Mallikarjunan[1], S. Mercy Shalinie[1], G. Preetha[2]

[1] Department of Computer Science and Engineering, Thiagarajar College of Engineering, India
[2] Department of Computer Applications, Fatima College, India
{arjunkambaraj, shalinie}@tce.edu, ppreetha.2009@gmail.com

Abstract

Computer security investigation would benefit from more information about the characteristics of the human attacker behind a security incident. Present security mechanisms focus on the characteristics of attack, rather than that of the attacker. Attacker behavior analysis is a challenging problem, as relevant data cannot be found easily. We apply cognitive analysis on the network traffic data logs to find the attacker category and infer his intentions. We propose a Fuzzy-rule based approach to categorize the attacker. To make the system more resilient, the attacker's profile is subjected to behavioral analysis. Real time case study results assert that the proposed technique achieves a good accuracy in classifying the attacker, by discovering the attacker's behavioral pattern. Further it can be used to assist security and forensic investigators in profiling human attackers.

Keywords: Network forensics, Attacker behavior, Attacker profile, Fuzzy-rule based approach

1 Introduction

Incidents of cyber crime have increased dramatically over the past decade. However, due to the mysterious nature of the cyber crime, there have been few prosecutions and even fewer convictions. Due to the advancement in technology and automation of many business processes, cyber attackers have devised many new forms of computer abuse. These attackers use traditional methods to repeat conventional attacks. In addition to these attacks, new types of criminal activity have been evolving with the advancement in technology. Correspondingly computer crime investigation and computer forensics have also evolved.

The proposed work investigates the occurrence of disruptive or suspected network attacks on one or more connected systems. It is well-known that network attacks typically do not occur in isolation [1]. The activities that cause damage and consequent detection are not stand-alone. They need some detailed information of the target systems. It is preceded by few stages of probing to obtain usable information about the target system and find its vulnerabilities.

Investigations into visible breaches of security such as occurrence of malicious attacks or attempts are essential, instead of relying on casual root-cause analysis to conclude that the systems crashed or the network went down. Different attackers have varying intentions, and differ in their level of attack sophistication and strategy. It is critical to gather evidence about attacker strategies and types of attack execution. The sequence of network events leading up to the final breach should be discovered by profiling the attackers, and analyzing their behavior. The information should be archived and leveraged to identify previously unknown security weakness in the system. It is therefore important to profile the attacker, along with network traffic traces, as a form of digital evidence [2-3].

The paper focuses on the digital forensics task of discovering attacker behavior patterns. It does not perform a real-time monitoring that analyses live network traffic data and triggers alerts, as found in [4-5]. Detection time is crucial for real-time monitoring systems. The proposed work concentrates on discovering the accuracy of attacker behavior pattern, his intentions and propose counter measures.

To the best of our knowledge, there are no previous research attempts specifically addressing the attacker behavior pattern discovery problem. Traditionally the Intrusion detection problem has been addressed, with a number of open-source and commercial tools [6-10]. Their packet capturing and logging functionalities are used to generate the logs that are input to the proposed algorithm. The existing techniques detect a single real-time attack. This differs from the proposed work of finding an attacker's behavior pattern from all the network activities.

The Attacker behavior pattern discovery technique focuses on the relationship between technology and the cyber attackers, by applying the criminal profiling for attacker detection [11]. In [12], the authors found that

*Corresponding Author: K.Narasimha Mallikarjunan; E-mail: arjunkambaraj@tce.edu
DOI: 10.3966/160792642018091905028

cyber criminals adapt and devise new mechanism continuously; their mode of operation and targets vary immensely. These works are complementary to our algorithm, in finding the correlation among attacks and profiling attacker behavior. We propose a Fuzzy rule-based reasoning approach to help security and forensic investigators, to profile human attackers and their behavioral characteristics.

This paper is organized as follows: Section 2 presents the state of the art concerning behavior analysis and intrusion detection systems. Section 3 discusses the proposed novel approach for the attacker behavior pattern discovery. In Section 4, we demonstrate our evaluations of the proposed Fuzzy rule based approach, and discuss the results of a case study. Finally, we draw conclusions and suggest future lines of research in Section 5.

2 Related Work

Recently, attackers adopt sophisticated methods to launch attacks that target or utilize a large number of hosts, spread over a wide geographical area or multiple administrative domains. An integrated solution to large scale collaborative intrusion detection was proposed in [13]. The insider threat problem has received much attention within the research community [14-15]. Anomaly detection could be host-based, and the normal usage patterns of an individual user could be profiled [16]. They have demonstrated that a combination of physical characteristics related to the user can significantly decrease the time taken to detect an intruder.

In spite of advances in research, there is no unifying framework which seeks to fully characterize an attacker in terms of the following factors: kind of attacker, reason for the attack, human factors that lead to threats, impact of one's background on the likelihood of attack, the behavior exhibited by the attacker before or during an attack, the common attack vectors and steps within an attack, the assets and vulnerabilities that are typically targeted.

R. Katipally et al have proposed an attacker behavior analysis using Hidden Markovian Model (HMM) [1]. The distinguishing factor of our work is its broad nature, and ability to model the behavior of the initiators of following kinds of attacks: DoS, Phishers, Hackers, Botnet Operator and Insider in a single comprehensive framework.

The proposed framework will be useful to security practitioners and researchers. It provides a basis for elucidating the threat that enterprises face and the important elements (e.g precursors, indicator, attacker's types and attack steps), that are worth taking note of within the attacker chain. For researchers, the framework supplies a well grounded conceptualization of attackers and their intentions by identifying the various profiles and their inherent charecterstics.

3 Proposed Methodology

In this section, the proposed work for attacker intention prediction from a behavior analysis perspective is explained in detail. It consists of two main parts: The creation of Fuzzy rule-based framework for finding the broad_category of attacker (sub Section 3.1) and the novel behavior analysis technique based on behavioral characteristics to find the exact_category of attacker (sub Section 3.2, 3.3 & 3.4)

3.1 Analyzing Attacker Behavior Characteristics

Attackers may be classified into the following nine categories: Criminals, Insider, Terrorists, Hackers, Phishers, Nations, Malware authors, Botnet operators, Amateur/Script kiddies [17].

The Attacker behavior pattern discovery can be performed using the proposed Fuzzy rule-based framework as shown in Figure 1.

Input: Network logs, Auth log, Web server log, Commands history log

Output: Attacker Intention and attack pattern

Algorithm:

While Intrusion Detection System detects suspicious alerts do

1.1 Collate Network logs, Auth log, Web server log, Commands history log to form Meta Alert

1.2 Infer Meta Alert of an Intruder

1.3 Compute Fuzzy_membership_function and propose Fuzzy rule-base to find broad_ category of attacker

1.4 Out of inferred broad_category, compute exact_ category of attacker (P_A) in proposed action rule-base

1.5 Search Attacker Profile P_A for match in stored profiles P_X under the same category

1.6 If $P_A = P_X$ then

1.6.1 Retrieve attacker profile and his pattern of attack

1.6.2 Identify the attacker

1.7 Else If $P_A \neq P_X$ then

1.7.1 Add attacker P_A under this category,

1.7.2 Based on exact_attacker category, infer his next plan of action from proposed attack step rule-base

End while

Figure 1. Algorithm for finding attacker intention

Initially the Log analyzer module in the Intrusion Detection System (IDS) pre-processes the raw alerts received into specific network parameters: such as packet inter-arrival rate, mean time between packet-

arrival rates, and statistical information about the network traffic. Though packet arrival time plays an integral role in segregating legitimate traffic from malicious one, the accuracy and the effectiveness of the proposed method can be improved by introducing additional parameters such as packet size, protocol type [18].

Based on the mean time between packet-arrival rates, an Intrusion Detection System may detect an ongoing attack. To detect the attacker's motive, the attack traces can be analyzed to identify the attacker's intention.

Alerts such as probing, enumeration and login attempts will not be captured by the same log. So the different log entries captured and their time stamps are analyzed to create a sequence of events called the Meta alert. A sample Meta alert consisting of sequenced log event is shown in Figure 2. The alerts from different logs are grouped together, based on their associative nature of one action acting, as a base or a stepping stone to next level of intrusion. The different actions of the user which may occur sporadically over a period of time, will now be sequenced and relation between the alert could also be identified.

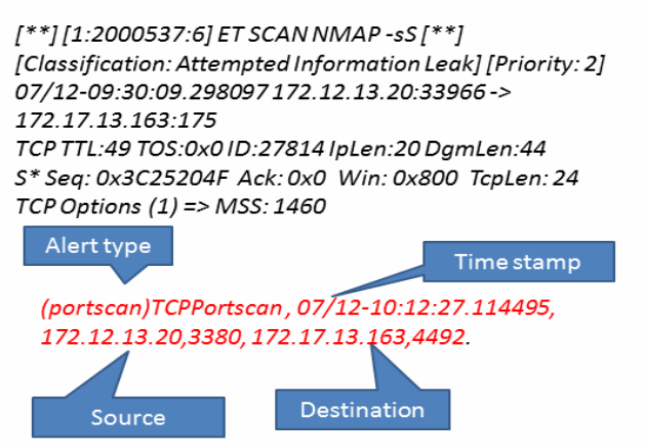

Figure 2. Real time Meta alert sequencing

The existing literature of various attacker characteristics [19] is distilled, and their behavior characteristics are summarized using the proposed Fuzzy rule base for action based classification of attackers. Fuzzy logic controllers are expected to work in situations where there is a large uncertainty or unknown variation in the parameters, and structures of the system under control [20]. Fuzzy system plays a vital role in complex non linear systems [21], when there is difficulty in designing a mathematical model. Any kind of cyber attack is detected using alerts generated from the Log analyzer module, and the behavior of the attacker like footprint clearance, back-door creation and malware attempts are observed as metrics in the fuzzification module as shown in Figure 3.

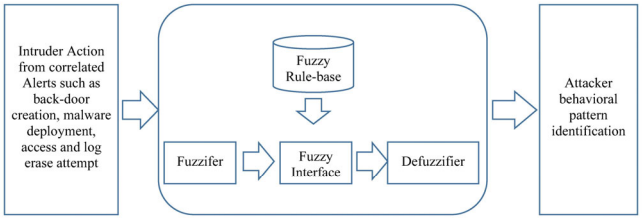

Figure 3. Proposed Fuzzy rule-based approach

The output from the Fuzzy Inference System categorizes the attacker broadly, as discussed in Figure 3. For each and every input, linguistic variables are defined and parameter values are assigned. The membership function for the linguistic variables is defined using the Triangular membership function. The knowledge base stores details about all the input and the output Fuzzy partitions. It includes knowledge about variables like Footprint clearance, back-door creation and malware attempts, their membership functions and their values. It includes the term set and the corresponding membership functions, defining the input variables to the Fuzzy rule based system, and the output variables or the actions to be taken is as shown in Figure 4.

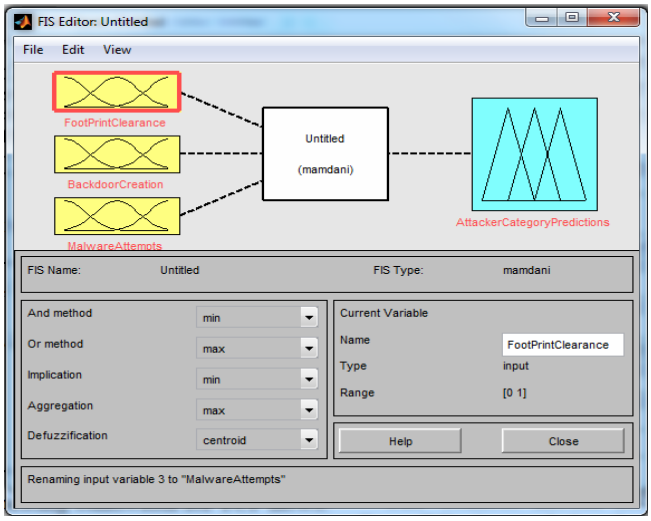

Figure 4. Membership function definitions

The rules defined in the Fuzzy module stores category of attackers in the Fuzzy interface engine, which will take care of behavioral prediction of attackers as shown in Figure 5. The various distinct steps and their occurrence frequency (low or high) are analyzed and classifications of attackers are mapped. Each rule is selected such that it contain one distinct attribute to identify uniqueness in classifying the profiles.

The different stages of the Fuzzy rules are validated and broad attacker category with high similarity within the rule base is predicted as given in Figure 6.

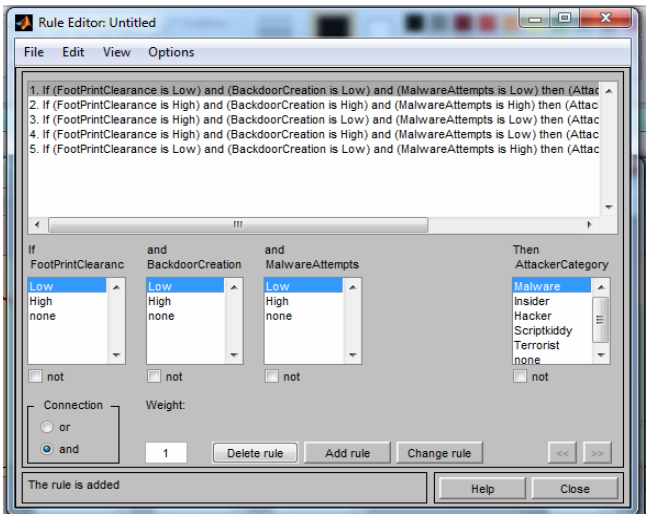

Figure 5. Rules for attacker behavioral prediction

Input: Alert processed from logs obtained based on traffic flow from online monitoring system

Output: attacker_category_predictions

Algorithm:

1. Initialize the required foot_print_clearance {u}, backdoor_creation {v} and malware_access_ Attempts {w} variables.
2. Compute Fuzzy_membership_function
   - 2.1 $\mu(x; a, b, c) = \mathbf{0}$, for $x > \mathbf{0}$ or $x > 0$
   - 2.2 $\frac{x-a}{b-a}$, $\boldsymbol{f}$ or $a \le \boldsymbol{x} \le b$
   - 2.3 $\frac{c-x}{c-b}$, $\boldsymbol{f}$ or $b \le \boldsymbol{x} \le c$
3. If u and v and w is high then attacker_category_ predictions as malware_author or botnet operator.
4. Else If u is high, v and w are low then attacker_ category_predictions as insider.
5. Else If u, v is high and w is low then attacker_ category_predictions as hacker or criminal.
6. Else If u, v and w are low then attacker_ category_predictions as script kiddy.
7. Else If u, v is low and w is high then attacker_ category_predictions as terrorist.
8. Else attacker_category_predictions as nation or phisher.

End

Figure 6. Algorithm for finding broad_attacker Category

The different profiles are analyzed and the most similar membership function is identified to predict the attacker category. Each attacker profile though have similar steps in their execution they also have certain unique variation in the methods to achieve the desired effect. The fuzzy engine takes into account all these values to derive rules such that the overlapping of attacker group is minimized with distinct attribute selection. Figure 7 shows the Fuzzy rules prediction for different values of the action of the attackers, like foot_print_clearance, back-door creation and malware_ access_attempts, and these are obtained from the Meta alerts for the intruder classified based on time stamp. The Meta alert sequences the various alerts and commands from the logs, to analyze the action performed by the command and actions that has led to the alert creation.

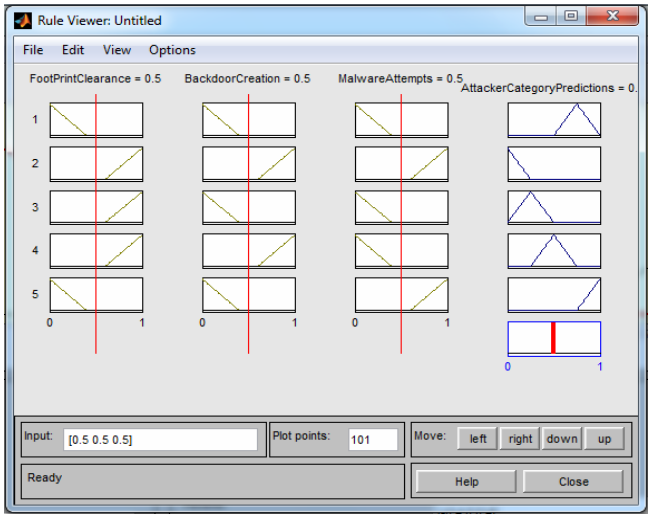

Figure 7. Predicted broad Category of Attacker

3.2 Proposed Action-base for Classification of Attackers

The Fuzzy Inference system can predict the broad category of attackers. But for arriving at the exact category of the attacker, more details about his behavioral characteristics are needed. All the categories of the attackers, along with their behavior attributes are shown in Table 1 and Table 2. These values have been proposed after careful behavior analysis, based on their defined and proven characteristics obtained during various cyber investigations [17, 19, 22-23]. The row description and column description of Table 1 is given as Table 1.1 and Table 1.2.

Existence of a specific attack sequence in predicting of attack intention is denoted by √ in the Tables. Considering the case of a script kid type of attackers, mostly rely on existing tools and spyware available. It would not be of interest for such attacker in creating new tools of attack execution like that of a hacker or a phisher. Hence the marking: R3, R4, R11, R12 is true for a script kid profile.

Table 1. Action-base for Attacker behavior Analysis

	C1	C2	C3	C4	C5	C6	C7	C8	C9
R1		√							
R2	√		√	√	√		√	√	
R3	√	√	√	√	√	√	√	√	√
R4			√	√		√		√	√
R5			√	√		√			
R6		√			√	√			
R7	√	√		√	√		√	√	
R8			√	√					
R9	√	√			√				
R10				√	√		√	√	
R11	√	√	√	√	√	√	√	√	√
R12	√	√	√		√	√		√	√
R13	√						√	√	
R14		√		√	√		√	√	
R15	√							√	
R16								√	

Table 1.1. Row Description of Table 1

Row	Behavior Characteristics
R1	Initial Knowledge about the network
R2	Knowledge about attack execution
R3	Application based attacks
R4	Network based attacks
R5	Permanent Destruction of network Infrastructure
R6	Information Espionage
R7	Monitory Gains
R8	Brag about their expertise
R9	Commit identity theft
R10	Develop own malicious scripts
R11	Using of tools existing
R12	Using spyware and malwares
R13	Creates back doors for repeated visits
R14	For hire
R15	Organized groups
R16	Coordinated execution

Table 1.2. Column Description of Table 1

Column	Attacker Category
C1	Criminals
C2	Insiders
C3	Terrorist
C4	Hackers
C5	Phishers
C6	Nations
C7	Spyware/Malware authors
C8	Bot net Operators
C9	Amateur/ script kids

Similarly when there is an instance of information gathering, it indirectly gives out the information that the intruder cannot be a part of insider attacker profile, as he/she will have prior knowledge about the network. Different profiles are analyzed to make sure that there is at least one distinct feature or a distinct combination of features for each profile. Once the attacker category is identified the intention for their attack could be predicted from the knowledge base.

3.3 Proposed Attack Step-base for Intention Prediction

Various categories of the attackers along with their attacking strategies are proposed in Table 2. The row description and column description of Table 2 is given as Table 2.1 and Table 2.2 respectively. The attack step rule-base having an intention of each attacker category has been proposed by summarizing from various cyber investigations as reported in [22]

Table 2. Attack Steps-base for Intention Prediction

	C1	C2	C3	C4	C5	C6	C7	C8	C9
R1	√		√	√		√			√
R2	√		√	√		√			√
R3	√	√	√	√	√	√	√	√	
R4	√	√	√	√	√		√	√	
R5	√	√	√	√	√	√	√	√	

Table 2.1. Row Description of Table 2

Row	Attack Steps
R1	Scanning/Reconnaissance
R2	Enumeration
R3	Exploit by Access Attempt
R4	Exploit by Denial of Service
R5	Exploit by Malware Attempt

Table 2.2. Column Description of Table 2

Column	Attacker Category
C1	Criminals
C2	Insiders
C3	Terrorist
C4	Hackers
C5	Phishers
C6	Nations
C7	Spyware/Malware authors
C8	Bot net Operators
C9	Amateur/ script kids

3.4 Attacker Behavior Pattern Discovery

From the broad category suggested by Fuzzy-rule base, each intruder is categorized and profiled, based on the match with the predefined attacker categories, listed in Tables 1 and 2. For each intruder, the exact category C_i to which he/she would behaviorally belongs is calculated using the proposed positional hamming distance formula as specified in Equation 1

$$C_i = \sum_{x=1}^{n} A_x P_x I_x \quad \textbf{(1)}$$

Where

A_x is the Attribute of the intruder which will be Boolean value depending on whether he performs the current attack step or not

P_x is the current position of the attack steps-rule base listed in Table 2

I_x is the Attacker's characteristics for each attacker

profile in action base in Table 1

n is the Total number of attacker characteristics present in the action base as analyzed in Table 1

The attacker's behavioral characteristics using Equation 1 will find the most matching attacker category, from action base and attack steps Based on the attacker category, the traces will be compared with the existing profile traces. The matching values are calculated for each profile. The profile with the highest matching trace is highlighted to the administrator for identifying the best response action to be initiated for minimizing the intruder's attacking effect.

4 Experimental Results

This section evaluates and illustrates whether the proposed approach has applicability of attacker category identification.

4.1 Evaluation Using Case Study

A well known cyber attack investigation of Mitnick [23] was taken to evaluate the proposed methodology. The behavior of the attacker was concluded as "criminal" after the cyber attack investigation. To prove the accuracy of the proposed methodology, the Mitnick case scenario was converted into corresponding behavioral parameters pertaining to the Tables 1 and 2. The Fuzzy rule base inference predicted that the attacker category could be criminal or hacker. The intruder profile characteristics were matched using Equation 1 for these two categories. The intention of the intruder was to steal data rather than to showcase his proficiency about the system, which is an inherent character of a criminal. The intruder has manipulated an un-attended vulnerability rather than help to patch the vulnerability. It is concluded, his behavior as a criminal action, with the knowledge of hacking as shown in Figure. 8.

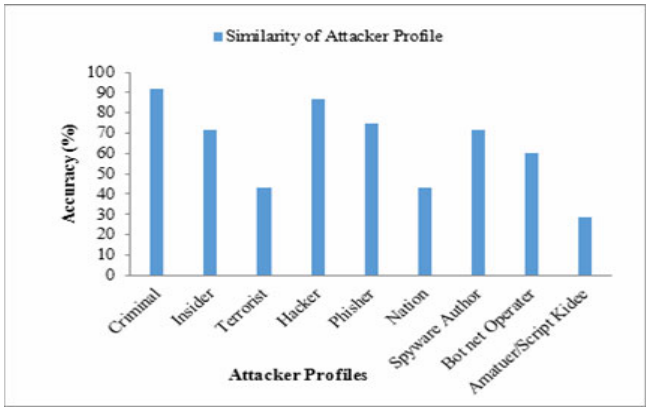

Figure 8. Attacker Category Prediction for the Kevin Mitnick attack Scenario

Figure 9 shows that the new proposed methodology could exactly predict the attacker's category and his intentions and plan of execution.

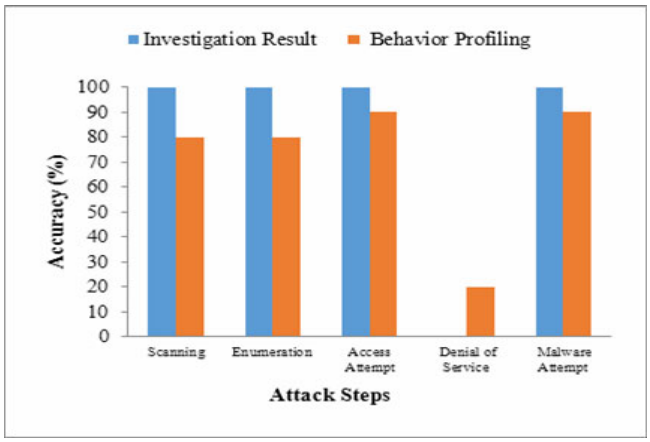

Figure 9. Attacker Prediction Accuracy for attack Scenario

The results match with the proven investigation results [23]. The Attacker Behavior Based profile creation helps in generalizing the attack sequence pertaining to each attacker category which in turn aid for the prediction of next steps by the similar attackers in the same category.

4.2 Real Time Experimental Results

The experimental setup consists of twelve machines targeting the victim machine in a span of one week as shown in Figure 10. Two machines each from two different sub networks were connected in the environment set up. The users were given set of allowed instructions to be followed during attack phase.

i. Open a new file, copy a configuration file, deface a web service running on the victim server and deny access to the web service.

ii. Record the steps they follow to achieve their goal for further profiling.

iii. Form groups, if needed.

iv. Write their own scripts or use any available tools.

v. Get connected using wired network only.

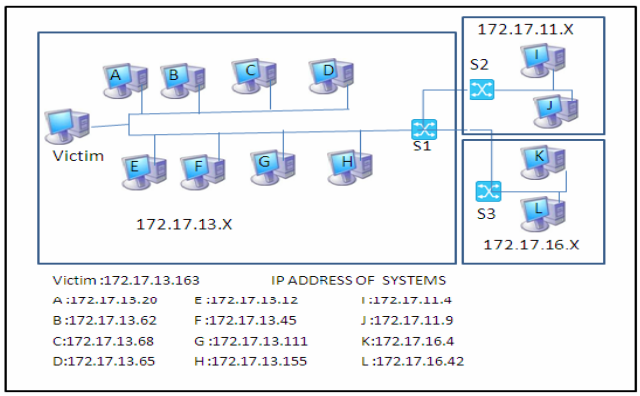

Figure 10. Experimental Scenario

Initially all the log traces and alert messages were analyzed and correlated. The logs were collected from the system log, auth log and web server logs. The commands typed in the console and command prompt was also recorded along with time stamp. These

different discrete logs were converted into Meta alerts with the time stamp as the key to correlate with the alert logs provided by the Intrusion Detection system (i.e. SNORT Logs). Applying the proposed Framework as shown in Figure 1 classified the traces into attacker category as displayed in Figure 11. Based on the attacker category the intention of each category of attacker is identified from attack step-rule base and counter measures are suggested.

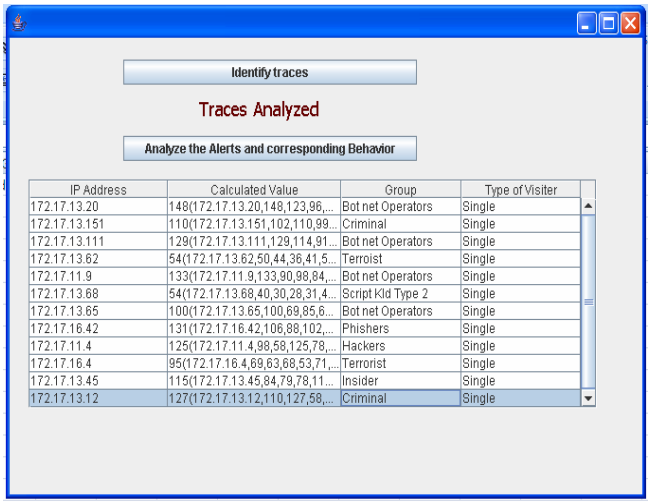

Figure 11. Meta Alert Generation for Attacker Profiling

The various attacker category profiles matching the identified IP addresses are listed out and the intruders are classified based on their actions and the behavior of the cyber systems as shown in Figure 12. The suspicious IP addresses are mapped with all the stored profiles and their similarity percentage is visualized.

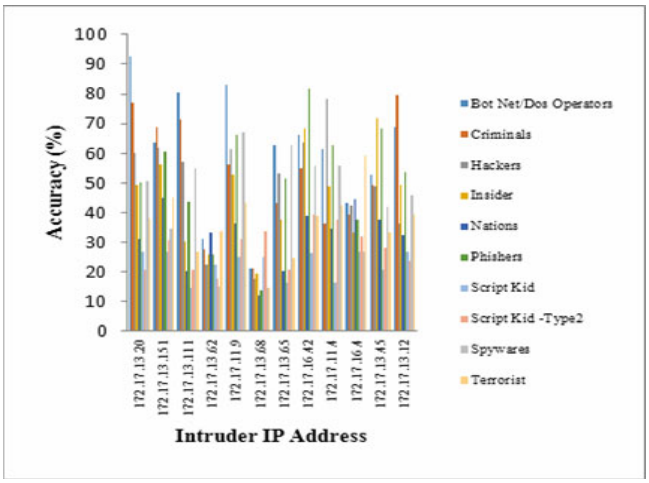

Figure 12. Attacker Behavior Classification using proposed Fuzzy approach

The various attacker category profiles matching to an identified single intruder is shown in Figure 13.

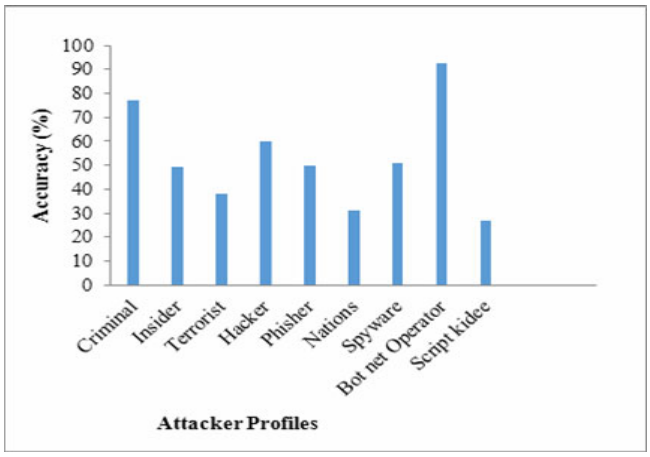

Figure 13. Attacker Behavior Classification using proposed Fuzzy approach for a single attacker

Figure 14 shows the threat modeling for the real time experimental scenario and reports the probable threats. Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables one to identify, quantify, and address the security risks associated with an application. The threat model checks the given network, considering all the software and hardware components, and emulates the un-patched vulnerabilities and configuration issues, that could be utilized by an intruder in achieving his/her intentions. The various instances that are listed in the Table 3 acts as a benchmark for the prediction correctness of the proposed method.

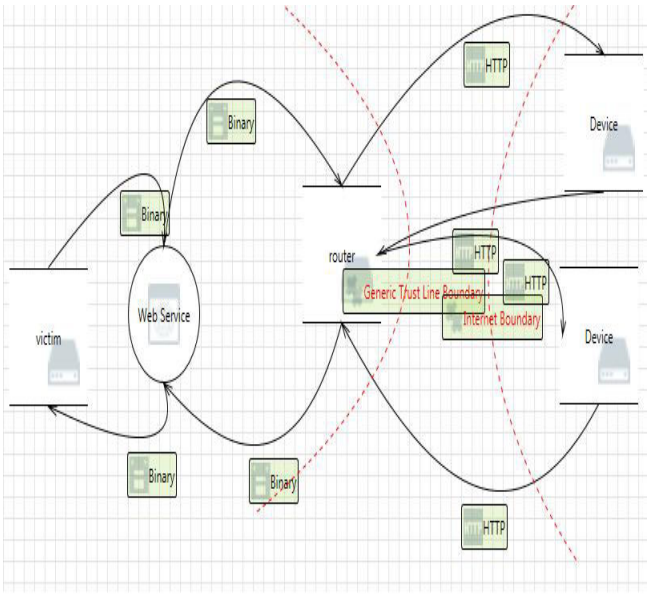

Figure 14. Threat modeling for attack scenario

Figure 11 shows that nations/script kiddies are the least possibility out of attacks from the various source IPs. Nations/script kiddies will not be launching Denial of service as reported in Behavior analysis in attack step base in Table 2. Threat modeling also reveals that Denial of service is not the attacker's highest choice

but still it may also occur as reported in Table 2. Hence the justification that this kind of attacker category is correct since nations/script kiddies can perform DoS only with the help of recruiting criminals. The Threat model also highlights the various available vulnerabilities the intruder could utilize to maximize his intrusion effect, and the different vulnerabilities that could be utilized in sequence to achieve the desired activity of the intruder, to the system administrator as shown in Table 3. Based on the knowledge acquired the system administrator could plan a suitable countermeasure.

Table 3. Threat Modeling Inference

Threat	Number of Instances
Denial of Service	10
Information disclosure	2
Repudiation	4
Spoofing	26

When compared with the existing method [1] which also proposes attacker behavior analysis using Hidden Markovian Model (HMM), the proposed method performs better in identifying the attacker's intention, as the HMM model gives out a list of groups and their intentions. The proposed method matches the user profile with the most probable attacker profile and lists out his/her intentions as a result. It also dives deep into the different alerts and their relationship with each other, and predicts the attacker's intentions accurately. A comparison of the existing and proposed methods and the different features they address are shown in Table 4

Table 4. Comparison of Results

Features	HMM based Existing Methods	Proposed method
Number of Attacker categories	5	9
History of commands used	No	Yes, considered for sub classifying the attacker profile
Alert grouping	Yes, Done for Packet count (for DoS attack variants)	Yes, used to sequence the number of instances and also for identifying their attack intention
Prediction of next action of intruder	No	Yes, since stored profiles contain their actions and commands used
Accuracy of attacker's Intention prediction	Less Accurate, Since broad classification leads to a set of attack groups and attack intention	Better Accuracy, Since attack steps and knowledge about the attack execution are input, the intention prediction is more accurate

The contribution of our work is that the attacker pattern discovery process usually involves large amount of log data, because numerous individual alerts are received from the intrusion detection system. In our proposed model, Fuzzy rules provide the broad category of attacker, which helps to fine tune alert logs and network performance logs. These logs are analyzed and correlated to identify the behavioral trails. These trails are matched with the existing stored attacker profiles in that category and thus the system administrator could identify the corresponding attacker profile. The system administrator can in turn recommend a suitable damage control and recovery procedure.

5 Conclusion

In this paper, a Fuzzy rule based method of classifying the attacker's behavior based on the attack steps and the various actions of the attackers has been proposed. This work helps in predicting the attacker's intentions more accurately and classifies the attacker's profile to aid in identifying the best mitigation technique that could be applied to minimize the attack impact. The model could be extended further in several directions. Refinement in the modeling of attacker's behavior constitutes a promising area for future work. This includes drawing upon the existing body of literature in order to integrate additional behavioral models into the existing model with nine categories of attackers. The attacker group still may try to deploy variance in the step of execution which has to be also profiled for accurate prediction. Furthermore, we can integrate alternative approaches to model zero day attack actions.

Compliance with Ethical Standards:

The authors have no conflict of Interest and all experiments have been conducted in the Smart and Secure Environment (SSE) Laboratory sponsored by National Technical Research Organization (NTRO) within the campus.

References

[1] R. Katipally, L. Yang and A. Liu, Attacker Behaviour Analysis in Multi-stage Attack Detection System, *in Proc. of the seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tenessee*, USA, 2011, Article No. 63, pp. 1-6.

[2] P. A. Watters, S. McCombie, R. Layton and J. Pieprzyk, Characterizing and Predicting Cyber Attacks using the Cyber Attacker Model Profile (CAMP), *Journal of Money Laundering Control*, Vol. 15, No. 4, pp. 430-441, 2012.

[3] L. Wang, A. Liu and S. Jajodia, Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts, *Computer Communications*, Vol. 29, No. 15, pp. 2917-2933, September, 2006.

[4] B. Landreth and H. Rheingold, Out of the Inner Circle: A *Hacker's Guide to Computer Security*, Microsoft Press, Washington, 1985.

[5] M. Kjaerland, A Taxonomy and Comparison of Computer Security *Incidents from the Commercial and Government Sectors, Computers and Security*, Vol. 25, No. 7, pp. 522-538, October, 2006.

[6] S. Forrest, S. A. Hofmeyr, and A. Somayaji, Computer Immunology, *Communications of the ACM*, Vol. 40, No. 10, pp. 88-96, October, 1997.

[7] K. Sequeira and M. Zaki, ADMIT: Anomaly-based Data Mining for Intrusions, *Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton*, Alberta, Canada, 2002, pp. 386-395.

[8] D. Wagner and R. Dean, *Intrusion Detection via Static Analysis, IEEE Symposium on Security and Privacy*, Oakland, CA, 2001, pp. 156-168.

[9] J. Raiyn, A Survey of Cyber Attack Detection Strategies, *International Journal of Security and Its Applications*, Vol. 8, No. 1, pp 247-256, January, 2014.

[10] E. Eskin, A. Arnold, M. Prerau, L. Portnoy and S. Stolfo, A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data, in: D. Barbara, S. Jajodia (Eds), *Applications of Data Mining for Computer Security*, Vol. 6, Springer, Bosten, 2002, pp. 77-101.

[11] C. Colombini, A. Colella, Digital Scene of Crime, Technique of Profiling Users, *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, Vol. 3, No. 3, pp. 50-73, September, 2012.

[12] S. Kapetanakis, A. Filippoupolitis, G. Loukas and T. S. Al Murayziq, *Profiling Cyber Attackers using Case-based Reasoning, 19th UK Workshop on Case Based Reasoning*, Cambridge, UK, 2014, pp. 39-48.

[13] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw and H. Owen, Real-time and Forensic Network Data Analysis using Animated and Coordinated Visualization, *in Proc. of the Sixth Annual IEEE SMC Information Assurance Workshop (IAW'05)*, West Point, NY, 2005, pp. 42-49.

[14] A. Filippoupolitis, G. Loukas and S. Kapetanakis, Towards Real-time Profiling of Human Attackers and Bot Detection, *in Proc. of CFET 2014: Cybercrime Forensics Education & Training, Canterbury*, UK, 2014, pp. 1-6.

[15] Z. Baig and K. Salah, Distributed Hierarchical Pattern-Matching for Network Intrusion Detection, *Journal of Internet Technology*, Vol.17, No. 2, pp.167-178, March, 2016.

[16] A. Patcha and J. M. Park, An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends, *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Vol. 51, No. 12, pp. 3448-3470, August, 2007.

[17] A. Panchenko and L. Pimenidis, Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication, *Proc. of International Conference on Communications and Multimedia Security*, Crete, Greece, 2008, pp- 240-251.

[18] G. Preetha, B. S. Devi and S. M. Shalinie, Autonomous Agent for DDoS Attack Detection and Defense in an Experimental Testbed, *International Journal of Fuzzy Systems*, Vol. 16, No. 4, pp. 520-528, December, 2014.

[19] C. M. Steel, Idiographic Digital Profiling : Behavioral Analysis based on Digital Forensics, *The Journal of Digital Forensics, Security and Law*, Vol. 9, No. 1, pp. 7-18, 2014.

[20] S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, *Real Time DDoS Detection using Fuzzy Estimators, Computers & Security*, Vol. 31, No. 6, pp. 782-790, September, 2012.

[21] Y. Q. Fan, Y. H. Wang, and W. Q. Wang, Adaptive Fuzzy Tracking Control with Compressor and Limiters for Uncertain Nonlinear Systems, *International Journal of Fuzzy Systems*, Vol. 16, No. 1, pp. 31-38, March, 2014.

[22] R. Katipally, W. Gasior, X. Cui and L. Yang, Multistage Attack Detection System for Network Administrators using Data Mining (CSIIRW'10), *Proc. of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, USA, 2010, Article No. 51.

[23] http://cs.boisestate.edu/~jxiao/cs333/01-kevin mitnick.pdf

Biographies

K. Narasimha Mallikarjunan is pursing Ph.D. at Anna University and is working as Assistant Professor in the Department of Computer Science and Engineering at Thiagarajar College of Engineering, Madurai. His current research interests include network security and information security.

S. Mercy Shalinie is currently Professor and Head of the department of the Department of Computer Science and Engineering at Thiagarajar College of Engineering. She has published several papers in International Journals/ Conferences. Her current areas of interest include machine learning, neural networks and information security.

G. Preetha is currently working as Assistant Professor in the Department of computer Applications at Fatima College, Madurai. She has published several papers in International Journals/Conferences. Her current research interests include network security and wireless adhoc networks.