A Framework for Intrusion Detection and Prevention

Rejuan Ahamed Anik
School of Computer Scisce
and Engineering (SCSE)
Lovely Professional University
Phagwara, India
soloastra00@gmail.com

Atul Malhotra
School of Computer Science and
Engineering (SCSE)
Lovely Professional University
Phagwara, India
atulmlhotra@gmail.com

Anik Sorkar
School of Computer Science and
Engineering (SCSE)
Lovely Professional University
Phagwara, India
thesorkar@gmail.com

Md Hasibul Ahsan Shakil
School of Computer Science and
Engineering (SCSE)
Lovely Professional University
Phagwara, India
cshakil30@gmail.com

***Abstract*— Cyber security attacks have been very common these days due to the widespread use of internet-connected systems for enterprise and home users. The enterprise systems are targeted by a variety of network layer and transport layer attacks which result in critical monetary and technological damages. In this paper, we propose a network intrusion detection and prevention framework which targets the detection of the network layer, data-link layer, and transport layer attacks in real-time. The framework utilizes an exhaustive rule set to identify and stop various attacks against the system. The execution of the framework showed an accuracy of more than 94% in detecting and preventing attacks.**

Keywords—Cyber security, intrusion detection and prevention, deaunthentication attack, ARP poisoning, evil twin.

I. Introduction

Nowadays, the involvement of the internet in normal life has increased rapidly. The use of the internet has become very crucial for everyone. So, with the increase in the use of the internet for personal activities, it is also necessary to keep the system secure from malicious activities as cyber-attacks are increasing at an alarming rate with the evolution of technology. There are a variety of attacks which target the information system in order to steal the information or corrupt the data present with in them. The prominent attacks which target the networks are evil twin attack, deauthentication attack etc. A list of prominent attacks has been presented in table 1. So, to identify and prevent the system from such attacks, the intrusion detection systems came into existence. Intrusion detection systems (IDSs) have the capacity to identify any anomalous network usage or access. Intrusion detection system can monitor, collect, and analyze data in order to detect known assaults, identify abnormal network usages, and reveal network misuse. IDSs collect data and issue alerts based on the type of intrusion detected. This paper proposes a framework for network intrusion detection and prevention which can detect data link layer, network layer and transport layer attacks and defend against them.

II. Literature Review

Parag K, *et al.* designed and developed an Intrusion Detection System with outside-the-network hardware that checks all incoming requests to the cloud [1]. The approach utilized by the authors was Misuse Intrusion Detection, and the system used was Network Intrusion Detection System. The attackers would have an easier time attacking the hardware because it is located outside the network. This would be the primary downside of the authors' suggestion.

Vieira K, *et al.* developed an Intrusion Detection System for cloud and grid environments, which is installed in the cloud and grid's middleware layer [2]. The main disadvantage of the approach is that Network Based Intrusion Detection does not prioritize the security of each and every computer on the network. The design and security frameworks of the cloud and grid environments would differ. As a result, a unified system for both cannot be built.

Praveen Kumar Rajendran, *et al.* developed framework of Hybrid Intrusion Detection System for Private Cloud has been developed using [3] .Net framework as front end and SQL Server as back end to store the information. The Hybrid Intrusion Detection system has been implemented on the Microsoft Azure Cloud environment. The dynamic feature of the Hybrid Intrusion Detection System is achieved by creating a simple and informative User Interface. Scalability and self-adaptability of a Hybrid Intrusion Detection System are achieved by running the system in both the network and all of the network's hosts. The property of efficiency is accomplished by detecting both types of intrusion, namely Anomaly Intrusion and Misuse Intrusion.

Sibi Chakkaravarthy Se., *et al.* proposed an intrusion detection system for detecting wireless attacks in IEEE 802.11 networks, by merging KDE and HMM via a tandem queue with feedback [4]. The proposed KDE-HMM technique/method combines the benefits of both statistical and probabilistic features to produce better results. The performance of the suggested KDE-HMM technique has been experimentally validated, and it is discovered that the proposed KDE-HMM identifies the aforementioned attacks with 98 percent accuracy.

Stephen Glass *et al.* proposed a unique intrusion detection mechanism that detects external adversary man-in-the-middle and wormhole assaults against wireless mesh networks [5]. A simple modification to the wireless MAC protocol is proposed to reveal the presence of a frame-relaying attacker. We test the updated MAC protocol and find that the detection method has a high detection rate with no false positives at the cost of a very little loss of bandwidth. The proposed update is applicable to MANETs, wireless mesh networks, and infrastructure networks.

Neminath Hubballi, *et al.* investigated existing false alarm minimization techniques in signature-based Network Intrusion Detection Systems (NIDS) [6]. The authors present a taxonomy of false alarm reduction techniques in signature-based intrusion detection systems, as well as the advantages and disadvantages of each class. Further it's famous that state of the art IDS generates several false alarms. There are unit techniques projected in IDS literature to reduce false alarms, several of that area unit wide employed in observe in business Security data and Event Management (SIEM) tools.

Gideon Creech, *et al.* proposed a new host-based anomaly intrusion detection methodology based on discontiguous system call patterns, with the goal of increasing detection rates while decreasing false alarm rates [7]. The key concept is to apply a semantic structure to kernel level system calls in order to reflect intrinsic activities hidden in high-level programming languages, which can help understand program anomaly behavior. Excellent results were demonstrated using a variety of decision engines, evaluating the KDD98 and UNM data sets, and a new, modern data set.

Ming Zhang, *et al.* introduced an anomaly detection model based on One-class SVM to detect network intrusions [8]. The training dataset for the one-class SVM is only normal network connection records. However, after training, it is capable of distinguishing between normal and abnormal attacks. The observed behavior of the user is analyzed to infer whether or not the normal profile supports the observed one. This is carried out using two-class classifiers. A new hybrid approach using Support Vector Machine (SVM) and Naïve Bayes (NB) is proposed to provide better accuracy and to reduce the problem of high false positive.

Hisham Shehata, *at al.* Galal suggested a framework of behavior-based features for describing malicious behavior displayed by malware instances [9]. To extract the proposed model, first perform dynamic analysis on a recent malware dataset within a controlled virtual environment, capturing traces of API calls invoked by malware instances. The different structure of malware variants poses a serious problem to signature-based detection technique, yet their similar exhibited behaviors and actions can be a remarkable feature to detect them by behavior-based techniques.

Eduardo K. Viegas, *et al.* demonstrated a new method for developing intrusion databases [10]. The authors proposed a new evaluation scheme adapted to the field of machine learning intrusion detection. The researchers proposed a new multi-objective feature selection method that takes into account real-world network properties. The objective is that the databases ought to be straightforward to update and reproduce with real and valid traffic, representative, and in public on the market. Using our projected technique, we tend to propose a brand-new analysis theme specific to the machine learning intrusion detection field.

Mrutyunjaya Panda, *et al*. proposed hybrid intelligent decision technologies that use data filtering with directed learning methods and a classifier to produce better classified judgements in order to detect network assaults [11]. The results show that the Naive Bayes model is very appealing due to its integrity, elegance, robustness, and effectiveness. Decision trees, on the other hand, have demonstrated their effectiveness in both generalization and the detection of new assaults. The results reveal that there is no single best algorithm that outperforms others in all cases. In some circumstances, the data's properties may be important. A domain expert or expert system may use categorization results to make better selections when selecting an algorithm.

F. Amiri *et.al*, Proposed Selection Feature method to improve the performance of existing class dividers by excluding unrelated features [12]. In addition, an improved Vector Small Square Support Machine called PLSVM has been introduced. The line of line and non-line selection factor within the pre-processing phase has been considered in this work. PSSVM has done well in classifying general attack and inspection records, respectively at 95.69% and 86.46%. In this work, the impact of changing the aesthetic aspect ratio and the test function has been investigated by selecting a line-based relationship (LCFS) feature, a choice of advanced feature. (FFSA) and algorithms for selecting integrated information feature (MMIFS). A review of the KDDcup99 data set shows that feature selection algorithms can greatly improve the accuracy of categories. In contrast, PSSVM missed a large number of powerful attacks such as DoS and U2R attacks with exactly the same behaviors as normal, recorded at 78.76% and 30.7% respectively.

Mishra, *et al*, point out that implementing wireless network research on wireless networks is not easy due to basic structural differences, especially the lack of a fixed infrastructure [13]. The authors argue that the type of wireless ad network response depends on the type of intervention, network settings and applications used, and reliance on evidence. Some of the possible solutions include updating the communication channels between nodes, identifying vulnerable areas, redesigning the network to establish vulnerable nodes, and initiating a re-validation application across all nodes in the network. The authors also discuss seven MANET IDS proposals in the following ways: confusing distributed distribution and mobile-based acquisition. The IDS agent works in each mobile location and performs location data collection and location acquisition in both cases. The difference between the two approaches lies in global identification: distributed confusing discoveries using information from neighboring sites to build a co-found engine while mobile-based acquisitions use portable agent technology to obtain access and response.

Akash Garg, *et al.* discussed on Snort, mostly using signature-based IDS (intrusion detection systems) because it is an open-source software [14]. It is used world widely in intrusion detection and prevention domain. In this paper, the authors used IDEVAL data set we detect attacks using Snort on this dataset. The most vital purpose of intrusion detection systems is to spot attacks against info systems. It is a security technique trying to spot numerous attacks. Snort is usually used signature based mostly IDS because it is an open supply code.

Wathiq Laftah, Al-Yaseen, *et al.* proposed a multi-level hybrid intrusion detection model that uses support vector machine and extreme learning machine to improve the efficiency of detecting known and unknown attacks [15]. A modified K-means algorithm is also proposed to build a high-quality training dataset that contributes significantly to improving the performance of classifiers. Several intrusion detection systems have been developed to protect networks using different statistical methods and machine learning techniques. This study aims to design a model that deals with real intrusion detection problems in data analysis and classify network data into normal and abnormal behaviors.

III. Methodology

Network anomalies have been an inherent part of today's internet as the networked systems continue to grow in scale and number. The increase in network-based services has further added to the possibilities of attackers identifying and targeting network anomalies through those services. So, in an attempt to protect and prevent networked systems from being compromised, a framework for intrusion detection and prevention is presented here which attempts to detect the malicious network traffic transmitted at the data link layer, network layer, and transport layer. The framework performs real time monitoring of the traffic and inspects the packet header and payload to identify the malicious behavior. The network administrator can define level of detection by selecting the appropriate detection sensitivity in order to inspect the traffic at a higher granularity. The attacks identified by the framework are given below.

- Deauthentication attack: A Wi-Fi deauthentication attack is a type of denial-of-service attack that sends deauthentication frame to AP.
- ARP poisoning: In ARP poisoning attack a large number of forged ARP requests and replies packets sent to overload the switch and the attacker flooded the target computer ARP cache.
- Evil twin: An evil twin attack is a spoofing attack that works by manipulating users into connecting to a fake Wi-Fi access point that mimics a legitimate network.
- Rogue access point: A rogue access point is an access point that has been established on a network without the consent of the legitimate network owner.

1. Rule Sets

A. For deauthentication attack detection and prevention

```
Get ip
Set threshold_point =50
Set temp_ip=ip
If (temp_ip =ip)  && ( deauthenthication_packet >= 50)
{
 Print response
        “deauthentication attack detected”
Call prevention(temp_ip)
}End of if
```

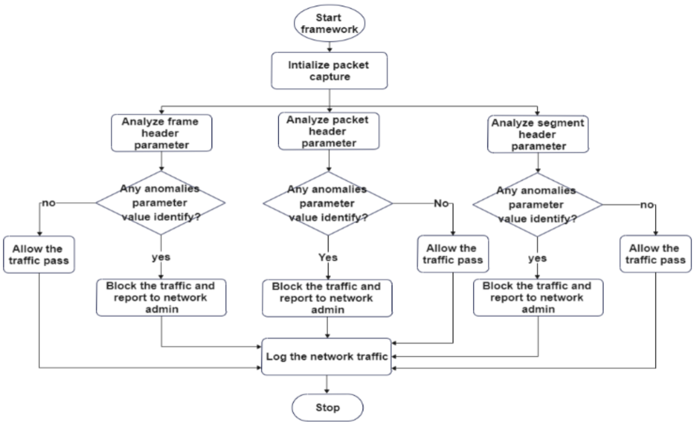
B. For Evil Twin Attack Detection

```
Set threshhold_point=2
Get bssid
Get ssid
Set saved_bssid =bssid
Set saved_ssid = ssid
Get number_of_ssid
If (number_of_ssid)> threshold_point
    {
     Print response
            “Evil twin attack detected”
 } End of if
  else {
      Get beacon_packet
          If (bssid != saved_bssid) && (ssid !=saved ssid)
             {
               Print response
                        “Evil twin attack detected”
                Print response
                        “attacker”+bssid “attacker”+ssid
              }End of if
 }end of else
```

C. For Arp Poisoning Attack Detection

```
For each ip address
If (ip_1.mac = ip_2.mac)
   {
     Print response
          “Arp poisioning attack detected for ip_1 and ip_2”
           Call prevention(ip_1,ip_2)
   }
End of if
```

2. Flow Chart


Start framework
Intialize packet capture
Analyze frame header parameter
Analyze packet header parameter
Analyze segment header parameter
Any anomalies parameter value identify?
Any anomalies parameter value identify?
Any anomalies parameter value identify?
no
No
no
yes
Yes
yes
Allow the traffic pass
Allow the traffic pass
Allow the traffic pass
Block the traffic and report to network admin
Block the traffic and report to network admin
Block the traffic and report to network admin
Log the network traffic
Stop

IV. IMPLEMENTATION

For experimenting with our framework, we use a laptop that runs Kali Linux v2021.1. We also use an integrated Network Interface Card (NIC) that monitors the channel, injects packets as needed, and supports the 802.11 protocol. All of the attacks detailed in this work were carried out using this method. In addition, while the attacks are being carried out, we use another NIC to monitor, capture, and record packets from the channel. Only monitor mode functionality is required for this NIC. Finally, we attack experimental access points. It has three radios and supports the 802.11 protocol and WEP Wi-Fi security. We configured the first radio as a WEP AP on the 2.4 GHz band, the second radio as unused, and the third radio as our framework offered. We use two extra laptops for the client; both are running Kali Linux distribution. We set up our Wi-Fi adapter to monitor mode cause monitor mode captures all relevant data packets to determine whether the packets are malicious or not.

V. RESULT & ANALYSIS

To evaluate the effectiveness of the proposed model, a set of metrics have been adopted to determine the most efficient intrusion detection model. In this section, we evaluate the performance of our framework model using live dataset. We study the variations in detection rate.

- Detection Rate: The percentage of attacks that are detected out of the total number of attacks.

The combination of anomaly detection based on ruleset and detection based on attack allows the intrusion detection model to achieve a high rate of intrusion detection (almost 96.25%) as shown in below.

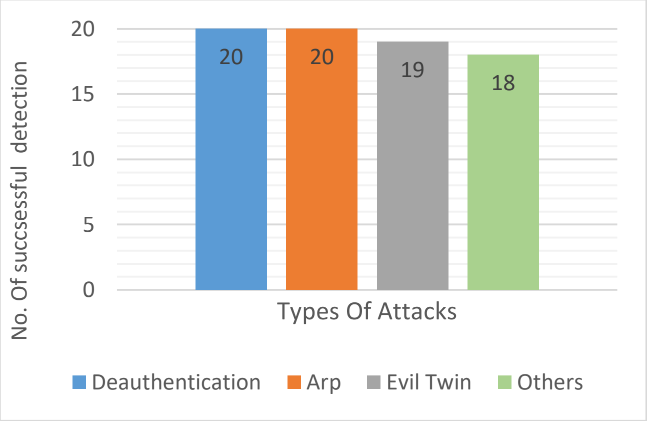


Fig. 1. Detection rate for low attack intensity

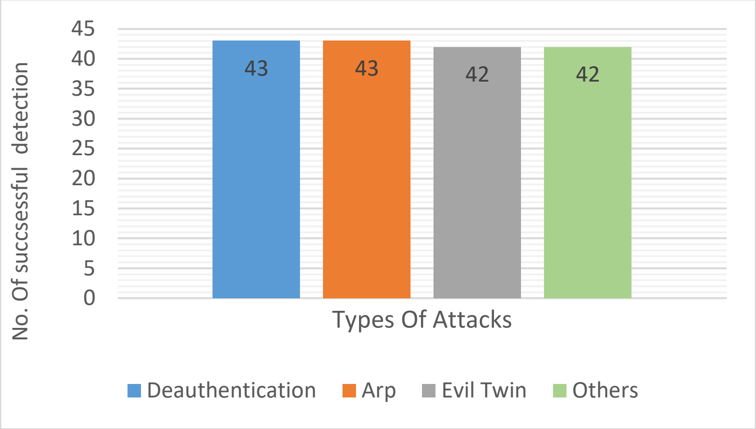


Fig.2. Detection rate for medium attack intensity

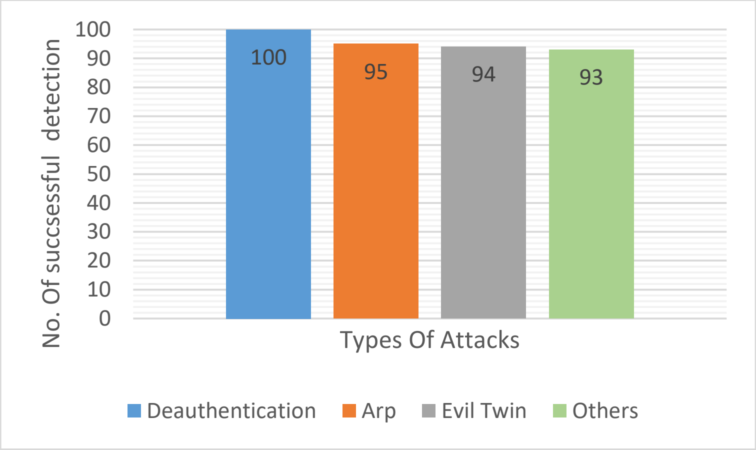


Fig.3. Detection rate for high attack intensity

To determine the effectiveness of our approach, we compared our model with different intensity level of detection rate, analyzing the detection rate generated by this framework. Below we present different accuracy level of our IDS based on attack intensity.

A. *Accuracy Rate*

Accuracy: $\frac{\text{No.of detection}}{\text{Total no.of attacks}} \times 100$

Detection rate for low attack intensity "Fig.1.": $\frac{77}{80} \times 100 = 96.25\%$

Detection rate for medium attack intensity "Fig.2.": $\frac{170}{180} \times 100 = 94.45\%$

Detection rate for high attack intensity "Fig.3.": $\frac{382}{400} \times 100 = 95.5\%$

VI. CONCLUSION

The main objective of this paper is to focus on detecting anomalies in the wireless network. Using rule-based detection, the known attacks in the network layer are detected accurately with a high detection rate, and the known attacks in the network layer are detected and prevented. We implemented a network intrusion detection and prevention framework for detecting and containing various network layer, data-link layer and transport layer attacks. Execution of the framework showed an impressive detection rate of 94.45% to 96.25% for low-intensity attacks to high-intensity attacks. The framework is able to monitor the network in real-time, ensuring the maximum possible security for the enterprise network. The framework could be extended further to include the monitoring and mitigation of application-layer attacks.

References

[1] Elbasiony, Reda M., Elsayed A. Sallam, Tarek E. Eltobely, and Mahmoud M. Fahmy. "A hybrid network intrusion detection framework based on random forests and weighted k-means." *Ain Shams Engineering Journal* 4, no. 4 (2013): 753-762.

[2] Bhuyan, Monowar H., Hirak Jyoti Kashyap, Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Detecting distributed denial of service attacks: methods, tools and future directions." *The Computer Journal* 57, no. 4 (2014): 537-556.

[3] Li, Wenchao, Ping Yi, Yue Wu, Li Pan, and Jianhua Li. "A new intrusion detection system based on KNN classification algorithm in wireless sensor network." *Journal of Electrical and Computer Engineering* 2014 (2014).

[4] Alheeti, Khattab M. Ali, Anna Gruebler, and Klaus D. McDonald-Maier. "An intrusion detection system against malicious attacks on the communication network of driverless cars." In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 916-921. IEEE, 2015.

[5] Shah, Syed Ali Raza, and Biju Issac. "Performance comparison of intrusion detection systems and application of machine learning to Snort system." *Future Generation Computer Systems* 80 (2018): 157-170.

[6] Hubballi, Neminath, and Vinoth Suryanarayanan. "False alarm minimization techniques in signature-based intrusion detection systems: A survey." *Computer Communications* 49 (2014): 1-17.

[7] Creech, Gideon, and Jiankun Hu. "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns." *IEEE Transactions on Computers* 63, no. 4 (2013): 807-819.

[8] Zhang, Ming, Boyi Xu, and Jie Gong. "An anomaly detection model based on one-class svm to detect network intrusions." In *2015 11th International conference on mobile ad-hoc and sensor networks (MSN)*, pp. 102-107. IEEE, 2015.

[9] Galal, Hisham Shehata, Yousef Bassyouni Mahdy, and Mohammed Ali Atiea. "Behavior-based features model for malware detection." *Journal of Computer Virology and Hacking Techniques* 12, no. 2 (2016): 59-67.

[10] Viegas, Eduardo K., Altair O. Santin, and Luiz S. Oliveira. "Toward a reliable anomaly-based intrusion detection in real-world environments." *Computer Networks* 127 (2017): 200-216.

[11] Panda, Mrutyunjaya, and Manas Ranjan Patra. "A comparative study of data mining algorithms for network intrusion detection." In *2008 First International Conference on Emerging Trends in Engineering and Technology*, pp. 504-507. IEEE, 2008.

[12] Amiri, Fatemeh, MohammadMahdi Rezaei Yousefi, Caro Lucas, Azadeh Shakery, and Nasser Yazdani. "Mutual information-based feature selection for intrusion detection systems." *Journal of Network and Computer Applications* 34, no. 4 (2011): 1184-1199.

[13] Misra, Sudip, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, and Mohammad S. Obaidat. "A learning automata-based solution for preventing distributed denial of service in internet of things." In *2011 international conference on internet of things and 4th international conference on cyber, physical and social computing*, pp. 114-122. IEEE, 2011.

[14] Garg, Akash, and Prachi Maheshwari. "Performance analysis of snort-based intrusion detection system." In *2016 3rd international conference on advanced computing and communication systems (icaccs)*, vol. 1, pp. 1-5. IEEE, 2016.

[15] Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri. "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system." *Expert Systems with Applications* 67 (2017): 296-303.