A Comprehensive Study on Intrusion and Extrusion Phenomena

Md. Abdul Hamid
Department of Information Technology
King AbdulAziz University
Jeddah-21589 Kingdom of Saudi Arabia

Marjia Akter
Department of CSE
University of Asia Pacific
Dhaka, Bangladesh

M. F. Mridha
Department of CSE
Bangladesh University of Business & Technology, Dhaka, Bangladesh

Muhammad Mostafa Monowar
Department of Information Technology
King AbdulAziz University
Jeddah-21589 Kingdom of Saudi Arabia

Madini O. Alassafi
Department of Information Technology
King AbdulAziz University
Jeddah-21589 Kingdom of Saudi Arabia

Abstract—This paper presents a comprehensive survey on intrusion and extrusion phenomena and their existing detection and prevention techniques. Intrusion and extrusion events, breach of security system, hamper the protection of the devices or systems. Needless to say that security threats are flourishing with new level of complexity making difficulty in recognizing them. Therefore, security is the remarkable issue at the core of developing a boundless, constant and reliable web. In this paper, our purpose is to unveil and categorize all possible intrusion and extrusion events, bring out issues related to events and explore solutions associated with them. Nevertheless, we suggest further recommendations to improve the security in these issues. We strongly believe that this survey may help understanding intrusion and extrusion phenomena, and pave the way for a better design to protect against security threats.

Keywords—Intrusion; extrusion; intrusion detection; security and survey

I. INTRODUCTION

No doubt, computing technology has changed the lifestyle of people drastically. All of these are happening through connecting devices, we call it networks. As devices are getting smarter and knowledgeable, people became much more dependent towards these devices. Things that come with comfort and contentment also brings issues and worries with it.

As networks are assisting individuals to communicate through the connecting devices, threats and breaches are getting more prominent. Computer security is the protection of electronic data and information against inner and outer, malevolent and vulnerability threats [1]. It renders protection as well as prevention from attacks and keeps the information secure. However, due to growth of the new technologies along with sophisticated devices, types and nature of the attacks are also changing [2].

All probable occurrences, contraventions, or approaching threats that violate system security are known as intrusion and extrusion events. More precisely, if an insider or outsider potentially intrudes the local system with his own remote system, it is known as intrusion event. Extrusion, known as an attack event, that generates from the local host system to take control over the system. It is usually done by the insider who is authorized to use any devices of the organization. To shield devices and networks against intrusion or extrusion events, security must be enough savvy and intelligent [3]. The concept of network security was first initiated in the late 1980s and since then experts have been exhorting to the unpredictable risk of numerous unsecured interconnected devices to the internet [4]. Now a days, numerous attacks events relate to intrusion and extrusion are continuously increasing concerns, devices like computer, refrigerators and even TVs are being used to dispatch malicious things to hackers. Hackers usually do not attack the devices themselves, but instead use other malicious devices to break into [5].

Some remarkable attack events related to intrusion and extrusion that affected the world most are RFIT botnet (December, 2018), ThinkPHP exploitation (11 December, 2018), D-link router exploitation, Shaolin botnet (exploitation of NETGEAR vulnerability, January, 2019), Mirai botnet [6][7], the botnet barrage, Notpetya ransomware attack (June, 2017), etc. Most of these attacks are not discussed and also not prevented even though systems have enough security. So, it is hard to accept that even after 28-years, system does not have enough security to detect or prevent such events. Without these exception, devices and systems also face some regular intrusion and extrusion attacks, such as Address resolution protocol attack, Internet Control Message Protocol (ICMP) attack, Fraggle attack, ICMP tunneling attack, Internet Protocol (IP) fragment attack, Malformed packet, Outbound raw attack, Ping-of-death attack, Distributed denial of services, Phishing, Supply chain attack, Router attack etc, to name a few.

Although the conventional solutions exist on the aforementioned attacks, still the occurrence of the mentioned remarkable events indicate that no systems are fully protected. We have explored a large number of surveys on attacks. Some surveys [8][9][10][11] discussed about the attacks in different layers. Some [12][13][14] have only discussed about DDoS attacks. Some [15][16][17] surveys mainly focused on intrusion detection and prevention systems. As network is expanding its region, more intrusion and extrusion events are occurring which are never discussed before.

This article incorporates up-to-date taxonomy, as well
as descriptions of important scientific work in the field of incursion and extrusion. It offers an overview of the current intrusion and extrusion detection system in an organized and thorough fashion so that interested academics may rapidly learn about essential areas of anomaly detection. The intricacy and implications of the various approaches and their assessment procedures will be explored.

There have been no papers that thoroughly cover infiltra-
tion and extrusion detection, outcomes, and various types of attacks. Furthermore, the advancement of intrusion-detection systems has resulted in the proposal of numerous distinct systems in the interim. This document provides up-to-date information on the subject.

We have presented a comprehensive and in depth study on intrusion and extrusion events. Mostly, extrusion attacks [18] and their detection systems [19] are not covered in existing surveys. For better understanding, we have discussed about attacks’ real-life examples, constructive definitions, attacks’ consequences, their complexities, limitations and merits, method comparison and efficiency, etc.

As time passes, a scenario with a relatively novel phenomena emerges, and network defenses are inadequate. Because of the ubiquity of computer networks and our ever-increasing reliance on them, becoming aware of the threat might have disastrous repercussions. The density of study on this topic is continually increasing, and more scholars are becoming involved in this field of work on a daily basis. The potential of a new wave of cyber or network assaults is not just a possibility to be considered; it is a known truth that can occur at any time. We think that study should not be restricted to the concerns raised in this work.

Nevertheless, most of these events have never been categorized for understanding of the problems. In our paper, we categorize the attacks on the basis of intrusion and extrusion and we provide a comprehensive discussion on those events for better understanding. We further relate those events in terms of TCP/IP layers. All these motivated us in writing this article. We firmly believe that our effort might convey indelible influence to the research community towards next level of perfection.

The rest of the of paper is organized as follows. Section 2 outlines the taxonomy of intrusion and extrusion events. The intrusion events are described in details in Section 3. Section 4 continues with the detailed description on extrusion events. We present a big picture in tabular form summarizing all the intrusion and extrusion events in Section 5. Finally, We present open challenges and future research Issues in Section 6 and at end, we conclude our research in Section 7.

II. TAXONOMY OF INTRUSION AND EXTRUSION

This paper categorizes different attacks into intrusion and extrusion events. Nevertheless, each of the attack is associated with any of the layers in TCP/IP protocol suite. Hence, our main classification also exhibits the corresponding layer where the attack occurs as demonstrated in Fig. 1. We have enlisted 14 intrusion and 10 extrusion events knowing that this list will grow in course of time. AS far as our knowledge perceives, this is the first attempt that accumulates all the intrusion and extrusion events, along with their comparative analyses.

III. INTRUSION EVENTS

This body of our work digs out the intrusion events manifesting their definitions, explaining how they occur and presenting the possible solutions for them along with figures wherever applicable. When a trusted insider violates the regular use of the system, then an intrusion event occur. The most common intruders may be the hackers, company’s employees, criminal enterprises etc. Any attack that roots from a remote system to a local system is considered to be intrusion. Suppose, an attacker disguises himself as a legitimate host and sends request (i.e. malware, malformed packets, emails, etc.) to the targeted PC. If an authorized user accepts the request, the malware or malformed packets might attack or freeze his PC or this request might lead him to a proxy fake website and force him to fill the personal information. Thus, the information will be revealed to the attacker. This process is known as intrusion event. Fig. 2 illustrates a generalized model of how intrusion event occurs.
A. TCP-ACK Storm Attack

This particular attack occurs over TLS/SSL connections along with TCP connections that remain unprotected. However, system having IPsec or link-layer encrypted connections is protective against this attack [20].

It is launched by a man in the middle attacker who only eavesdrops when needed and creates malicious packets. Theoretically, this attack [21] might spread in a limitless manner. The worst case can be N-packets of ACK-storm DoS attack may consume the overall bandwidth of a network. When a receiver receives an unacceptable packet from the attacker, the host acknowledges the packet and sends the expected sequence number to the attacker by using its own sequence number. In most cases, an attacker receives a packet with receiver’s sequence number larger than the one sent by a receiving client with the standard TCP connection. Even though, this packet is unacceptable, it generates an acknowledgment packet. This generated packet eventually generates other acknowledgment packets causing unlimited loops for each data packet. Whenever the ACK packet [22] is lost, it will not be retransmitted since it contains no meaningful data. ACK storm is less if the network drops more packets.

The Mitnick case (1994): A disguised attacker verily hacked the computers in the San Diego Supercomputer Center. This was happened to be the most secure computer system in US [23]. The financial services industry also experienced same type of attack. In March 2019, the attack was so sophisticated which was not previously seen before. Though it has an easy fix by tuning TCP or using a packet-filtering firewall system.

Fig. 3. TCP-ACK Storm: Attacker Changes One Network Packet with Malicious Packet.

Fig. 3 depicts the procedure of TCP-ACK storm with one packet that consists of three processes:

1) Attacker picks up a packet from connected network among host A and host B as there is an open port exist in the router.
2) Then, attacker generates one packet which will address to host A and sends with host A’s address to host B. Packet must have at least one byte of data. Packet must be inside the TCP connection.
3) Finally, hacker manages to send packets form Host A to Host B maintaining the time frame. As the attackers gets reply, it will continue in a loop of back and forth of packets.

The basic one packet TCP-ACK storm attack [24] can be further amplified to the Two-packets Ack-Storm attack, exhausting bandwidth and lengthening the session duration. This attack causes disruption of the regular web activities by sending huge traffic.

Some existing solutions related to this attack are shown in Table I.

B. Fraggle Attack

Fig. 4. An Example of Fraggle Attack.

Fig. 4 attacker is attacking the computers using BOT PC A to generate UDP flood to PC X, Y and Z. This UDP flood is then propagated to the nodes downward. Note that, port 7 is open for all computers and it supports character generation system. Eventually, the traffic will overwhelm the target PC T and block its normal functioning, resulting in fraggle attack.

The Fraggle attack is a type of amplification attack where UDP packets are dispatched to ports 7 and 19 depending on which one is open. Also, character generation service may run which is eligible for character generation. This intrusion may cause havoc to the system with the help of the insiders as they unintentionally help the hackers to flood UDP packets. As this attack is not new, all operating systems are protected from such attack. Therefore, no new such attacks [28] have been found nowadays, although in the late 90s, the attack was very acute.

A successful attempt of Fraggle attack may hang any system servers for an indefinite period of time (e.g., hours, days or even months). To Identify Fraggle attack, three types of techniques are introduced: traffic degree monitoring, source IP address monitoring, and packet attributes analysis. When the attack is detected, some countermeasures might be taken such as filtration [29], congestion control [30], Submissive trace back [31], Reproduction [32], etc.
TABLE I. STATE-OF-THE-ART SOLUTIONS OF TCP-ACK STORM

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raz et al 2011</td>
<td>Modifying the TCP</td>
<td>✓</td>
<td>✓</td>
<td>Hassle-some for the network architecture.</td>
<td>Generated everlasting TCP amplification</td>
<td>only 1% packet loss</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Neminath et al 2018</td>
<td>State transition model</td>
<td>✓</td>
<td>✓</td>
<td>Snatches TCP’s capability to re-synchronizing the sequence numbers</td>
<td>Real experiment of attack and detection in test bed setup</td>
<td>Close to 100%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Duc et al 2019</td>
<td>Hypervisor at close state</td>
<td>✓</td>
<td>✓</td>
<td>Analyzed TCP Ack Storm DoS attack against virtual network systems</td>
<td>Defining the packet size every-time is hard for the system</td>
<td>Takes 60sec to detect</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Topalova et al 2019</td>
<td>MLPNN structure</td>
<td>✓</td>
<td>✓</td>
<td>It doesn’t have prevention method</td>
<td>Analysis of automated system based on Multi layer neural network</td>
<td>Approximately 75%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

C. An ICMP Redirect Message Attack

ICMP redirect message sends out of bound message that passes the information to a host regarding the existence of more optimal routes through the server network. But this system is effectively misused by the attacker to redirect the traffic or information to his own system. In this attack, the hacker poisons the router by sending ICMP redirect message to the targeted host, so that all traffic uses optimal way for the destination. These attacks mostly happen on the port or network layer. These attacks can also cause problems if there exists firewall and non-deterministic traffic. Zimperium Mobile Security Labs have researched last year attack named “DoubleDirect” which can be generated through ICMP redirect message attack. It enables the attacker to redirect target’s traffic to attacker’s PC. Once the process is done, attacker may steal or inject payload to the victim’s PC. Machine learning approach generates the best detection rate till now.

In Fig. 5 host A is the source and host B is the destination. The files are supposed to transfer from source to destination through router. But the attacker redirects the messages by manipulating the router. Hence, the files finds the new path and goes to the attacker’s PC considering it as the destination. In what follows, the Table II enlists some existing solutions to this attacks.

D. Internet Protocol (IP) Fragmentation Attack

IP fragmentation attack exploits the IP fragmentation mechanism as an attack vector. Black nurse attack is one of the most common organizational names of IP fragmentation attack. Basically, it is based on sending crafted IP fragments in order to eliminate firewall services.

This process may occur in two ways as described in the following:

1) UDP and ICMP fragmentation attacks: This attack exploits the transmission of malicious UDP or ICMP packets exceeding the maximum transmission unit. The inability of reassembling these packets causes high resource consumption resulting in the victim server issues.

2) TCP fragmentation attacks: This attack, also regarded Teardrop attack, inhibits reassembly procedure of the TCP/IP for the fragmented data packets resulting in data packets overlap. Consequently, the server gets swamped.

Improving packet loss and 95% accuracy rate makes sparsely tagged fragmentation marking a best solution for this attack. Table II presents existing solutions related to this attack.

E. Perpetual Echo Attack

Perpetual echo attack, a fraudulent activity, takes place at port 7. Source port and the destination port perpetually echo each other when the connection is established. UDP requests are sent to a malicious IP address for all victims to get back their responses. The malicious source address is not the
### TABLE II. STATE-OF-THE-ART SOLUTIONS OF AN ICMP REDIRECT MESSAGE ATTACK

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerna et al. 2015</td>
<td>Centralized system</td>
<td>✗</td>
<td>✓</td>
<td>If Central server is unable to find correct match, it needs to send broadcast request. Time complexity increases</td>
<td>Analyze ICMP and Voting with Backward Compatibility, Less Cost, Minimal Traffic and Easily deployed</td>
<td>complexity O(logN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jaspreet et al. 2017</td>
<td>Signature based machine learning tool</td>
<td>✓</td>
<td>✗</td>
<td>Low accuracy rate</td>
<td>Application of machine learning tools</td>
<td>93% accuracy</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dalal et al. 2018</td>
<td>FIECast proxy service</td>
<td>✗</td>
<td>✓</td>
<td>No solution for DNS amplification originated from an external network towards a host inside a LAN</td>
<td>Crypto free solution without modification of protocol</td>
<td>complexity and convergence time can take up to 200 massages</td>
<td>Yes</td>
<td>Yes but some modification required.</td>
</tr>
<tr>
<td>Ahmed et al. 2018</td>
<td>AR-match technique</td>
<td>✓</td>
<td>✓</td>
<td>Weak hash function algorithm for high-security purpose</td>
<td>solving High complexity using Ar-match technique</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vegas et al. 2019</td>
<td>BigFlow</td>
<td>✓</td>
<td>✗</td>
<td>Only worked on limited bandwidth</td>
<td>Analyze the behavior of several traditional ML classifiers</td>
<td>Accuracy approximately 90%</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jonas et al. 2019</td>
<td>Open Flow</td>
<td>✗</td>
<td>✓</td>
<td>There is no rate limiting of the Virtual machine when sending to much traffic into the network</td>
<td>improvement of security of libvirt virtual machines connect via an Open vSwitch</td>
<td>Not mentioned</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The hacker remains disguised and the targeted user becomes the victim of large traffic. This may lead to DoS attacks on the UDP ports. Some UDP applications unconditionally respond to every datagram received. If a datagram is inserted into the network with one of these applications as the destination and another of these applications spoofed as the source, the two applications will respond to each other continually. Each inserted datagram will result in another perpetual echo conversation between them. In the worst case, the attacker’s attempt is to hide attacks or render them become untraceable. Ant colony optimization has more efficiency to generate true alarm rate while detecting the attack.

In Fig. 6, the attacker uses another PC’s IP address to remain hidden and sends UDP flood through port 7 of the router to the target PC to establish connection. If one connection is established, the affected PC will be working as BOT that sends UDP flood to other PC. Table IV presents existing solutions to this attack.

#### F. Internet Control Message Protocol (ICMP) Tunneling Attack

ICMP tunnel is created where the information flow may not be regulated by security technique. ICMP is used as an attack vector shield of IP-Sec gateway. In the worst case, attackers are able to disturb the network design architecture by doing malicious activity. An ICMP tunneling attack makes connection between the hosts, and ruins the firewall service in a way that it fails to alarm if any data sent via ICMP. It is a covert connection between hosts using ICMP messages.
and reply packets. It can be done by changing the payload data so that it contains the attacker’s data. So, if anyone uses ICMP messages, he may easily inject malicious data to be destined to the targeted PC. The targeted PC also replies into another ICMP message and returns it back.

In Fig. 7 host A is using an original server through a proxy server. Proxy server may be easily manipulated or authorized by the attacker without the knowledge of the firewall. ICMP messages are used as the payload in this figure. Thus, the information is routed through the attacker’s PC without anyone’s interference or knowledge.

**G. Smurf Attack**

Smurf attack mostly resembles to ping flood attack due to their similar nature of sending ICMP echo request packets. It, being an amplification attack vector [57], accelerates its damage potential through utilizing broadcast network characteristics. It is different than ping flood.

1990 is the year when first smurf attack [58] happened in University of Minnesota. It has effected more than 1 hour and chaining throughout the state. It has completely shut down many computers and servers. As a result, we face loss of

---

**TABLE III. STATE-OF-THE-ART SOLUTIONS OF INTERNET PROTOCOL(IP) FRAGMENTATION ATTACK**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bernstein et al 2012</td>
<td>Edwards-curve Digital Signature Algorithm</td>
<td>✗</td>
<td>✓</td>
<td>It is not a benchmark framework</td>
<td>Strong defenses against software side-channel attack</td>
<td>Drastically reducing the number of branches</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hasmukh et al 2018</td>
<td>Sparsely-Tagged Fragmentation Marking approach</td>
<td>✓</td>
<td>✓</td>
<td>Authentication of the marking at victim is needed to prevent compromise routers to spoof the marking</td>
<td>Improves the Probabilistic packet marketing by reducing the number of packets</td>
<td>95% accuracy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mahmud et al 2018</td>
<td>SecuFAN proposed tool</td>
<td>✓</td>
<td>✓</td>
<td>Mitigates the attack</td>
<td>verify authenticity and integrity</td>
<td>Completion time 35ms</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Chaoqin et al. 2018</td>
<td>Integrated IP Source Address Validation Architecture (ISAVA)</td>
<td>✓</td>
<td>✓</td>
<td>Filtering rate is not 100 percent accurate</td>
<td>Maximizes the SDN control pattern</td>
<td>Transfer time ‘8s</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bakker et al 2019</td>
<td>BGP Flowspec rules</td>
<td>✓</td>
<td>✗</td>
<td>It can not be used as the only way of defense</td>
<td>Specify rules on traffic and it’s limitations</td>
<td>Effectiveness is higher than Impact</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Al-Ani et al 2019</td>
<td>New mechanism against attacks</td>
<td>✓</td>
<td>✗</td>
<td>Can not block all kinds of packets</td>
<td>It can evade the OpenFlow firewall</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**TABLE IV. STATE-OF-THE-ART SOLUTIONS OF PERPETUAL ECHO ATTACK**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gupta et al 2014</td>
<td>Ant Colony Optimization</td>
<td>✓</td>
<td>✗</td>
<td>The performance of the model considerably varies on a larger and more congested network</td>
<td>real experiment and implementation</td>
<td>better detection rates and reduced false alarm rates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Okeke et al 2016</td>
<td>Prey Predator (PP) approach</td>
<td>✓</td>
<td>✗</td>
<td>Many issues like manifesting and buffer overflow exists</td>
<td>Described the application of Prey Predator approach</td>
<td>Not mentioned</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
data and slowdowns. We need to IP broad casting to eliminate Smurf attack.

Following describes the procedure of Smurf attack.

1) The malware generates a network packet attached to a fake IP address. There is a ping message inside the packet. Upon receiving these spoofed packets, the nodes echo back causing a loop eventually leading to a complete denial of service.

2) An insider may directly inject smurf Trojan or it may be accidentally downloaded from forged e-mail or web site. Typically it will remain as it is until activated by the attacker. Consequently, a good number of Smurfs are integrated with rootkits, allows hackers to create backdoor for system access.

Table V shows state-of-the-art solutions of smurf attack.

H. Router Attack

Router attacks mainly exploit the vulnerabilities in the networking protocols that lead to inconsistency in software and weak authentication. It normally occurs in the network layer. Attacks, that can be a part or origin from router attacks, are mainly brute force and denial of service attacks. When it occurs, it impacts network services and business operations.

2018’s report from eSentire shows 539% of increase in router attackers since 2017. ACI (American consumer institute) also found 84% WiFi routers are under risk of cyber attacks or malicious activity. As, people are not aware of security vulnerabilities properly, hackers takes the chance. Black hole routers can detect most types of the router attack and can be modified if the attacker’s way changes with time.

In Fig. 8 attacker modified the valid protocol to make new protocol which is malicious and may cause havoc to the system. Some attacks that might disrupt the performance of the router is discussed in the following.

1) Brute Force: Brute force attack is a method where trial and error process is used to get data such as user’s password or pin details. In this attack, an automated software generates a large number of close to accurate guesses as to get the desired value. It may be used by the attacker to crack the encrypted data. It may also be used to test the security system of any organization.

2) Packet Mistreating Attack: Router attacks may lead to packet mistreating, mostly like DoS attacks. These packets get mistreated by injecting malicious packets to confuse and overwhelm the system.

3) Routing Table Poisoning: A routing table in a router is not immune to protection and encryption vulnerabilities. Routing table may poison the whole routing routine. These attacks are achieved by manipulating the packet information that are routed through the router.

4) Hit and Run Attacks: This attack is also known as test hacks, and occurs when malicious data is injected into a router. However, the injection process may or may not be successful. The main aim of the is to disturb the environment of a system.

5) Persistent Attacks on Routers: Persistent attack is somewhat similar to hit and run, but in this attack, the injection process becomes successful and the attacker may gain control over the system. After injecting, it will continue it’s intended work. The attacker will continue to add malicious packets and confuse the routing table thereafter.

Table VI depicts some existing solutions related to router attack.

I. Slow and Fast Port Scans Attack

Port scanning is one of the dangerous network intrusions for getting exploitable communication channel between the attacker and the target. Attacker uses attack to discover service to get into the network. It consists of probing a host in a network for open host. It not only scans but also gathers information that attempts to profile the services running on a potential target. Port scan attack on 4G router of HUAWEI company, detected last year, is one of the recent port scan attack complained by the consumers. Artificial immune systems and fuzzy logic provide more accuracy and also have a robust model compared to other models.

In Fig. attacker uses two scanners to send malicious requests disguised as service messages for scanning system.
messages are spaced in time at least in minutes, but mostly in hours or days. It may take weeks or even months to complete the process. As time passes by, network noise can destroy the scans which might remain unnoticed. Suspicion may be avoided through scanning target slowly by the attacker. Attackers send probe packets in every 5 or 15 minutes. Since slow scan does not create any deviation in the normal traffic, detection of this scan through anomaly and real time detection is very difficult.  

2) An attacker scans the port in order to change the traffic settings. It can last for minutes or some fractions seconds. 

Table VII shows some of the existing solutions of slow and fast port scan.

J. Restricted IP Attack

It allows an attacker to limit access to the site to an attacker’s defined set of IP addresses. If anyone attempts...
TABLE VII. STATE-OF-THE-ART SOLUTIONS OF SLOW AND FAST PORT SCAN ATTACK

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mathieu et al 2018</td>
<td>Scan Chain Encryption</td>
<td>✓</td>
<td></td>
<td>It is only applied on non-modifiable cores</td>
<td>Secure and cost efficient mechanism</td>
<td>100% fault coverage</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Markus et al 2018</td>
<td>Classification algorithm</td>
<td>✓</td>
<td></td>
<td>It is not applied on real world network data.</td>
<td>Problem setting and the underlying flow-based data are analyzed</td>
<td>Not used any accuracy measure-ment</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manuel et al 2019</td>
<td>Time-aware metrics in NIDS evaluations</td>
<td>✓</td>
<td></td>
<td>Application of time-aware machine learning models is missing</td>
<td>Used time-aware evaluation metrics for the early intrusion detection problem, identifying advantages and disadvantages</td>
<td>0.85 recall and precision</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mohammad et al 2019</td>
<td>Fuzzy Rule Interpolation</td>
<td>✓</td>
<td></td>
<td>Prevention method is missing</td>
<td>Effectively detect the very slow and slow port scans based solely on the sparse fuzzy rules.</td>
<td>Not mentioned</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Hartpence et al 2020</td>
<td>Sequential Neural Networks</td>
<td>✓</td>
<td></td>
<td>No new algorithm is focused</td>
<td>Sequential NN architecture</td>
<td>99% accuracy</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GUSTAVO et al 2020</td>
<td>Artificial Immune Systems and Fuzzy Logic</td>
<td>✓</td>
<td></td>
<td>Real network environment should be considered</td>
<td>Method comparisons are discussed with efficiency</td>
<td>99.9% accuracy</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

for site access from different IP address not belonging to the list of authorized IP addresses, it will be redirected to an access denied page. No blocks will be rendered, and no JavaScript will be added to the page. The module also has various configuration options including white list or blacklist pages, bypass IP checking by role, and alter the output when blocked. System administrator uses this option for enforcing IP-based restrictions to minimize unwanted traffic.

Over 30% of secure access cloud customers are using the IP address restriction to limit access to corporate resources from a specific set of IP addresses, while still performing strong user authentication.

![Fig. 10. Restricted IP Attack: Attacker Restricts the IP to Stop Valid users to Visit the Website.](image)

In Fig. 10, attacker sends commands to the BOT PC to attack the main server in order to modify the restrict IP list, so that which PCs are in the restricted list may easily get access in the server.

Table VIII shows some of the existing solutions of the restrict IP option.

K. Address Resolution Protocol(ARP) Attack

![Fig. 11 shows how ARP attack occurs. Let us assume, two hosts PC1 and PC2 are connected through a switch. An attacker, say PC3, is also connected in the same switch. It has modified the MAC address of other hosts with his own MAC address which is EE:EE:EE:FF:FF:FF. In such way, it may get the desired data that is being transferred between the system and the host.](image)

ARP spoofing is an attack that occurs when a hacker dispatches fake ARP messages to the local system network. It ends up connecting a hacker’s media access control (MAC) address with the IP address of the device that existed in the network. Once the attacker is connected with the system device, he may get his desired information from that device by disguising his own identity. This attack enables attackers to intrude, edit or steal data from the system and also stops data from being transmitted between the system and the host.

In April 2018, Cisco Talos released information on the Sea Turtle campaign that hijacked and redirected traffic from more than 40 government and enterprise organizations using ARP.
TABLE VIII. STATE-OF-THE-ART SOLUTIONS OF RESTRICTED IP OPTION

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code Modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manju et al 2014[77]</td>
<td>SQL Injection detection mechanism</td>
<td>✔</td>
<td>X</td>
<td>Not enough efficient to integrate in a system.</td>
<td>Detects more SQL injection vulnerabilities hidden behind the inadequate blacklist defense.</td>
<td>Detects all attack in the test case</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Kim et al 2019[80]</td>
<td>ARP table update state-based detection approach</td>
<td>✔</td>
<td>X</td>
<td>100 ARP replies is the limit. Attacker may do less reply to attack.</td>
<td>Analyzes SDN, SFC, and the vulnerabilities</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Fig. 11. Occurrence of ARP Attack: Attacker Manipulates ARP Table to Connect as Legitimate Server.

As ARP intrusion can have many forms, detection can be difficult and needs perfection. We can have lots of false alarms, which could lead the team ignoring the alarms without investigation. The most simple way to get rid of this intrusion is to use static, read-only entries for the services in the ARP cache. There exists a good number of research efforts presenting intelligent methods to get rid of this intrusion.

Table IX shows some effective detection and prevention systems of ARP intrusion.

**L. Ping of Death Attack**

A ping of death (PoD) sends a malicious ping to a computer. The maximum size of an IPv6 packet including the IP header is 65,535 bytes. Many ancient computers[88] cannot handle this large size of packets and will crash if it receives one. This attack exploits early TCP/IP implementations including Windows, Mac, Linux and other network devices like router and fax etc. Since sending packets in large form causes IP fragmentation by attacker, targeted system can get lot of ICMP packets via ping without waiting for the reply. Once the system becomes vulnerable to this attack, other attacks may dig in like Trojan horse. Cloud flare protection can demolish the PoD attacks before they reach the targeted host. There is no specific works related to this attack. Certainly, some DDoS attack related paper added the solution of this intrusion as a small part of it. The low rate[89] “Ping of death” attack, dubbed BlackNurse, effects firewalls from Cisco, Zyxel, and possibly Palo Alto in 2016.

Fig. 12 shows a general model of such attack. In this figure, BOT have sent ICMP spoofed ping messages in the network. The server will broadcast ping flood resulting in other PCs connected with the server unable to work. This mostly happens on the data link layer. This attack is less common today as many computers are immune to this attack. Generally in this attack, attacker transmits malformed or oversized packets exploiting ping command that results in system crash.

One of the solutions is to add a verification to reassemble the function to make sure data packets size don’t get maximized. Other solution can be creating a memory buffer to handle the space of every incoming packets. Cloud flare
### TABLE IX. STATE-OF-THE-ART SOLUTIONS OF ARP INTRUSION

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghazi et al. 2016 [83]</td>
<td>ARP table, ARP filtering, authenticating</td>
<td>✗</td>
<td>✓</td>
<td>All ways of ARP spoofing is not discussed and detected.</td>
<td>Defense implementation</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sweta et al. 2018 [84]</td>
<td>Secondary ARP table</td>
<td>✓</td>
<td>✓</td>
<td>Time interval between hosts is fixed. Authorized connection may take longer time can be concluded as attack.</td>
<td>Real time implementation</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jing et al. 2019[32]</td>
<td>ARP reply message process in OpenFlow platform</td>
<td>✓</td>
<td>✗</td>
<td>The system is not flexible enough to integrate</td>
<td>Discussed new features in OpenFlow network</td>
<td>Min.5679.76 Max.8307.89</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sanguankotchakorn et al. 2019[83]</td>
<td>Hybrid controller</td>
<td>✓</td>
<td>✗</td>
<td>Detecting Switched DDoS attack is taking around 9 seconds which is really slow.</td>
<td>Discussed Controller mitigation process</td>
<td>Entropy falls 1 to 0 with time</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sanguankotchakorn et al. 2019[86]</td>
<td>A non-cryptography-based and called MR-ARP</td>
<td>✓</td>
<td>✗</td>
<td>It takes longer time to determine the secure path</td>
<td>Analyzed Mitigation technique</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Al-An et al. 2020[87]</td>
<td>Match-Prevention</td>
<td>✗</td>
<td>✓</td>
<td>the bandwidth consumption of Match Prevention is 18% higher</td>
<td>Discussed security challenges</td>
<td>100% success rate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

![Fig. 12. Ping of Death: Spoofed Ping Messages Add with the Broadcast IP of the Server to Manipulate clients PC.](image1)

![Fig. 13. SYN Flood Attack: Attacker Sends Command to BOT PC Sends SYN Traffic to Server.](image2)

There is no specific works related to this attack. Certainly, some DDoS attack related paper added the solution of this intrusion as a small part of it.
### TABLE X. STATE-OF-THE-ART SOLUTIONS OF SYN FLOOD ATTACK

<table>
<thead>
<tr>
<th>Reference</th>
<th>Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hussain et al 2016</td>
<td>Three Way Counter Algorithm for Attack Detection</td>
<td>✓</td>
<td>✓</td>
<td>Cloud security is not justified</td>
<td>HoneyPot method is emphasized</td>
<td>Attack detection rate of Tcp port 60%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Kshirsagar et al 2016</td>
<td>System architecture for efficient detection</td>
<td>✓</td>
<td>✓</td>
<td>Authors have used only 4 features to detect attack which is not efficient</td>
<td>load of CPU is minimized after The attack</td>
<td>Cpu load value ranges from 8-11% after detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Kumar et al 2018</td>
<td>SAFETY</td>
<td>✓</td>
<td>✓</td>
<td>Victims from multiple destination can not be detected</td>
<td>SAFETY brings 13 percent regarding processing delay experienced by a legitimate node</td>
<td>100% TPR while has approximately 27% FPR</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bae et al 2018</td>
<td>DDoS Cyber-Shelter model</td>
<td>✓</td>
<td>✓</td>
<td>Authentication data can get access to the service even during the attacks are made. Data can be manipulated</td>
<td>a cost-effective way</td>
<td>lowest false positive rate of 0.0003% at maximum</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Zhong et al 2018</td>
<td>Three modules, such as sniffer module, analysis module and active defense module</td>
<td>✓</td>
<td>✓</td>
<td>Most network administrators do not have set up such rules, it gives potential attackers the convenience of attacks</td>
<td>provide reference for tracking SYN flood attack</td>
<td>Network administrators are no longer required</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Khalid et al 2019</td>
<td>SYN Flood Attack Detection Based on Bayes Estimator (SFADBE)</td>
<td>✓</td>
<td>✓</td>
<td>Bandwidth issue exists</td>
<td>low cost and robust threshold is 8.0</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dang et al 2019</td>
<td>SSP (a coordination of the SDN Open-flow switch)</td>
<td>✓</td>
<td>✓</td>
<td>94 percent accuracy which is not good enough for integration in a system</td>
<td>SSP improves the successful connection rate and average connection retrieval time</td>
<td>SSP can reduce the number of HOCs by 68% in case of 100 pkt/s rate, and by 86% in case of 500 pkt/s.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Evmorfos et al 2020</td>
<td>Random Neural Network with Deep Learning</td>
<td>✓</td>
<td>✓</td>
<td>Neural Network's recurrent structure needs to improve</td>
<td>substantially better attack detection and significantly lower false alarm rate</td>
<td>Accuracy 80.7%</td>
<td>False</td>
<td>No</td>
</tr>
</tbody>
</table>

**M. SYN Flood Attack**

In a SYN flood attack, the attacker does not respond with the expected ACK to the server. Also, the attacker might spoof the source IP address in the SYN packets which causes the server to transmit SYN-ACK to a fake IP address. Due to the creation of a half open connection [99] [91], the malicious client consumes server resources unnecessarily and prohibits the server in establishing connections to the other clients. One of the ways of mitigating this attack is the use of Cloud flare between the target server and the SYN flood.

A well-documented DDOS attack was introduced in 1996 by panix. In 2005 [100] [101], the website of this company got hijacked again in the period of holiday. It took off their sleep to get everything back together.

Fig. 13 depicts a sample scenario of this attack. In this
figure, by sending initial connection request through SYN packets, the hacker makes the ports of the Victim server overwhelmed.

Some state-of-the-art solutions of SYN floods attack are presented in Table X.

N. Malformed Attack

Malformed packet consists of malware or other malicious elements. In this attack, a BOT PC sends incorrectly formed packets to the victim to crash the system by receiving attacker instruction. The massive combination of DDoS and IoT attacks have been blown up in late 2016. This is the largest one till now. It has extremely terrifying capability of exploiting about 1.2 TB per seconds. Best way to filter this attack is to allow legitimate traffic and discard floods of packets like ICMP or UDP.

Categorizing it as follows: (i) IP address malformed attack and, (ii) IP packet malformed attack.

1) IP address malformed attack contains the same source and destination IP address which confuses the target system resulting in system crash.

2) In this attack, system is forced to process and waste additional time due to randomizing the optional fields in IP packet along with setting all QoS bit to 1. This attack might lead to the system crash if combined with multiple attackers.

Some existing solutions related to this attack is enlisted in Table XI.

IV. Extrusion Events

In this section, we excavate the extrusion events. In what follows, we present their definitions, explain how they occur and outlined the possible solutions with necessary figures and tables, wherever applicable. As stated earlier, extrusion event might bring vulnerability to the remote system device by getting injected with malware or by opening a malicious web page etc.

Fig. 15 shows a generalized model of an extrusion in a system. Basically, in Fig. 15 two hosts are connected with the same LAN. LAN connects to the switch and switch connects to the internet. Firewall is the barrier between the attacker and the target. Also, numerous attackers and BOT PC (created by attackers) are connected with the internet through LAN. If any user of that host clicks on malicious websites, or opens malware related software, then extrusion may occur. As numerous attackers frequently upload malware through internet and also send phishing e-mails, it is highly probable to get infected by clicking malicious links or downloading malicious files. This section describes all possible extrusion events and the related existing counter measures.

A. Supply Chain Attack

According to November 2018 study by Opus Ponemon Institute, 59 percent of organizations in UK and US has already experienced data tempering and compromised security issues by their third party stakeholders.

Fig. 16 shows a general model of a supply chain attack. In this figure, attacker changes the script of any targeted server which makes the server compromised. Eventually, the malicious or compromised server makes other server compromised and thus the chain continues.

Due to the repeated attack on different servers, it is almost impossible to detect it. Other attacks only target the victim
TABLE XI. STATE-OF-THE-ART SOLUTIONS OF MALFORMED ATTACK

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patil et al 2019 [105]</td>
<td>Threshold value set for detect malformed packet</td>
<td>✓</td>
<td>✓</td>
<td>The mechanism misapprehends some malformed packets. However, they are dropped as excess flood packets due to crossing the threshold limit</td>
<td>All kinds of flood attack can be detected</td>
<td>Not mentioned</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Venugopal et al 2019 [106]</td>
<td>Generates ACL</td>
<td>✓</td>
<td></td>
<td>Legitimate addresses requires to be minimized to run the system</td>
<td>Detailed DDos attack</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Fig. 16. A Chain System of Attack: an Attacker Changes the Script of the Server to Manipulate System

The common default passwords, common default setting is also an concerned issue.

Popular destruction-of-service attack vectors include:

1) Business Email Compromise (BEC): Business email compromise attacks uses the ID of someone on the particular network to trick the victim into sending money or info to the attacker. The most common victims are those who use wire transfers to send money to international clients.

2) Cyberwarfare: Cyberwarefare generally refers to attacks that relate to cybernet. In every case, it has been observed that a terrorist group or hacker groups aimed at a particular nation or political organization to do their work done. This event is also new to the network system, and no specific solution has come out.

C. Distributed Denial of Services (DDoS) Attack

DDoS attack is a fraudulent attempt to make any service unavailable to the users. It can be launched from globally distributed compromised devices, also known as Botnet. It is hard to differentiate legal user traffic from malicious traffic when dispatched across many points of origin. This may cause long-term reputation damage.

The Google attack in 2017, the AWS DDoS attack in 2020, the Mirai Krebs and OVH DDoS attacks in 2016, the Mirai Dyn DDoS attack in 2016, the Six Banks DDoS attack in 2012 are the most famous DDoS attacks that caused most harm to the organization. Traceback approach has both prevention and
Fig. 18. DDoS Attack: Several Bot PCs Compromised the Server to Attack the Target.

detection method and also has an efficient code enhancement system.

Fig. 18 depicts a model of how DDoS occurs. In this figure, the attacker commands the BOT computer to send illegitimate traffic in order to flood the system server PC. From the system server PC, users/clients also get illegitimate traffic, causing the system unavailable.

It can be categorized into three types [109], which are:

1) Volume Based Attack: This attack is related with ICMP flood attack, UDP flood attack and also spoofed packet flood attack. Attacker intends to change the value of the bandwidth of victim’s site. The parameter of this attack is measured in bits/second.

2) Protocol Attack: This type of attack is related with fragment packet attack, syn flood attack, ping of death and smurf attack and many more. Here, the attacker attacks actual server data, communicating devices between hosts, firewalls as well as load balancer. The parameter of this attack is measured in packet/second.

3) Application Layer Attack: This attack is related with Post/Get php flood attack, slow attack and many more. Mainly the attacker targets the victim’s windows or OpenBSD vulnerabilities. Attacker makes the victim believed that the request is innocent and legitimate. The main goal of the attack is to crash the main server of the system. The magnitude of this attack is measured in requests per second.

Solutions related to this event are presented in Table XII.

D. Phishing Attack

Phishing attack targets the victim’s computer through mails, messages or via link by pretending to be a legitimate person or organization to lure the victim. By doing these, the attacker gets to know the victim’s personal sensitive data [115] for example, ID card information, credit card information and passwords, etc.

In 2020, Doharty associate claimed their customer faced one phish, two phish, red phish, blue phish in the name of phishing attacks. They also fell for it and gave away their password details. Support vector machine and Naive Bayes algorithm have approximately 100% efficiency to defend any kind of phishing attacks.

Usually, the attacker performs the phishing attack using one of the following ways:

1) The attacker can hand over the important information.
2) Attacker spams out the phishing messages to many people, so that at least some people will be the customers of some specific bank or organization.

Phishing attack may be categorized as follows.

1) Spear Phishing: Spear phishing may attack a particular person of an organization often with content tailor made only for the victim. The attacker requires sufficient knowledge about the organization to produce such content. The content may relate to victim’s colleagues, names and relationship with employees. With this kind of data, attacker may generate a trusted email.

2) Clone Phishing: The attacker attaches a malicious link or attachment utilizing a previously delivered valid email. Once the user clicks on the link, he becomes the victim. Then the attacker gets his desired information from that victim using certain measurements. Victim may give organization’s confidential data to the attacker in some cases [116].

Fig. 19. Scamming a Victim’s Computer using Phishing Attack: Attackers Send Mails to Victim’s Computer to collect Information by Clicking on Scam Website.

Fig. 19 illustrates how a phishing attack takes place. In this figure, attacker sends malicious e-mails or other documents. If the user clicks on a link provided by an attacker given through a message, then he may provide his username, password, etc. to that website which may resemble as real but actually is a malicious site. Now attacker may enter into his account. Most of the messages are sent to the HR staff with the infected file that disguised as a job seeker’s resume, for instance [117]. Most of these attachments are often zip files, or documents with embedded code. It plays a significant role in other attacks like Trojan and ransomware.

Some state-of-the-art solutions to this attack are presented in Table XIII.

E. URL Poisoning Attack

URL poisoning attack, also addressed as location poisoning, tracks down any web user’s page sequence or information
TABLE XII. STATE-OF-THE-ART SOLUTIONS OF DDoS

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code Modification</th>
<th>Applied to all platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alan et al 2016</td>
<td>Artificial Neural Network (ANN) algorithm</td>
<td>✓</td>
<td>✓</td>
<td>It is not designed for encrypted packets</td>
<td>detect DDoS attacks based on specific characteristic features (patterns)</td>
<td>98% accuracy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Zhuotao et al 2018</td>
<td>Umbrella</td>
<td>✓</td>
<td></td>
<td>It hampers user’s privacy</td>
<td>capable to deal with large scale attacks involving millions of attack flows</td>
<td>90%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mehr et al 2019</td>
<td>SVM based solution</td>
<td>✓</td>
<td></td>
<td>Feature correlation needs be more precise. Traffic generation and real-time performance is missing</td>
<td>use time pattern for prevention</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David et al 2019</td>
<td>Statistical approach</td>
<td>✓</td>
<td></td>
<td>Real time implementation is missing</td>
<td>higher detection rate and accuracy and lesser processing time</td>
<td>99.6% accuracy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Saxena et al 2020</td>
<td>A third party auditor (TPA) based packet traceback approach</td>
<td>✓</td>
<td>✓</td>
<td>Threshold value should vary with real time update. But the value is fixed.</td>
<td>Easy DDoS prevention in the cloud environment</td>
<td>97.4% accuracy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wang et al 2020</td>
<td>Multilayer perceptrons</td>
<td>✓</td>
<td>✓</td>
<td>If feedback mechanism works incorrectly, the system will get wrong knowledge</td>
<td>correct the detector when it performed poorly</td>
<td>92%</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

by adding an ID when a user visits a particular website. Exploiting this ID thereafter, the attacker can determine the visited web pages. Accumulating this sort of information might be helpful to comprehend different user activities including how a user gets to a page, what he likes and so on. This may lead to tie in user behavior to demographics.

Israeli researcher Omer Gil has introduced a method called as deception attack. It has many advantages over cached pages. It mainly targets e-commerce and online payment gateway. This attack occurs on by exploiting cookies. In this attack, user may never find a way to opt out from the trap. A system that is infected by URL poisoning will assign an ID to the victim when he visits the first page. Then, this ID will be a part of the URL without victim’s knowledge. All information related to this ID might be recorded as long as he visits the same page. It may also be attached with the browser when a victim visits any original site.

In Fig. 20, attacker intentionally enters ID to the victim’s page and stores the number sequence. Further, attacker uses the data for the illegal purpose. Our rigorous exploration in this very topic reveals that no specific research works exist to the solution of this attack.

Fig. 20. URL Poisoning Attack: Victim’s Visited Page is Recorded using ID Number.

F. Outbound Attack

A traffic that generates from the insiders is known as outbound traffic [127]. The main reason of locking down outbound attack as securely as inbound is DDoS attack. If an open port is not available to move out traffic, a system network may be immune to this event [128]. Fig. 21 shows a sample scenario of an outbound attack.

Outbound attack can lead to Wild botnet attack that maybe be worst case of this attack.

In this figure, hacker sends traffic to overwhelm the target

![URL Poisoning Attack Diagram](image-url)
<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jain et al, 2018</td>
<td>PHISH-SAFE: URL Features-Based Phishing Detection</td>
<td>✓</td>
<td></td>
<td>Accuracy is relatively low. trained using more than 33,000 legitimate URLs</td>
<td>90% accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Adebowale et al, 2019</td>
<td>An Adaptive Neuro-Fuzzy Inference System (ANFIS) based robust scheme</td>
<td>✓</td>
<td>✓</td>
<td>SVM still shows less accuracy than other algorithms. Efficient and integrated features of images, frames and text of phishing websites</td>
<td>98.5% accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Rao et al, 2019</td>
<td>an application named as Jail-Phish</td>
<td>✓</td>
<td></td>
<td>Similarity score may not be able to detect correctly every time. a real time application for the phishing detection accuracy of 98.6%</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Suleman et al, 2019</td>
<td>Uniform Resource Locator (URL) based phishing detection</td>
<td>✓</td>
<td></td>
<td>Prevention method is not discussed Improved feature selection method</td>
<td>95 percent accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Liew et al, 2019</td>
<td>A supervised machine learning technique of Random Forest (RF)</td>
<td>✓</td>
<td></td>
<td>Need real time implementation to show accuracy of the mechanism. Analyzes 11 best classification features</td>
<td>97.5 percent accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Mao et al, 2019</td>
<td>A learning-based aggregation analysis mechanism</td>
<td>✓</td>
<td></td>
<td>F1 score is relatively low. enable automated page-layout-based phishing detection techniques</td>
<td>93.7 percent accuracy</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Jain et al, 2019</td>
<td>A machine learning based approach</td>
<td>✓</td>
<td></td>
<td>If any attacker alters page internal resources such as image, text, code etc then their approach will predict false result too. language independent and detect the website written text</td>
<td>98.4 percent accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Chiew et al, 2019</td>
<td>A new hybrid ensemble feature selection framework</td>
<td>✓</td>
<td></td>
<td>Computationally expensive. automatic, flexible and robust feature selection</td>
<td>94.6 percent accuracy</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Orunsolu et al, 2019</td>
<td>Support Vector Machine and Naïve Bayes algorithm</td>
<td>✓</td>
<td>X</td>
<td>If any attacker tries to copy a web page using advance tools, then the outlook of such website will be a replica of the legitimate page. extracted features automatically</td>
<td>99.96% accuracy</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

PC. As, he sends payload with the traffic, target may click on this. Once clicked, the server is compromised. Nevertheless, the user also establishes outbound HTTPS connection with the attacker which surely tunnels back and takes control over the system. In most cases, the employee has no idea that they have been compromised, nor does their employer. In such a case, the computer needs to be reinstalled but at least the rest of the network will still be intact. If this connections are restricted to specific protocols and can only be established by the specific users or authenticated users, then the attacks become ineffective. There is no specific research study found on this very topic.

G. Violating Traffic Regulation Conditions Attack

Traffic regulation means to achieve the required quality of services goals such as bandwidth, load, delay,
Fig. 21. Outbound Attack: Hacker Sends Payload to Target PC to Comprise the Server.

security etc. Our concern is the issue of security [130]. Policies that relate to traffic regulation might monitor the TCP connections on all IP addresses and ports in a system. IDS traffic regulation (TR) policies for TCP ports limits the total number of connections an application has been active at one time. Attacker may violate the traffic regulation policies by modifying TCP connection of the hosts. It could result in establishing TCP connection by the attacker with the target’s host to do malicious activity. After successfully connected with the host, it takes full control over host. To the best of our knowledge, we have not found any significant research endeavors addressing the solutions on this attack.

H. Social Engineering Attack

Social engineering attack is one of the most popular and easy ways to get any information from any person that may relate to any organization. The attacker designs the process so deceptively that any person may easily be manipulated. In the context of cyber security, this is used to lure victim to disclose sensitive data, perform security breaches or infect system unknowingly [130].

Shark Tank 2020, Toyota 2019, Cabarrus County 2018, Ethereum Classic 2017, Democratic Party 2016, Ubiquiti Networks, Sony Pictures, Target South Carolina Department of Revenue, RSA, etc. are the most popular social engineering attacks till date.

During the process of conversation, victims are not aware of the intention of the attacker. Therefore, they easily fall in trap. Many types of explicit methods are used to seduce or attract the victim to start a conversation [137]. It may be classified into two types which are, (i) Hunting and (ii) Farming [137].

1) Hunting approach executes the social engineering attack by doing minimum conversation between the target and the hacker. Once hacker is successful in getting the information, he terminates the conversation between them. This process is the most used one in the cyber world. It can encounter a single operand at once [138].

2) Social engineering farming is not something that is practiced often. This is used for some particular situations. To get the information, attacker needs longer period of time to keep himself connected with the user. During this process, the conversation or interaction may change between them. Some cases, target may understand the tactics. If not, then user may get blackmailed by the hacker [138].

In Fig. 22 attacker collects information about the victim and makes a customized attack for the victim. Then, he collects response from the victim and uses the sensitive information against him. The main focus of this attack is to ignore manual security process by deceiving user. They may get the weakest link to attack people emotionally [137].

Table XIV lists some existing solutions researched so far.

I. Malware Attack

Malware [139] can be a file or software program which is harmful for a system or computer. They may vary from function to function that can do theft, encryption or delete any important data, alter or hijack programs of a system, and monitor any activity of the users without their permissions. Attacker uses ways to spread the malware through physical or virtual means. Some malwares are automatically downloaded to the system as they are designed without the user’s knowledge [140]. Some types of malware, that have new techniques, are designed to not only deceive the users but also to detour the anti-virus easily. Anti-sandbox technique can detect malware and delay execution after it leaves the sandbox [141].

Fear has been upgraded its level during the time of corona virus. Many cyber criminals, and ransomware are introduced in this period. Covidlock is one of them [142].

Some types of malware include the following:

1) Virus: A virus is a type of malware that may execute itself without any command and may spread on its own.

2) Worm: A worm can replicate itself without any host or user program. It spreads itself without human intervention and is directed by malware attackers.

3) Trojan: A trojan virus disguised as legitimate to get access to a system. If it is activated, it starts to follow installations. It can execute their malicious actions by itself.

4) Spyware: Spyware is made to get a collection of information of data on a user device and monitor activity of the victim without their knowledge. It is like keeping an eye on users.

5) Ransomware: Ransomware infects a system, encrypts its data and demands a certain amount of ransom money from the victim in exchange for fixing the system.

6) Rootkit: A rootkit is created by a hacker to get access into the administration level of the target’s system. If it is installed, the system gets threat from root or deep infrastructure.
### TABLE XIV. STATE-OF-THE-ART SOLUTIONS OF SOCIAL ENGINEERING ATTACK

<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sawa et al 2016 [131]</td>
<td>Natural language processing techniques</td>
<td>✓</td>
<td>✗</td>
<td>Total CPU time for execution of all stages was 2421 seconds which is long</td>
<td>applicable to many attack vectors sincerely on dialog text</td>
<td>Precision 100 percent and recall 60 percent</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Abeywardana et al 2016 [132]</td>
<td>A layered defence strategy SERA</td>
<td>✓</td>
<td>✗</td>
<td>Classification needs more enhancement.</td>
<td>Detailed information of attacks Not mentioned</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Dan et al 2019 [133]</td>
<td>Data Protection Mode</td>
<td>✓</td>
<td>✓</td>
<td>Attack ratio is still high enough to harm the organization.</td>
<td>Modular design, More state transitions and Incorporates and implements the data protection process Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Lansley et al 2019 [134]</td>
<td>A two-stage approach that detects social engineering attacks and based on natural language processing</td>
<td>✓</td>
<td>✗</td>
<td>More algorithm needed to evaluate the program for comparison.</td>
<td>evaluated using both real and semi-synthetic conversation points accuracy 0.917</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Mouton et al 2019 [135]</td>
<td>SEADM</td>
<td>✓</td>
<td>✗</td>
<td>The method is not adhered to every request.</td>
<td>Explored social engineering as a domain Not mentioned</td>
<td>yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

7) Backdoor: A backdoor is a form of virus or remote access Trojan. It constructs a backdoor into a compromised system that facilitates the attacker for remote access without causing any disturbance of user’s security issues.

8) Adware: The main purpose of the adware is to trail the browsing history of a user with the intention of displaying advertisements. This allures an user to make any purchase.

9) Keylogger: Keylogger is a type of monitoring system which nearly sees everything that users actually do on the computers including emails, web pages etc.

State-of-the-art research works on malware attack are depicted in Table XV.

#### 7. IoT Botnet Attack

A group of computers, appliances and connected devices [149] [150] that have been controlled by a hacker or a hacker group for illegitimate purpose is known as IoT botnet. It is made up of computers that can be accessed remotely by a hacker without the victim’s knowledge. It forwards the data to the other computers through internet. Botnets are increasing and have become more advanced since the evolution of IoT. It may target many devices and appliances on any infrastructure and inject them with malicious payloads or packets. The evolution of IoT increases the risk of security breaches [151] [152].

In Fig. 23, the IoT is comprised of diverse devices including cameras, routers, DVRs, wearable and other embedded technologies.

Three botnets have been occurred in 2018. It gave rise to different domains, but all of them are inter connected. Each of them are skillful and ingenious system which can detect fraud. Google, White Ops, and other tech companies came together at that time to invade the operation of this attack.

![Connected IoT Devices](image)

**Fig. 23. Connected IoT Devices: Botnet Devices are Connected to Every Possible Device Through Internet.**

As most of the devices are Linux and Unix based, they become the common target of the attacker. Since in those system, an executable format exists which is modifiable by the attacker. The modified file becomes the malware that targets SSH or telnet network protocols. Once the system is compromised, the payload is delivered to the system through installation and thus turned into a botnet. [153] [154]. Some existing solutions related to this attack is summarized in Table XVI.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrea et al 2018</td>
<td>MADAM</td>
<td>✓</td>
<td>✓</td>
<td>Performance measurement is missing</td>
<td>developed a binary rewriting tool</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mishra et al 2019</td>
<td>VMANALYZER</td>
<td>✓</td>
<td>✗</td>
<td>Imbalanced dataset which leads to uncertainty in the normal traces of processes.</td>
<td>feature vector is built for each process in monitored TVM</td>
<td>4.7-100 percent accuracy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maiorca et al 2019</td>
<td>Command-and-control botnets</td>
<td>✓</td>
<td>✗</td>
<td>Details of methods are missing.</td>
<td>categorize known vulnerabilities of learning-based PDF malware</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Gan et al 2020</td>
<td>A dynamical propagation model</td>
<td>✗</td>
<td>✓</td>
<td>Adjusting system parameter is difficult.</td>
<td>discussed behavior of malware under an infected cloud environment</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Alazab et al 2020</td>
<td>An automated process by using a scoring and grouping technique</td>
<td>✓</td>
<td>✗</td>
<td>Use of more machine learning algorithms may achieve more accurate results.</td>
<td>assist in the process of malware forensic investigation</td>
<td>94.3 percent accuracy</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mishra et al 2020</td>
<td>KVMInspector</td>
<td>✓</td>
<td>✗</td>
<td>It is not incorporated with network monitoring functionalities</td>
<td>Considered as security check</td>
<td>81.25%–99.92%(UNM) and 95.43%–97.81%(Elog)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

V. INTRUSION AND EXTRUSION EVENTS: A BIG PICTURE

In this section, we have recapitulated all the intrusion and extrusion events by means of their types, how and where they occur, consequences and existing solutions, as presented in Table XVII.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Proposed Method/ Model</th>
<th>Detection</th>
<th>Prevention</th>
<th>Limitations</th>
<th>Merit</th>
<th>Efficiency</th>
<th>Code modification</th>
<th>Merit Efficiency</th>
<th>Applied to all platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meidan et al 2018</td>
<td>N-BaIoT</td>
<td>✓</td>
<td>✓</td>
<td>Connection between IoT devices that has low prediction rate in their network is not allowed due to security policies.</td>
<td>Create experimental setup for dataset</td>
<td>.0007 FPR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tzagkarakis et al 2019</td>
<td>Sparsity representation framework</td>
<td>✓</td>
<td>✓</td>
<td>The decision threshold is estimated using only begin training instances.</td>
<td>Lightweight method</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Banerjee et al 2019</td>
<td>Honeynet</td>
<td>✓</td>
<td>✓</td>
<td>Malicious binaries, attack replays are not considered.</td>
<td>Provides activity logs of the intrusion attempt</td>
<td>100 percent accuracy</td>
<td>yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dange et al 2020</td>
<td>CNN-based deep learning model</td>
<td>✓</td>
<td>✓</td>
<td>There is a difference in power consumption as it negotiates the condition of various WiFi signal.</td>
<td>Provides details of IoT attacks</td>
<td>Not mentioned</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Attack name</td>
<td>Type</td>
<td>How it occurs</td>
<td>Where it occurs</td>
<td>Consequences</td>
<td>Existing methods/ models</td>
<td>Complexity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP ACK storm attack</td>
<td>Intrusion</td>
<td>It can exploits a design architecture in the TCP specifications</td>
<td>Application layer</td>
<td>Effect the websites regular work by sending lots of traffic</td>
<td>Modifying the TCP , State transition model, hypervisor at close state, FMVEA and multitet semantic, MLPNN structure</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraggle attack</td>
<td>Intrusion</td>
<td>Dispatches numerous numbers of malicious traffic to overwhelm a router’s transmittable address in the network</td>
<td>Transport layer</td>
<td>Cripple any servers for hours, or even days</td>
<td>SACL filtering method</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An ICMP redirect message attack</td>
<td>Intrusion</td>
<td>A message is designed for informing a host that there is a more optimal route is available so that user may redirect to the malicious traffic system.</td>
<td>Transport layer</td>
<td>Cause problems in fire-walled environments where flow traffic patterns are non-deterministic</td>
<td>BigFlow, OpenFlow, PreCast proxy service, AR-match technique, Signature based and Machine learning tool, Centralized system</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet protocol fragment attack</td>
<td>Intrusion</td>
<td>Attacker uses the fragmentation protocol within IP to attack the system.</td>
<td>Transport layer</td>
<td>System may freeze or overwhelmed because of the attack.</td>
<td>BGP, Flowspec rules, Edwards-curve Digital Signature Algorithm, Sparingly-Tagged Fragmentation Marking approach, SecuPAN proposed tool, Integrated IP Source Address Validation Architecture (ISAVA)</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perpetual echo attack</td>
<td>Intrusion</td>
<td>Any illegitimate activity happens at port 7 in the form of spoofing any system knows as perpetual attack.</td>
<td>Transport layer</td>
<td>Large amount of network traffic causes delay.</td>
<td>Prey Predator (PP), Ant Colony Optimization, Modified protocol specifications</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Control Message Protocol (ICMP) tunneling attack</td>
<td>Intrusion</td>
<td>Attacker inserts malicious data by using ICMP tunneling and echo the packet to remote computer</td>
<td>Network layer</td>
<td>Any sensitive data or access in private sector may done by this attack.</td>
<td>A novel mechanism of 5 algorithms, Covert Channel Detection using Support Vector Machine, Stateless and monitoring model, Stateless model</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smurf attack</td>
<td>Intrusion</td>
<td>The attacker creates a malicious network packets attached to a IP and send it to the victim’s system</td>
<td>Network layer</td>
<td>It can freeze company servers for days and months. Data loss can happen</td>
<td>SDN based technique, an enhanced History-based IP Filtering scheme, Pattern Matching Techniques, principal component analysis</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router attack</td>
<td>Intrusion</td>
<td>Injecting vulnerabilities to the router</td>
<td>Network layer</td>
<td>Attacks impact network services and business operations distributed</td>
<td>Distributed router shadow, an Interest flow balancing method, Run-time protector and Restart-time protector, Pushback method, Scalable Method</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slow and fast port scan attack</td>
<td>Intrusion</td>
<td>May blend into the network noise never exceeding detection thresholds and exhausting detection system state</td>
<td>Network layer</td>
<td>Creates changes in the normalcy of the traffic.</td>
<td>Distributed router shadow, an Interest flow balancing method, Run-time protector and Restart-time protector, Pushback method, Scalable Method, Exposure map, Distributed Cooperative Model, ADRISYA, Scan Chain Encryption, Scanning Classification algorithm, time-aware metrics in NIDS evaluations, Fuzzy Rule Interpolation</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack name</td>
<td>Type</td>
<td>How it occurs</td>
<td>Where it occurs</td>
<td>Consequences</td>
<td>Existing methods/ models</td>
<td>complexity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted IP attack</td>
<td>Intrusion</td>
<td>Attacker restricted the access to the particular site and defined set of IP address</td>
<td>Network layer</td>
<td>Restrict user’s website</td>
<td>ARP table update state-based detection approach, SQL Injection detection mechanism, An adaptive framework, Packet filtration, payload distribution model, generic authorization framework</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP attack</td>
<td>Intrusion</td>
<td>When a hacker dispatches false ARP messages to the local network and connect it with the system.</td>
<td>Data link layer</td>
<td>Hackers can steal sensitive information from the targeted computers.</td>
<td>Discrete event system, IP probing, ARP table, ARP filtering, Centralized methodology (central server), Novel mechanism, Secondary ARP table etc.</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping of death attack</td>
<td>Intrusion</td>
<td>Attacker sends malicious ping to a system to flood the system.</td>
<td>Data link layer</td>
<td>It can crash, damage or freeze the victim’s computer by sending oversized malformed packet</td>
<td>No specific solution</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYN floods attack</td>
<td>Intrusion</td>
<td>Connected with syn false packet and TCP connection established</td>
<td>Data link layer</td>
<td>Attacker makes the system unavailable for the user by flooding with legitimate traffic.</td>
<td>GT-IDS-DJ Method, Three Way Counter Algorithm for Attack Detection, system architecture for efficient detection, The Adaptive threshold algorithm and the cumulative sum (CUSUM), DDoS Cyber-Shelter model, three modules, such as sniffer module, analysis module and active defense module, AR modeling, SYN Flood Attack Detection Based on Bayes Estimator (SFADB), SSP—a coordination of the SDN Open-flow switch</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malformed attack</td>
<td>Intrusion</td>
<td>Incorrectly formed IP packets are formed and sent to the victim to crash the system.</td>
<td>Data link layer</td>
<td>The system of the victim may get confuse and gets crashed</td>
<td>TCP trace module, Threshold value set for detect malformed packet, Generates ACL</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply chain attack</td>
<td>Extrusion</td>
<td>A value-chain or third-party attack occurred by an outsider</td>
<td>Application layer</td>
<td>Causes major data breach</td>
<td>No solution yet</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DeOS (destruction of services) attack</td>
<td>Extrusion</td>
<td>Targets an organization’s entire online presence as well as their ability to recover from the attack afterwards</td>
<td>Application layer</td>
<td>Could put businesses in a position where they have to rebuild infrastructure from scratch or pay a high ransom to the attackers</td>
<td>No solution yet</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed denial of services (DDOS) Attack</td>
<td>Extrusion</td>
<td>Malicious attempt to make an online service unavailable to users</td>
<td>Application layer</td>
<td>Make any website or system and servers unavailable to legitimate users</td>
<td>Graphic model, central control of SDN, Artificial Neural Network (ANN) algorithm, Umbrella, SVM based solution, statistical approach, a third party auditor (TPA) based packet traceback approach, An Unsupervised Approach, multilayer perceptrons</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack name type</td>
<td>How it occurs</td>
<td>Where it occurs</td>
<td>Consequences</td>
<td>Existing methods/ models</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing attack</td>
<td>Targets are contacted via email, text or link disguised as legitimate institution</td>
<td>Application layer</td>
<td>Steals sensitive information</td>
<td>An Adaptive Neuro-Fuzzy Inference System (ANFIS), Jail-Phish, URL-based detection system, light-weight deep learning algorithm, Uniform Resource Locator (URL) based method, supervised technique of Random Forest (RF), learning-based aggregation analysis mechanism, Machine Learning techniques and algorithms etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL poisoning attack</td>
<td>Track the identification number added by the attacker in the web browser and gets information from that victim when he/she visits the particular site</td>
<td>Transport layer</td>
<td>Tracks user to get desired information</td>
<td>No specific solution yet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound attack</td>
<td>Attacker tunnels back in over that connection to take control of the employees’ computer</td>
<td>Network layer</td>
<td>Unlimited email or file transfers might let the attacker enter into the network and get sensitive information outside</td>
<td>No specific solution yet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Violating Traffic regulation conditions attack</td>
<td>Violating traffic regulations</td>
<td>Network layer</td>
<td>Causes any discontinuity to the network normal behavior</td>
<td>No solutions yet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering attack</td>
<td>Gather information about someone by exploiting human weakness that inherits every organization</td>
<td>Network layer</td>
<td>Can control one life through virtual manipulating</td>
<td>Data Protection Mode, two-stage approach that detects social engineering attacks and based on natural language processing, SEADM, CANDY, SMS-based second factor authentication, multi-layered shield, natural language processing techniques, layered defence strategy SERA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td>Any program or file that is harmful injected through any way in the system</td>
<td>Data link layer</td>
<td>It thefts, encrypts, or deletes the data. It can spy on computer activity without user knowledge or permission</td>
<td>A dynamical propagation model, an automated method by using a scoring and grouping technique, KVMInspector, VMANALYZER, command-and-control botnets etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT botnet</td>
<td>It is accessed from a remote computer without the owners’ knowledge and set forward transmissions to other computers on the Internet</td>
<td>Physical layer</td>
<td>It causes breaches to all related IoT devices</td>
<td>N-BaIoT, model, CNN-based learning, MOPSO, sparsity representation framework, Honeynet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

End of Table
VI. Open Challenges and Future Research Issues

Theoretically, it is expected from computer security mechanisms to prevent attacks and to provide solutions to the threats. If not impossible, it should be capable of predicting future threats. As a consequence, towards fulfilling this expectation, researchers around the globe are working to design, develop and implement increasingly secure systems.

Our effort of excavating numerous research papers conveys what aspects of intrusion and extrusion have been studied and what have not. What concerns us the most is that there is no unified policy or mechanism exists that could be applied to an enterprise system to tackle the possible intrusion or extrusion events. We strongly believe that there is a need for a smart system that might learn and take effective countermeasures against the impending threats. Therefore, we would like to make suggestions for future directions to the research community.

One of the challenges is to build new data sets. Due to the rapid advancement of technology, innovative attack methods also evolve. Protocol developed using existing old data sets do not reflect the impending innovative threats to be mitigated or neutralize. As a natural consequence, research on this very issue requires tremendous attention.

With the advent of deep learning technique, security research got new research dimension. However, one of the limitations of using this in security, particularly in intrusion detection, is to balance between high accuracy and minimal false alarms. This limitation mainly presents in the Convolution neural networks (CNN). Also, using Feed-forward neural networks (FNN) for multi-class classification is a limiting factor. The third limitation includes performance degradation in IDS under heavy traffic load. Furthermore, using Deep Neural Network (DNN) causes higher execution time due to the larger training dataset. However, developing new methods using deep learning, if not impossible, might mitigate the mentioned limitations.

One of the important concerns regarding present research endeavors is that researchers apply variations of machine learning, if results are convincing, they conclude their methods may be applicable for certain scenarios. However, we argue that an interpretable or explainable reasons should be there is to why certain machine learning methods work better.

Software defined network (SDN) mingled with machine learning approaches is the new trends in IDS. However, SDN itself might be the interest to the attacker. This obviates to excavate the vulnerabilities in SDN. On a different note, since SDN network controller suffers from performance degradation for larger network, new research efforts are essential to address the challenge.

We believe that each attack is unique and attackers are very intelligent. Irrespective of the nature and severity of attacks, the future research on this domain should consider not only the detection and prevention of existing attacks but also should predict the future threats. If not impossible, if that is achieved to a certain extent, research community may render meaningful and fruitful contributions to the society.

The difficulties that lay ahead of us in infiltration and extrusion detection systems have grown significantly in recent years. The following is a list of them.

- Inability to decrease the amount of false positives, reducing IDS efficiency. A good IDS should have a high level of accuracy and recall, as well as a low rate of false positives and false negatives. A key concern is how one can have faith in the outcome.
- The amount of time it takes to analyze such a vast amount of data for training is enormous.
- In IDS, improving classification accuracy is a significant goal. It forces to concentrate on a multi-classifier system.
- Due to a lack of computer resources and a significant increase in targeted assaults, a real-time intrusion detection system is urgently required. However, putting it into practice in a real-world setting is difficult.
- A problem is the lack of a common assessment dataset that can mimic real-time IDS.
- Many research employ the selection of functions to reduce the computer complexity in function reduction work. To carry out the data deduction task, greater focus is necessary.
- A combination detection and anomaly detection approach is necessary.

It’s not an amazing mountain to create an effective detecting system. The above mentioned difficulties might greatly contribute to this trip.

VII. Conclusion

Network attacks are a daily security concern that may be mitigated. As a result, it is critical to explore more complicated security alternatives than simple firewall systems today. This article discusses numerous forms of attacks on TCP/IP networks at each layer, the merits and limits of Intrusion Detection System (IDS) and Extrusion Detection System (EDS) solutions, IDS and EDS efficiency and code environment, and utilized techniques for both. Some intrusion detection systems have progressed significantly, and the data generated by software and the tactics used by attackers are getting increasingly sophisticated. This makes it difficult to discern between genuine system use and potential infiltration. A false alarm, also known as a false positive, occurs when an IDS erroneously detects an activity as a probable intrusion. Poorly designed intrusion detection systems, particularly behavior-based intrusion detection systems, can generate a large number of false positives. In the case of passive-response intrusion detection systems, this might result in an overwhelming administrative load (getting paged for a false alarm every 3 minutes becomes annoying very quickly). In the case of active-response IDS, this might potentially result in a DoS situation. If the IDS incorrectly blocks a valid user’s IP address. As a result, before adopting an IDS, considerable preparation and thought are required. The paper isolates the concerns and concentrates on why IDS and EDS are required for delivering secure network service. Because one of the most important criteria for enabling privacy is security.
unauthorized access, deletion, use, alteration, or disclosure of personal data should all be safeguarded by appropriate security precautions. Work on system design and algorithm design for secure communication over complicated networks can be done in the future.

In this paper, we have provided the thorough survey and the state-of-the-art of existing intrusion and extrusion events and introduced a refined security analyses by means of threats, counter measures and future research directions. The comprehensive review presented in our work may provide designers with new means to look for solutions in a unified manner according to several security and resource parameters. Finally, we are aware that attacks other than those considered in this paper might exist. We strongly believe that addressing provable security of intrusion and extrusion events is a challenge for future research, but not impossible.

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES


A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, “6lowpan: a study

C. Shannon, D. Moore et al.

D. Kundur and K. Ahsan, “Practical internet steganography: data

E. Viegas, A. Santin, A. Bessani, and N. Neves, “Bigflow: Real-

time and reliable anomaly-based intrusion detection for high-speed


485, 2019.

J. Andre and J. Naab, “Open vswitch configuration for separation of


C. Shannon, D. Moore et al., “Characteristics of fragmented ip

traffic on internet links,” in Proceedings of the 1st ACM SIGCOMM


A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, “Glowan: a study on
gos security threats and countermeasures using intrusion detection

system approach,” International Journal of Communication Systems,


Z. Trabelsi, S. Zeidan, and K. Hayawi, “Denial of firewalling attacks

dof: The case study of the emerging blacknurse attack,” IEEE Access,


A. Al-Ani, M. Anbar, R. Abdullah and A. K. Al-Ani, “Proposing a new

approach for securing dchpv6 server against rogue dchpv6 attack

in ipv6 network,” in International Conference of Reliable Information


in coap,” in 2016 3rd MEC international conference on big data and


D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang,

“High-speed high-security signatures,” in International Workshop on

Cryptographic Hardware and Embedded Systems. Springer, 2012,

pp. 124–142.

H. Patel and D. Jinwala, “Stf-dm: A sparsely tagged fragmentation with

dynamic marking an ip traceback approach.” Int. Arab J. Inf. Technol.,


M. Hossain, Y. Karim, and R. Hasan, “Secupan: A security scheme to

mitigate fragmentation-based network attacks in flownap,” in Proceed-

ings of the Eighth ACM Conference on Data and Application Security


C. Zhang, G. Hu, G. Chen, A. K. Sangaiha, P. Zhang, X. Yan, and

W. Jiang, “Towards a sdn-based integrated architecture for mitigating


D. Bakker, “Impact-based optimisation of bgp flowspec rules for ddo


A. A. Al-Ani, M. Anbar, S. A. Laghari, and A. K. A. Al-Ani, “Mechanism to

prevent the abuse of ipv6 fragmentation in openflow networks.” PloS


A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, A. Ingle, and V. Ambhore,

“Intelligent perpetual echo attacks detection on user datagram protocol

port 7 using ant colony optimization,” in 2014 International Conference on


K. Ghirardello, C. Maple, D. Ng, and P. Kearney, “Cyber security of

smart homes: Development of a reference architecture for attack

surface analysis,” 2018.

A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, A. Ingle, and V. Ambhore,

“Intelligent perpetual echo attack detection on user datagram protocol

port 7 using ant colony optimization,” in 2014 International Conference on


M. Okeke and A. Blyth, “Adopting flocks of birds approach to predator

for anomalies detection on industrial control systems,” International

Journal of Mathematical, Computational, Physics, Electrical and


D. Kundur and K. Ahsan, “Practical internet steganography: data


L. Jacquin, V. Roca, and J.-L. Roch, “Icmp: an attack vector against

ipsec gateways,” 2013.

M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, “Detecting slow

port scan attacks on secure circuits through scan chain encryption,” in

Proceedings of the 23rd International Conference on Design, Automation


M. Da Silva, M.-L. Flottes, G. Di Natale, and A. B. Vigna, “Slow port

scanning detection,” in Proceedings of the 2014 ACM workshop on Visu-


M. Dabbagh, A. J. Ghandour, K. Fawaz, W. El Hajj, and H. Hajj,

“Slow port scanning detection,” in 2011 7th International Conference


233.

M. Da Silva, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, “Preventing

scan attacks on secure circuits through scan chain encryption,” IEEE

Transactions on Computer-Aided Design of Integrated Circuits and


M. López-Vizcaíno, F. J. Novoa, D. Fernández, V. Carneiro, and F.

Scheda, “Early intrusion detection for os scan attacks,” in 2019

IEEE 18th International Symposium on Network Computing and


M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, “Detecting slow

port scan using fuzzy rule interpolation,” in 2020 2nd International


B. Hartpence and A. Kwasinski, “Combating tcp port scan attacks

using sequential neural networks,” in 2020 International Conference on

Computing, Networking and Communications (ICNC). IEEE, 2020,


G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proençna, “Artificial


