A Comprehensive Study on Intrusion and Extrusion Phenomena

Md. Abdul Hamid[1]
Department of Information Technology
King AbdulAziz University
Jeddah-21589 Kingdom of Saudi Arabia

Marjia Akter[2]
Department of CSE
University of Asia Pacific
Dhaka, Bangladesh

M. F. Mridha[3]
Department of CSE
Bangladesh University of Business &
Technology, Dhaka, Bangladesh

Muhammad Mostafa Monowar[4]
Department of Information Technology
King AbdulAziz University
Jeddah-21589 Kingdom of Saudi Arabia

Madini O. Alassafi[5]
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 sophisticate 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 exhorted 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 infiltration 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.

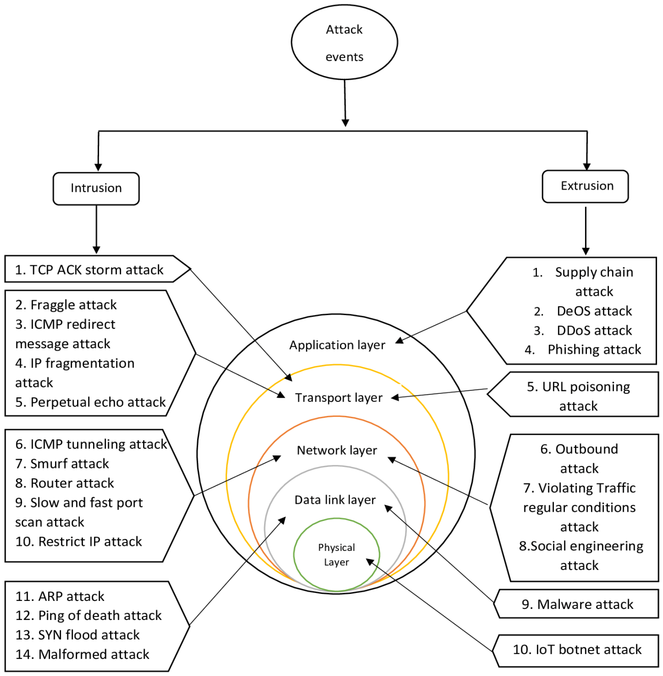

Fig. 1. An Overall Taxonomy of Intrusion and Extrusion Events.

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.

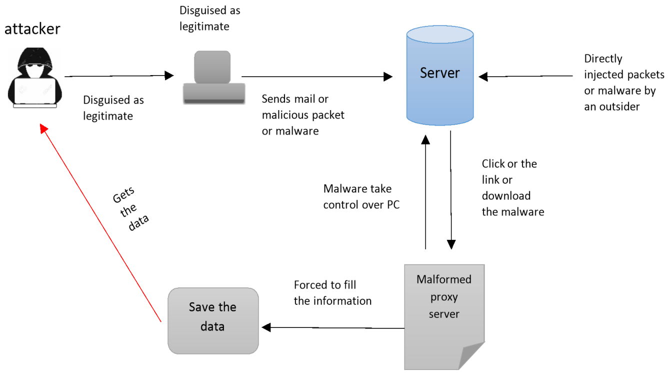
attacker
Disguised as legitimate
Disguised as legitimate
Sends mail or malicious packet or malware
Server
Directly injected packets or malware by an outsider
Malware take control over PC
Click or the link or download the malware
Gets the data
Forced to fill the information
Malformed proxy server
Save the data

Fig. 2. A Generalized Model Depicting the Occurrence of an Intrusion Event.

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.

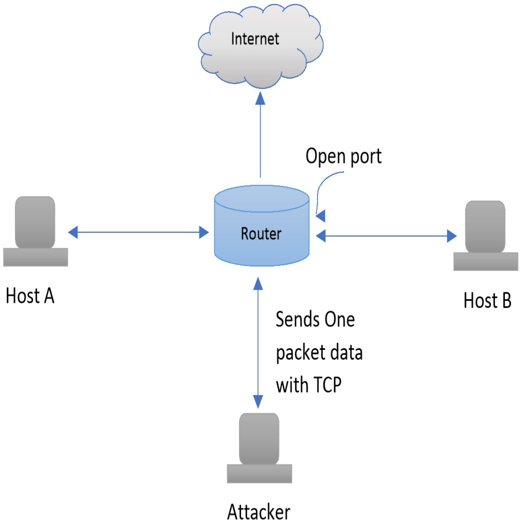

Fig. 3. TCP-ACK Storm: Attacker Changes One Network Packet with Malicious Packet.

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

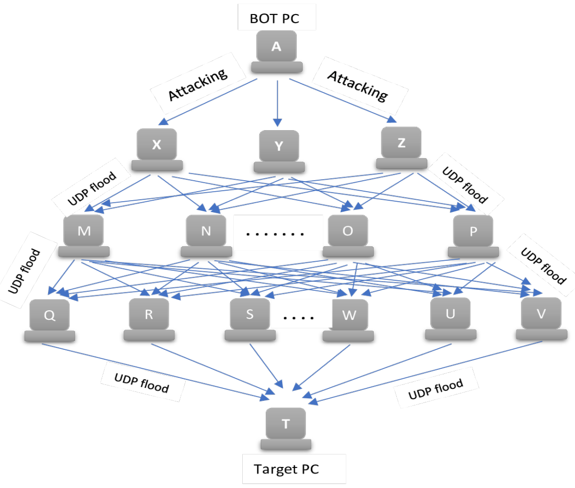

Fig. 4. An Example of Fraggle Attack.

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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Raz et al 2011[25]	Modifying the TCP	✗	✓	Hassle-some for the network architecture.	Generated everlasting TCP amplification	only 1% packet loss	Yes	Yes
Neminath et al 2018 [22]	State transition model	✓	✗	Snatches TCP's capability to re-synchronising the sequence numbers	Real experiment of attack and detection in test bed setup	Close to 100%	Yes	Yes
Duc et al 2019 [26]	Hypervisor at close state	✓	✗	Analyzed TCP ACK Storm DoS attack against virtual network systems	Defining the packet size every-time is hard for the system	Takes 60sec to detect	No	No
Topalova et al 2019 [27]	MLPNN structure	✓	✗	It doesn't have prevention method	Analysis of automated system based on Multi layer neural network	Approximately 75%	Yes	Yes

C. An ICMP Redirect Message Attack

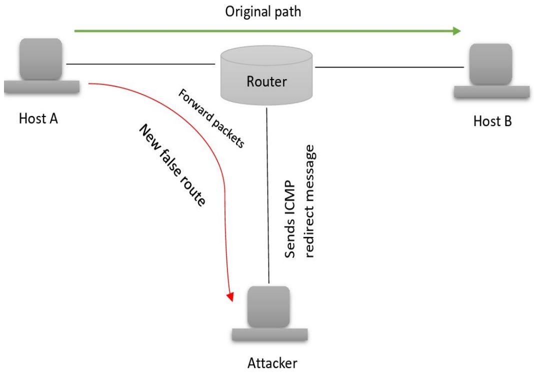

Fig. 5. ICMP Redirect Message Attack: Attackers Manipulating ICMP Messages between Server and Client's PC.

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 [33]. Zimperium Mobile Security Labs have researched last year attack named "DoubleDirect" which can be generated through ICMP redirect massage attack. It enables the attacker to redirect target's traffic [34] 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 [40] [41].

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 [42].

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

1) UDP and ICMP fragmentation attacks: This attack [43] 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 [44].

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

E. Perpetual Echo Attack

Perpetual echo attack [51], 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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Prerna et al. 2015 [35]	Centralized system	✗	✓	If Central server is unable to find correct match, it needs to send broadcast request. Time complexity increases	Analyze ICMP and Voting with Backward Compatibility, Less Cost, Minimal Traffic and Easily deployed	complexity O(logN)	Yes	Yes
Jaspreet et al. 2017 [36]	Signature based machine learning tool	✓	✗	Low accuracy rate	Application of machine learning tools	93% accuracy	No	No
Dalal et al. 2018 [33]	PrECast proxy service	✗	✓	No solution for DNS amplification originated from an external network towards a host inside a LAN	Cryto free solution without modification of protocol	complexity and convergence time can take upto 200 massages	Yes	Yes but some modification required.
Ahmed et al. 2018 [37]	AR-match technique	✗	✓	Weak hash function algorithm for high-security purpose	solving High complexity using Ar-match technique	Not mentioned	Yes	Yes
Viegas et al. 2019[38]	BigFlow	✓	✗	Only Worked on limited bandwidth	Analyze the behavior of several traditional ML classifiers	Accuracy approximately 90%	Yes	Yes
Jonas et al. 2019[39]	Open Flow	✗	✓	There is no rate limiting of the Virtual machine when sending to much traffic into the network	improvement of security of libvirt virtual machines connect via an Open vSwitch	Not mentioned	No	No

attacker's correct address. Hence, the hacker remains disguised and the targeted user becomes the victim of large traffic. This may lead to DoS attacks [52] 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, attacker's attempt is to hide attacks or render them and become untraceable. Ant colony optimization has more efficiency to generate true alarm rate while detecting the attack

In Fig. 6, 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.

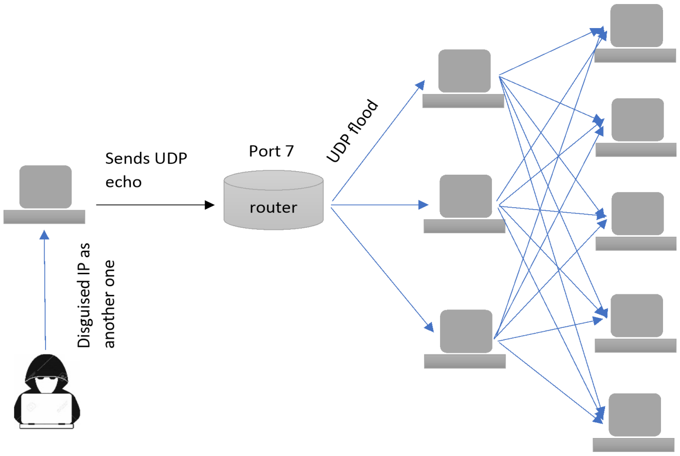

Fig. 6. Echo on user Datagram Protocol (UDP) Ports: Source Port Perpetuals Echo to All Target Ports Modified by Attacker.

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 [55]. 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 [56] between hosts using ICMP messages

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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Bernstein et al 2012 [45]	Edwards-curve Digital Signature Algorithm	✗	✓	It is not a benchmark framework	Strong defenses against software side-channel attack	Drastically reducing the number of branches	Yes	No
Hasmukh et al 2018 [46]	Sparsely-Tagged Fragmentation Marking approach	✓	✓	Authentication of the marking at victim is needed to prevent compromise routers to spoof the marking	Improves the Probabilistic packet marketing by reducing the number of packets	95% accuracy	Yes	Yes
Mahmud et al. 2018[47]	SecuPAN proposed tool	✓	✓	Mitigates the attack	verify authenticity and integrity	Completion time 35ms	Yes	No
Chaoqin et al. 2018 [48]	Integrated IP Source Address Validation Architecture (ISAVA)	✓	✓	Filtering rate is not 100 percent accurate	Maximizes the SDN control pattern	Transfer time 8s	Yes	Yes
Bakker et al 2019[49]	BGP Flowspec rules	✓	✗	It can not be used as the only way of defense	Specify rules on traffic and it's limitations	effectiveness is higher than Impact	Yes	No
Al-Ani et al 2019[50]	New mechanism against attacks	✓	✗	Can not block all kinds of packets	It can evade the OpenFlow firewall	Not mentioned	Yes	No

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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Gupta et al 2014[53]	Ant Colony Optimization	✓	✗	The performance of the model considerably varies on a larger and more congested network	real life experiment and implementation	better detection rates and reduced false alarm rates	Yes	Yes
Okeke et al 2016[54]	Prey Predator (PP) approach	✓	✗	Many issues like manifesting and buffer overflow exists	Described the application of Prey Predator approach	Not mentioned	No	No

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

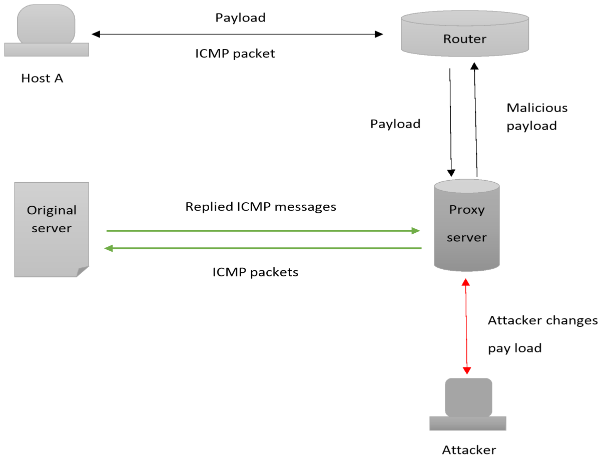

Fig. 7. ICMP Tunneling: Attackers Manipulating ICMP Payload to the Host A and Receiving Desired Packets.

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 [61]. It normally occurs in the network layer. Attacks [62][63], 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 [64] 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.

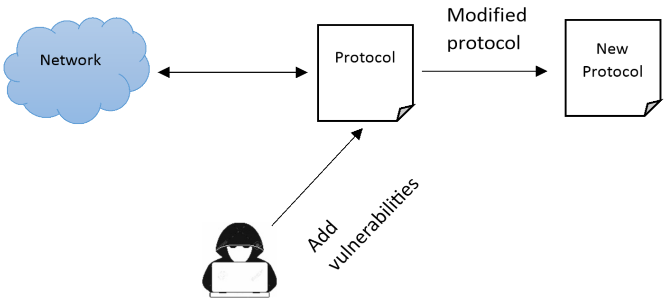

Fig. 8. Router Attack: Attacker Changed the Established Protocol with the Modified Protocol to Ensure Vulnerabilities in Network.

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 [67] 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 [68], 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. 9, attacker uses two scanners to send malicious requests disguised as service messages for scanning system

TABLE V. STATE-OF-THE-ART SOLUTIONS OF SMURF ATTACK

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Jayashree et al 2018 [59]	Pattern Matching Techniques	✓	✗	Accuracy is less than desired	Pattern matching technique for WSN	packet delivery ratio 1.3	Yes	No
Myo et al 2019 [57]	SDN based technique	✓	✗	Real time results are missing.	SDN and DDoS attack is discussed	average accuracy is 0.97	Yes	No
Trung et al 2019[60]	An enhanced History-based IP Filtering scheme	✓	✗	Lack of enhancement in the packet process	Described IP model for IP filtering	response time 60ms to 120 ms	Yes	No

TABLE VI. STATE-OF-THE-ART SOLUTIONS OF ROUTER ATTACK

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Ryoki et al 2016[65]	An Interest flow balancing method	✓	✓	The router does not record information for further use	Described countermeasures of IFA	Not mentioned	No	No
Yufeng et al 2018[21]	Distributed router shadow	✓	✗	The connection between router shadow and real router creates real difficulties	Structure and process of router shadow	minimum latency and intended load reduce	No	Yes
Dauod et al 2019[66]	HT-based threat model, known as Black Hole Router (BHR)	✓	✓	Increased the waiting time	Real life experiment of black hole method	10.83%, 27.78% and 21.31% overhead in area, power, and performance	Yes	Yes

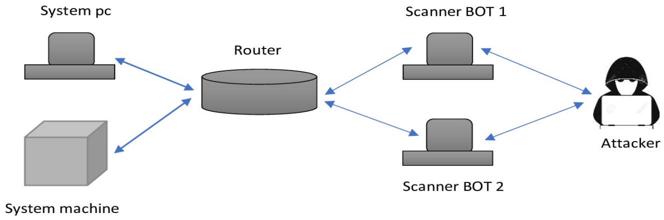

Fig. 9. Scan Attacks: Attackers use BOT Scanners to Scan Data from System's Machine.

devices. These scanners scan the system PC and machine and send results to the attacker.

These attacks are of two types, slow and fast port scan attacks.

1) Slow scan is an active scanning of devices[69] that connects to network where two successive probe 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[70].
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 [76] 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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Mathieu et al 2018 [71]	Scan Chain Encryption	✓	✗	It is only applied on non-modifiable cores	secure and cost efficient mechanism	100% fault coverage	No	Yes
Markus et al 2018 [68]	Classification algorithm	✗	✓	It is not applied on real world network data.	problem setting and the underlying flow-based data are analyzed	Not sued any accuracy measurement	Yes	Yes
Manuel et al 2019 [72]	Time-aware metrics in NIDS evaluations	✓	✗	Application of time-aware machine learning models is missing	Used time-aware evaluation metrics for the early intrusion detection problem, identifying advantages and disadvantages	0.85 recall and precision	Yes	No
Mohammad et al 2019 [73]	Fuzzy Rule Interpolation	✓	✗	Prevention method is missing	Effectively detect the very slow and slow port scans based solely on the sparse fuzzy rules.	Not mentioned	No	No
Hartpence et al 2020 [74]	Sequential Neural Networks	✓	✗	No new algorithm is focused	sequential NN architecture	99% accuracy	No	No
GUSTAVO et al 2020 [75]	Artificial Immune Systems and Fuzzy Logic	✓	✗	Real network environment should be considered	Method comparisons are discussed with efficiency	99.9% accuracy	Yes	No

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 [77][78] uses this option for enforcing IP-based restrictions to minimize unwanted traffic.

Over 30%[79] 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.

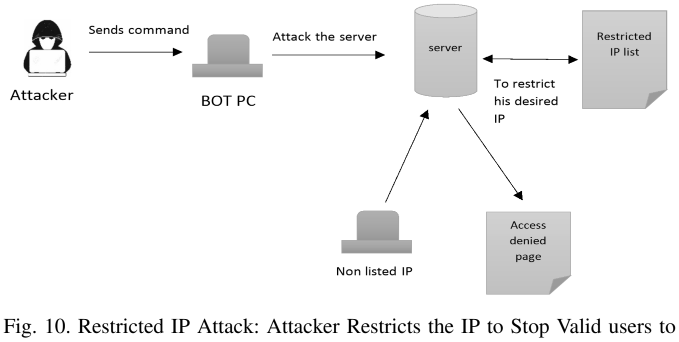

Fig. 10. Restricted IP Attack: Attacker Restricts the IP to Stop Valid users to Visit the Website.

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 two hosts.

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 [81].

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

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

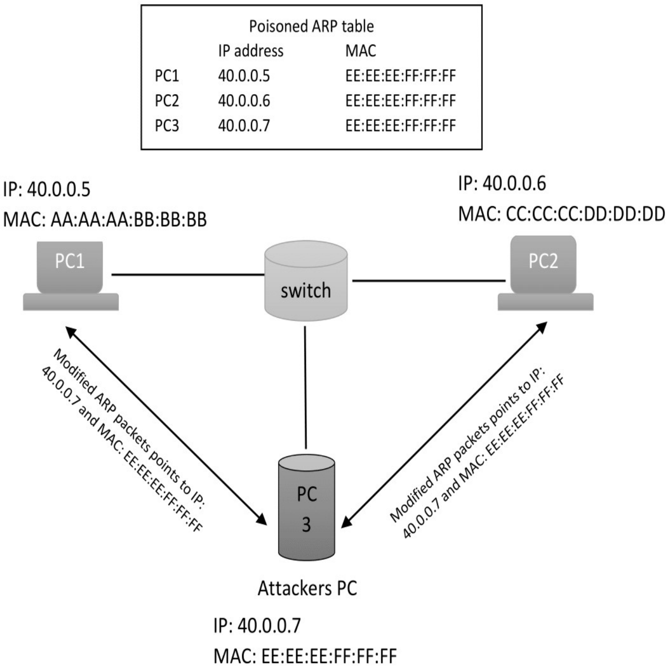

Fig. 11. Occurrence of ARP Attack: Attacker Manipulates ARP Table to Connect as Legitimate Server.

attack [82]. Match prevention is the best way to defend this attack as most ARP replies can be detected by this model.

ARP intrusion may result in the following types of attacks:

1) Session Hijacking: It is a cyber security attack on a user session over a network. In this attack, attackers exploit ARP spoofing attack to get one session ID and steal their sensitive information.

2) Man in the Middle Attack: This attack also employs ARP spoofing to disturb the traffic from a user and manipulates it to get access to user sessions. This attack re-routes the network traffic between the host and the attacker. So, the attacker will transmit the received packets to the desired destination. Hence, the communication between two original hosts is not disrupted and the sniffing process may go unnoticed.

3) Cloning Attack: In this attack, hacker himself change his IP and MAC to look exactly like the target host. Once the process is done, there will be two hosts having same address. The target host gets confused and the attacker takes the advantage as real one.

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

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Ghazi et al. 2016 [83]	ARP table, ARP filtering, authenticating	✗	✓	All ways of ARP spoofing is not discussed and detected.	Defense implementation	Not mentioned	Yes	Yes
Sweta et al. 2018 [84]	Secondary ARP table	✓	✓	Time interval between hosts is fixed. Authorized connection may take longer time can be concluded as attack.	Real time implementaion	Not mentioned	Yes	Yes
Jing et al. 2019[32]	ARP reply message process in OpenFlow platform	✓	✗	The system is not flexible enough to integrate	Discussed new features in OpenFlow network	Min. Min.5679.76 Max.8307.89 Avg. 7919.66 S.D 404.60	Yes	Yes
Sanguankotchakorn et al. 2019[85]	Hybrid controller	✓	✗	Detecting Switched DDoS attack is taking around 9 seconds which is really slow.	Discussed Controller mitigation process	Entropy falls 1 to 0 with time	Yes	Yes
Sanguankotchakorn et al. 2019[86]	A non-cryptography-based and called MR-ARP	✓	✗	It takes longer time to determine the secure path	Analyzed Mitigation technique	Not mentioned	Yes	Yes
Al-An et al. 2020[87]	Match-Prevention	✗	✓	the bandwidth consumption of Match Prevention is 18% higher	Discussed security challenges	100% success rate	Yes	Yes

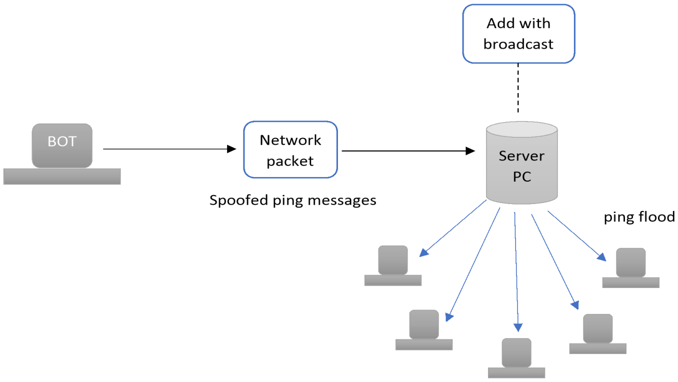

Fig. 12. Ping of Death: Spoofed Ping Messages Add with the Broadcast IP of the Server to Manipulate clients PC.

protection can demolish the PoD attacks before making any harm to the PC [90].

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.

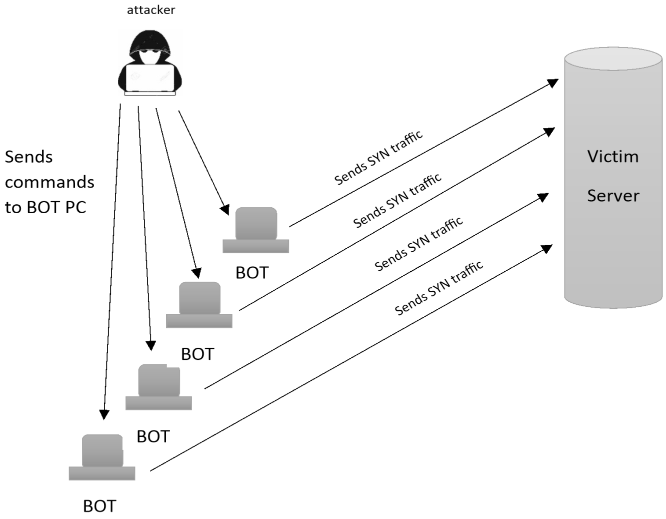

Fig. 13. SYN Flood Attack: Attacker Sends Command to BOT PC Sends SYN Traffic to Server.

TABLE X. State-of-the-Art Solutions of SYN Flood Attack

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Hussain et al 2016 [91]	Three Way Counter Algorithm for Attack Detection	✓	✗	Cloud security is not justified	HoneyPot method is emphasized	Attack detection rate of Tcp port 60%	No	No
Kshirsagar et al 2016 [92]	System architecture for efficient detection	✓	✗	Authors have used only 4 features to detect attack which is not efficient	load of CPU is minimized after The attack	Cpu load value ranges from 8-11% after detection	Yes	Yes
Kumar et al 2018 [93]	SAFETY	✓	✗	Victims from multiple destination can not be detected	SAFETY brings 13 percent regarding processing delay experienced by a legitimate node	100% TPR while has approximately 27% FPR	Yes	Yes
Bae et al 2018 [94]	DDoS Cyber-Shelter model	✓	✗	Authentication data can get access to the service even during the attacks are made. Data can be manipulated	a cost-effective way	lowest false positive rate of 0.0003% at maximum	Yes	Yes
Zhong et al 2018 [95]	Three modules, such as sniffer module, analysis module and active defense module	✓	✓	Most network administrators do not have set up such rules, it gives potential attackers the convenience of attacks	provide reference for tracking SYN flood attack	Network administrators are no longer required	Yes	Yes
Khalid et al 2019 [96]	SYN Flood Attack Detection Based on Bayes Estimator (SFADBE)	✓	✗	Bandwidth issue exists	low cost and robust	threshold is 8.0	Yes	Yes
Dang et al 2019 [97]	SSP (a coordination of the SDN Open-flow switch)	✓	✗	94 percent accuracy which is not good enough for integration in a system	SSP improves the successful connection rate and average connection retrieval time	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.	Yes	Yes
Evmorfos et al 2020 [98]	Random Neural Network with Deep Learning	✓	✗	Neural Network's recurrent structure needs to improve	substantially better attack detection and significantly lower false alarm rate	Accuracy False 80.7%	No	No

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 sleeps 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 [102] 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 [103]. This attack might lead to the system crash if combined with multiple attackers [104].

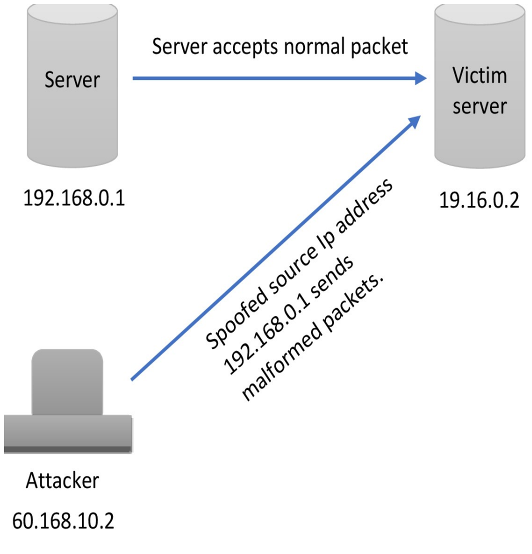
Server
Server accepts normal packet
Victim server
192.168.0.1
19.16.0.2
Spoofed source Ip address 192.168.0.1 sends malformed packets.
Attacker
60.168.10.2

Fig. 14. Malformed Attack: Attacker Spoofed the IP Address to Send Malformed Packet to the Victim Server.

In the Fig. 14 attacker changes his IP address to source IP address 192.168.0.1 and acts as an legitimate server. By establishing connection with the server it sends malformed packet. Packet malforming leads to packet manipulation. A larger ping more than 65,535 bytes [105] is enough to conduct a attack. So attackers send it by fragments. If the victim tries to reassemble it, they will face oversized packet or memory over flow. It could crush PC or servers in the mean time

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

IV. Extrusion Events

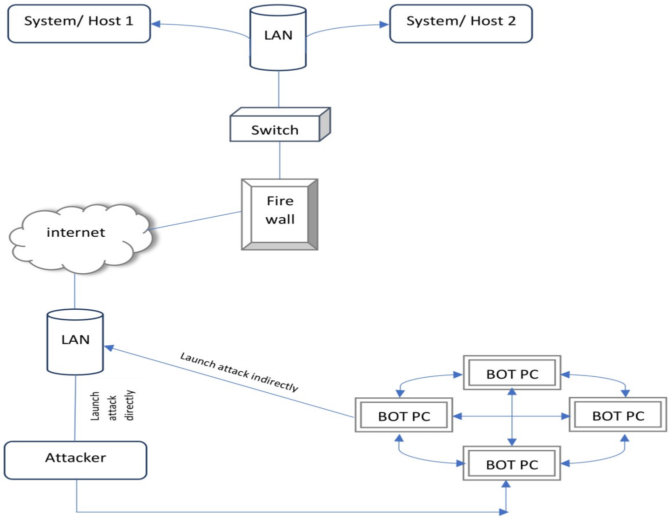

Fig. 15. A Generalized Model of Occurrence of an Extrusion Event.

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 November2018 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 [107].

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

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

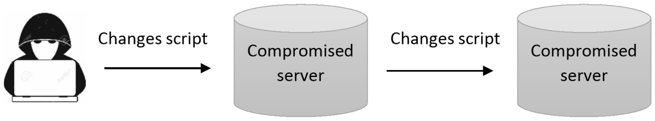

Fig. 16. A Chain System of Attack: an Attacker Changes the Script of the Server to Manipulate System

computer, but in this attack, the victim is not the ultimate target of the attack, rather stepping a stone to other networks. This attack mainly occurs on application layer. The 2013 attack against Target is the classic example of a supply chain attack. As the attack is new and very difficult to detect, no such paper has discussed about the solution to it.

B. Destruction of Services (DeOS) Attack

A destruction of services targets the entire organization's ability to recover from the attack afterwards. It is meant to damage the maximum amount possible, resulting in data loss, service disruptions and cost of data recovery. It puts business in such a position that either they have to rebuild their architecture from scratch or pay the money to the attacker.

In its 2017 Midyear Cybersecurity Report, Cisco said the rapid spread of WannaCry, for example, foreshadowed the emergence of what it is termed "destruction of service" (DeOS) attacks, which could present an existential threat and leave businesses completely unable to recover.

To defend against this attack, a system needs to check regular penetration test results, hiring more cyber security staffs and decreasing mean time to detect man in the middle destruction statistics. The quicker the threat is detected, less the damage occurs throughout the system.

In the Fig. 17 attacker commands the BOT PC's to attack the website of the organization to destroy the back up file or the database.

The two most common points of entry for attackers are through known exploitable vulnerabilities and acquired administrator credentials. This attack includes Cisco's 2017 that made Cisco worry to use creative ideas to mitigate the attack.

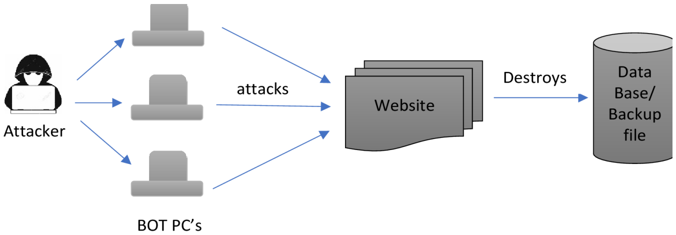

Fig. 17. DeOS Attack: Attacker Attacks the Main Structure of the Organization.

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 trafficn [108] 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

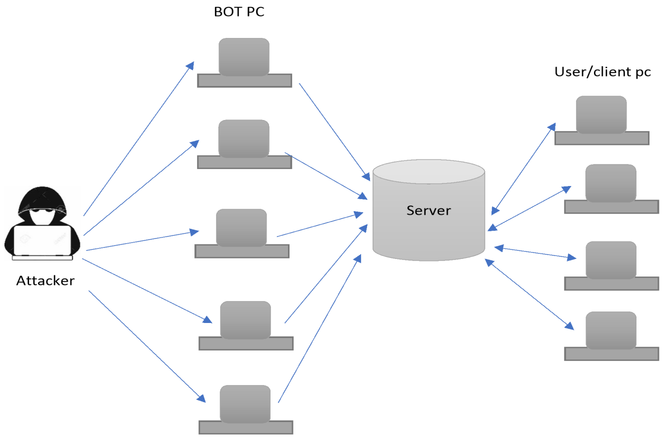

Fig. 18. DDoS Attack: Several Bot PCs Compromised the Server to Attack the Target.

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 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].

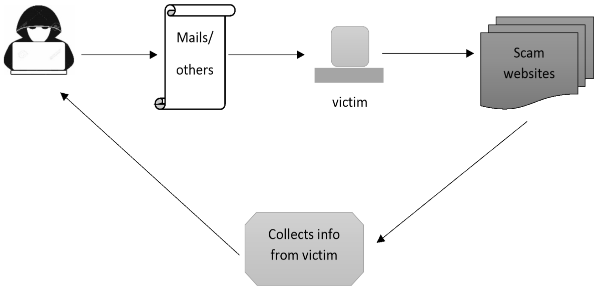

Fig. 19. Scamming a Victim's Computer using Phishing Attack: Attackers Send Mails to Victim's Computer to collect Information by Clicking on Scam Website .

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

Reference	Proposed Method/ Model	Detec-tion	Preven-tion	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Alan et al 2016 [109]	Artificial Neural Network (ANN) algorithm	✗	✓	It is not designed for encrypted packets	detect DDoS attacks based on specific characteristic features (patterns)	98% accuracy	Yes	Yes
Zhuotao et al 2018 [110]	Umbrella	✓	✗	It hampers user's privacy	capable to deal with large scale attacks involving millions of attack flows	Accuracy 90%	No	No
Mehr et al 2019 [111]	SVM based solution		✓	Feature correlation needs be more precise. Traffic generation and real-time performance is missing	use time pattern for prevention	Ryu controller is reduced by 36% 7 yes	yes	
David et al 2019 [112]	Statistical approach	✓	✗	Real time implementation is missing.	higher detection rate and accuracy and lesser processing time	99.6% accuracy	Yes	Yes
Saxena et al 2020 [113]	A third party auditor (TPA)based packet traceback approach	✓	✓	Threshold value should vary with real time update.But the value is fixed.	Easy DDoS prevention in the cloud environment	97.4% accuracy	Yes	Yes
Wang et al 2020 [114]	Multilayer perceptrons	✓	✗	If feedback mechanism works incorrectly, the system will get wrong knowledge	correct the detector when it performed poorly	Accuracy 92%	Yes	No

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.

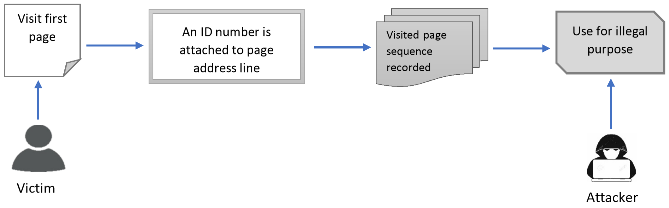
Visit first page
An ID number is attached to page address line
Visited page sequence recorded
Use for illegal purpose
Victim
Attacker

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

TABLE XIII. State-of-the-Art Solutions of Phishing

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Jain et al 2018 [118]	PHISH-SAFE: URL Features-Based Phishing Detection	✓	✗	Accuracy is relatively low.	trained using more than 33,000 legitimate URLs	90% accuracy	Yes	No
Adebowale et al 2019 [119]	An Adaptive Neuro-Fuzzy Inference System (ANFIS)based robust scheme	✓	✓	SVM still shows less accuracy than other algorithms	efficient and integrated features of images, frames and text of phishing websites	98.5% accuracy	Yes	No
Rao et al 2019 [120]	an application named as Jail-Phish	✓	✗	Similarity score may not be able to detect correctly every time	a real time application for the phishing detection	accuracy of 98.6%	Yes	Yes
Suleman et al 2019 [121]	Uniform Resource Locator (URL) based phishing detection	✓	✗	Prevention method is not discussed	Improved feature selection method	95 percent accuracy	Yes	No
Liew et al 2019 [122]	A supervised machine learning technique of Random Forest(RF)	✓	✗	Need real time implementation to show accuracy of the mechanism.	Analyzes 11 best classification features	accuracy 97.5 percent	Yes	no
Mao et al 2019 [123]	A learning-based aggregation analysis mechanism	✓	✗	F1 score is relatively low.	enable automated page-layout-based phishing detection techniques	93.7 percent accuracy	Yes	Yes
Jain et al 2019 [124]	A machine learning based approach	✓	✗	If any attacker alter 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	98.4 percent	Yes	No
Chiew et al 2019 [125]	A new hybrid ensemble feature selection framework	✓	✗	Computation-ally expensive.	automatic, flexible and robust feature selection	94.6 percent accuracy	yes	No
Orunsolu et al 2019 [126]	Support Vector Machine and Naïve Bayes algorithm	✓	X	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	99.96% accuracy	Yes	Yes

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 [128] 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 [129] means to achieve the required quality of services goals such as bandwidth, load, delay,

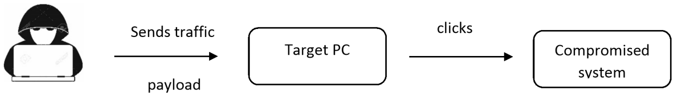

Fig. 21. Outbound Attack: Hacker Sends Payload to Target PC to Comprise the Server.

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 deceivingly 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 [136].

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].

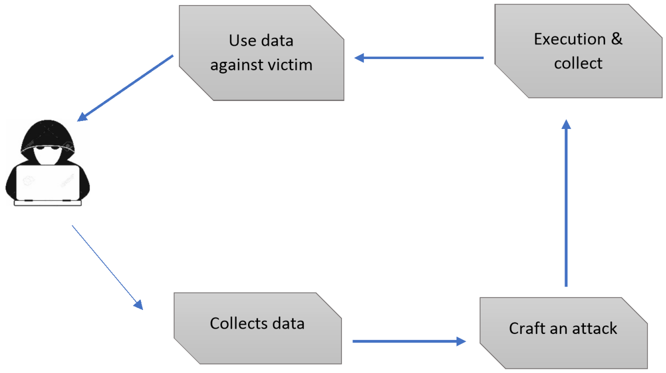

Fig. 22. Social Engineering Attack: Attack Phases.

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 it's 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

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

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.

J. 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 diverge 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.

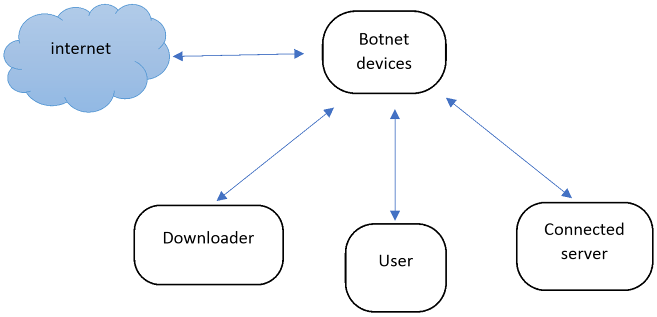

Fig. 23. Connected IoT Devices: Botnet Devices are Connected to Every Possible Device Through Internet.

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 XV. STATE-OF-THE-ART SOLUTIONS OF MALWARE ATTACK

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Andrea et al 2018 [143]	MADAM	✓	✓	Performance measurement is missing	developed a binary rewriting tool	Not mentioned	Yes	Yes
Mishra et al 2019 [144]	VMANALYZER	✓	✗	Imbalanced dataset which leads to uncertainty in the normal traces of processes.	feature vector is build for each process in monitored TVM	4.7-100 percent accuracy	Yes	yes
Maiorca et al 2019 [145]	Command-and-control botnets	✓	✗	Details of methods are missing.	categorize known vulnerabilities of learning-based PDF malware	Not mentioned	Yes	No
Gan et al 2020 [146]	A dynamical propagation model	✗	✓	Adjusting system parameter is difficult.	discussed behavior of malware under an infected cloud environment	Not mentioned	Yes	Yes
Alazab et al 2020 [147]	An automated process by using a scoring and grouping technique	✓	✗	Use of more machine learning algorithms may achieve more accurate results.	assist in the process of malware forensic investigation	94.3 percent accuracy	Yes	No
Mishra et al 2020 [148]	KVMInspector	✓	✗	It is not incorporated with network monitoring functionalities	Considered as advanced security check	81.25%–99.92%(UNM) and 95.43%0–97.81%(Elog)	Yes	yes

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 XVI. State-of-the-Art Solutions of IoT Botnet Attack

Reference	Proposed Method/ Model	Detection	Prevention	Limitations	Merit	Efficiency	Code modification	Applied to all platform
Meidan et al 2018 [14]	N-BaIoT	✓	✗	Connection between IoT devices that has low prediction rate in their network is not allowed due to security polices.	Create experimantal setup for dataset	.0007 FPR	Yes	Yes
Tzagkarakis et al 2019 [155]	Sparsity representation framework	✓	✗	The decision threshold is estimated using only begin training instances.	Lightweight method	Not mentioned	Yes	No
Banerjee et al 2019 [156]	Honeynet	✓	✗	Malicious binaries, attack replays are not considered.	provides activity logs of the intrusion attempt	100 percent accuracy	yes	No
Dange et al 2020 [157]	CNN-based deep learning model	✓	✗	There is a difference in power consumption as it negotiates the condition of various WiFi signal.	details of IoT attacks	Not mentioned	Yes	No

TABLE XVII. SUMMARY OF INTRUSION AND EXTRUSION EVENTS

Attack name	Type	How it occurs	Where it occurs	Consequences	Existing methods/ models	Complexity
TCP ACK storm attack	intrusion	It can exploits a design architecture in the TCP specifications	Application layer	Effect the websites regular work by sending lots of traffic	Modifying the TCP ,State transition model, hypervisor at close state, FMVEA and multiset semantic, MLPNN structure	Low
Fraggle attack	Intrusion	Dispatches numerous numbers of malicious traffic to overwhelm a router's transmittable address in the network	Transport layer	Cripple any servers for hours, or even days	SACL filtering method	Low
An ICMP redirect message attack	Intrusion	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.	Transport layer	Cause problems in fire-walled environments where flow traffic patterns are non-deterministic	BigFlow Open Flow, PrECast proxy service, AR-match technique, Signature based and Machine learning tool, Centralized system	Low
Internet protocol fragment attack	Intrusion	Attacker uses the fragmentation protocol within IP to attack the system.	Transport layer	System may freeze or overwhelmed because of the attack	BGP Flowspec rules, Edwards-curve Digital Signature Algorithm, Sparsely-Tagged Fragmentation Marking approach, SecuPAN proposed tool, Integrated IP Source Address Validation Architecture (ISAVA)	High
Perpetual echo attack	Intrusion	Any illegitimate activity happens at port 7 in the form of spoofing any system knows as perpetual attack.	Transport layer	Large amount of network traffic causes delay.	Prey Predator (PP), Ant Colony Optimization, Modified protocol specifications	Low
Internet Control Message Protocol (ICMP) tunneling attack	Intrusion	Attacker inserts malicious data by using ICMP tunneling and echo the packet to remote computer	Network layer	Any sensitive data or access in private sector may done by this attack.	A novel mechanism of 5 algorithms, Covert Channel Detection using Support Vector Machine, Stateless and monitoring model, Stateless model	High
Smurf attack	Intrusion	The attacker creates a malicious network packets attached to a IP and send it to the victim's system	Network layer	It can freeze company servers for days and months. Data loss can happen	SDN based technique, an enhanced History-based IP Filtering scheme, Pattern Matching Techniques, principal component analysis	High
Router attack	Intrusion	Injecting vulnerabilities to the router	Network layer	Attacks impact network services and business operations distributed router shadow, an Interest flow balancing method, Run-time protector and Restart-time protector.	Distributed router shadow, an Interest flow balancing method, Run-time protector and Restart-time protector, Pushback method, Scalable Method	Low
Slow and fast port scan attack	Intrusion	May blend into the network noise never exceeding detection thresholds and exhausting detection system state	Network layer	Creates changes in the normalcy of the traffic	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, Classification algorithm, time-aware metrics in NIDS evaluations, Fuzzy Rule Interpolation	High

Attack name	type	How it occurs	Where it occurs	Consequences	Existing methods/ models	complexity
Restricted IP attack	Intrusion	Attacker restricted the access to the particular site and defined set of IP address	Network layer	Restrict user's website	ARP table update state-based detection approach, SQL Injection detection mechanism , An adaptive framework, Packet filtration, payload distribution model, generic authorization framework	Low
ARP attack	Intrusion	When a hacker dispatches false ARP messages to the local network and connect it with the system.	Data link layer	Hackers can steal sensitive information from the targeted computers.	Discrete event system, IP probing, ARP table, ARP filtering, Centralized methodology (central server), Novel mechanism, Secondary ARP table etc.	Low
Ping of death attack	Intrusion	Attacker sends malicious ping to a system to flood the system.	Data link layer	It can crash, damage or freeze the victim's computer by sending oversized malformed packet	No specific solution	low
SYN floods attack	Intrusion	Connected with syn false packet and TCP connection established	Data link layer	Attacker makes the system unavailable for the user by flooding with legitimate traffic.	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 (SFADBE), SSP—a coordination of the SDN Open-flow switch	Low
Malformed attack	Intrusion	Incorrectly formed IP packets are formed and sent to the victim to crash the system	Data link layer	The system of the victim may get confuse and gets crashed	TCP trace module, Threshold value set for detect malformed packet, Generates ACL	Low
Supply chain attack	Extrusion	A value-chain or third-party attack occurred by an outsider	Application layer	Causes major data breach	No solution yet	High
DeOS (destruction of services) attack	Extrusion	Targets an organization's entire online presence as well as their ability to recover from the attack afterwards	Application layer	Could put businesses in a position where they have to rebuild infrastructure from scratch or pay a high ransom to the attackers	No solution yet	High
Distributed denial of services (DDOS) Attack	Extrusion	Malicious attempt to make an online service unavailable to users	Application layer	Make any website or system and servers unavailable to legitimate users	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	Low

Attack name	type	How it occurs	Where it occurs	Consequences	Existing methods/ models	complexity
Phishing attack	Extrusion	Targets are contacted via email,text or link disguised as legitimate institution	Application layer	Steals Sensitive information	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.	High
URL poisoning attack	Extrusion	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	Transport layer	Tracks user to get desired information	No specific solution yet	High
Outbound attack	Extrusion	Attacker tunnels back in over that connection to take control of the employees' computer	Network layer	Unlimited email or file transfers might let the attacker enter into the network and get sensitive information outside	No specific solution yet	Low
Violating Traffic regulation conditions attack	Extrusion	Violating traffic regulations	Network layer	Causes any discontinuity to the network normal behavior	No solutions yet	Low
Social engineering attack	Extrusion	Gather information about someone by exploiting human weakness that inherits every organization	Network layer	Can control one life through virtual manipulating	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	High
Malware	Extrusion	Any program or file that is harmful injected through any way in the system	Data link layer	It thefts, encrypts, or deletes the data. It can spy on computer activity without user knowledge or permission	A dynamical propagation model, an automated method by using a scoring and grouping technique, KVMInspector, VMANALYZER, command-and-control botnets etc	High
IoT botnet	Extrusion	It is accessed from a remote computer without the owners' knowledge and set forward transmissions to other computers on the Internet	Physical layer	It causes breaches to all related IoT devices	N-BaIoT, IoT-BAI model, CNN-based deep learning, MOPSO, sparsity representation framework, Honeynet	High

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.Loss or 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

[1] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 336–341.

[2] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 32–37.

[3] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 2014, pp. 230–234.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth international conference on computational intelligence and security*. IEEE, 2013, pp. 663–667.

[6] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1093–1110.

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[8] M. F. Muhammad, W. Anjum, and K. S. Mazhar, "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications (0975 8887)*, vol. 111, no. 7, 2015.

[9] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[10] O. Said and M. Masud, "Towards internet of things: Survey and future vision," *International Journal of Computer Networks*, vol. 5, no. 1, pp. 1–17, 2013.

[11] S. Kraijak and P. Tuwanut, "A survey on iot architectures, protocols, applications, security, privacy, real-world implementation and future trends," 2015.

[12] D. Peraković, M. Periša, and I. Cvitić, "Analysis of the iot impact on volume of ddos attacks," *XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju–PosTel*, vol. 2015, pp. 295–304, 2015.

[13] K. Sonar and H. Upadhyay, "A survey: Ddos attack on internet of things," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.

[14] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[15] T. F. Lunt, "A survey of intrusion detection techniques," *Computers and Security*, vol. 12, no. 4, pp. 405–418, 1993.

[16] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[17] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, p. 55, 2014.

[18] A. Tuteja and R. Shanker, "Optimization of snort for extrusion and intrusion detection and prevention," *International Journal of Engineering Research and Applications*, vol. 2, no. 3, pp. 1768–1774, 2012.

[19] M. J. Lekha, G. Padmavathi, and D. C. Wyld, "A comprehensive study on classification of passive intrusion and extrusion detection system," in *ICCSEA, SPPR, CSIA, WimoA-2013*. Citeseer, 2013, pp. 281–292.

[20] A. Gurina and V. Eliseev, "Anomaly-based method for detecting multiple classes of network attacks," *Information*, vol. 10, no. 3, p. 84, 2019.

[21] Y. Li, L. Tian, H. Qiu, and C. Zhang, "Distributed shadow for router security defense," *International Journal of Software Engineering and Knowledge Engineering*, vol. 28, no. 02, pp. 193–206, 2018.

[22] N. Hubballi and J. Santini, "Detecting tcp ack storm attack: a state transition modelling approach," *IET Networks*, vol. 7, no. 6, pp. 429–434, 2018.

[23] T. Duval, B. Jouga, and L. Roger, "The mitnick case: How bayes could have helped," in *IFIP International Conference on Digital Forensics*. Springer, 2005, pp. 91–104.

[24] O. Sbai and M. Elboukhari, "Classification of mobile ad hoc networks attacks," in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*. IEEE, 2018, pp. 618–624.

[25] R. Abramov and A. Herzberg, "Tcp ack storm dos attacks," in *IFIP International Information Security Conference*. Springer, 2011, pp. 29–40.

[26] S. N. Duc, M. Mimura, and H. Tanaka, "An analysis of tcp ack storm dos attack on virtual network," in *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2019, pp. 288–293.

[27] I. Topalova, P. Radoyska, and S. Sokolov, "Neural network implementation for detection of denial of service attacks," *Journal of Engineering Science and Technology Review*, 2019.

[28] S. Acharya and N. Tiwari, "Survey of ddos attacks based on tcp/ip protocol vulnerabilities," *IOSR Journal of Computer Engineering*, vol. 18, no. 3, pp. 68–76, 2016.

[29] Y. Chen, "A novel marking-based detection and filtering scheme against distributed denial of service attack," Ph.D. dissertation, University of Ottawa (Canada), 2006.

[30] U. Tariq, M. Hong, and K.-s. Lhee, "A comprehensive categorization of ddos attack and ddos defense techniques," in *International Conference on Advanced Data Mining and Applications*. Springer, 2006, pp. 1025–1036.

[31] M. Baentsch, L. Baum, G. Molter, S. Rothkugel, and P. Sturm, "Enhancing the web's infrastructure: From caching to replication," *IEEE Internet Computing*, vol. 1, no. 2, pp. 18–27, 1997.

[32] J. Xia, Z. Cai, G. Hu, and M. Xu, "An active defense solution for arp spoofing in openflow network," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 172–178, 2019.

[33] D. Hanna, P. Veeraraghavan, and E. Pardede, "Precast: An efficient crypto-free solution for broadcast-based attacks in ipv4 networks," *Electronics*, vol. 7, no. 5, p. 65, 2018.

[34] M. Baltatu, A. Lioy, F. Maino, and D. Mazzocchi, "Security issues in control, management and routing protocols," *Computer Networks*, vol. 34, no. 6, pp. 881–894, 2000.

[35] P. Arote and K. V. Arya, "Detection and prevention against arp poisoning attack using modified icmp and voting," in *2015 International Conference on Computational Intelligence and Networks*. IEEE, 2015, pp. 136–141.

[36] J. Kaur, "Wired lan and wireless lan attack detection using signature based and machine learning tools," in *Networking Communication and Data Knowledge Engineering*. Springer, 2018, pp. 15–24.

[37] A. K. Al-Ani, M. Anbar, S. Manickam, A. Al-Ani, and Y.-B. Leau, "Preventing denial of service attacks on address resolution in ipv6 link-local network: Ar-match security technique," in *Computational Science and Technology*. Springer, 2019, pp. 305–314.

[38] E. Viegas, A. Santin, A. Bessani, and N. Neves, "Bigflow: Real-time and reliable anomaly-based intrusion detection for high-speed networks," *Future Generation Computer Systems*, vol. 93, pp. 473–485, 2019.

[39] J. Andre and J. Naab, "Open vswitch configuration for separation of kvm/libvirt vms," *Network*, vol. 43, 2019.

[40] C. Shannon, D. Moore *et al.*, "Characteristics of fragmented ip traffic on internet links," in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*. ACM, 2001, pp. 83–97.

[41] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[42] Z. Trabelsi, S. Zeidan, and K. Hayawi, "Denial of firewalling attacks (dof): The case study of the emerging blacknurse attack," *IEEE Access*, vol. 7, pp. 61 596–61 609, 2019.

[43] A. Al-Ani, M. Anbar, R. Abdullah, and A. K. Al-Ani, "Proposing a new approach for securing dhcpv6 server against rogue dhcpv6 attack in ipv6 network," in *International Conference of Reliable Information and Communication Technology*. Springer, 2018, pp. 579–587.

[44] R. A. Rahman and B. Shah, "Security analysis of iot protocols: A focus in coap," in *2016 3rd MEC international conference on big data and smart city (ICBDSC)*. IEEE, 2016, pp. 1–7.

[45] 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.

[46] H. Patel and D. Jinwala, "Stf-dm: a sparsely tagged fragmentation with dynamic marking an ip traceback approach." *Int. Arab J. Inf. Technol.*, vol. 15, no. 4, pp. 721–728, 2018.

[47] M. Hossain, Y. Karim, and R. Hasan, "Secupan: A security scheme to mitigate fragmentation-based network attacks in 6lowpan," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*. ACM, 2018, pp. 307–318.

[48] C. Zhang, G. Hu, G. Chen, A. K. Sangaiah, P. Zhang, X. Yan, and W. Jiang, "Towards a sdn-based integrated architecture for mitigating ip spoofing attack," *IEEE Access*, vol. 6, pp. 22 764–22 777, 2017.

[49] D. Bakker, "Impact-based optimisation of bgp flowspec rules for ddos attack mitigation," B.S. thesis, University of Twente, 2019.

[50] A. Al-Ani, M. Anbar, S. A. Laghari, and A. K. Al-Ani, "Mechanism to prevent the abuse of ipv6 fragmentation in openflow networks," *PloS one*, vol. 15, no. 5, p. e0232574, 2020.

[51] 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 Electronic Systems, Signal Processing and Computing Technologies*. IEEE, 2014, pp. 419–424.

[52] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," 2018.

[53] 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 Electronic Systems, Signal Processing and Computing Technologies*. IEEE, 2014, pp. 419–424.

[54] 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 Computer Engineering, Paris*, vol. 10, no. 2016, 2016.

[55] D. Kundur and K. Ahsan, "Practical internet steganography: data hiding in ip," *Proc. Texas wksp. security of information systems*, 2003.

[56] L. Jacquin, V. Roca, and J.-L. Roch, "Icmp: an attack vector against ipsec gateways," 2013.

[57] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced support vector machine-(asvm-) based detection for distributed denial of service (ddos) attack on software defined networking (sdn)," *Journal of Computer Networks and Communications*, vol. 2019, 2019.

[58] S. Kumar, "Smurf-based distributed denial of service (ddos) attack amplification in internet," in *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*. IEEE, 2007, pp. 25–25.

[59] J. Agarkhed, G. Kalnoor, and S. R. Patil, "Intrusion detection system using pattern matching techniques for wireless sensor networks," in *Innovations in Computer Science and Engineering*. Springer, 2019, pp. 411–418.

[60] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," *IEEE Access*, vol. 7, pp. 18 701–18 714, 2019.

[61] A. K. Biswas, S. Nandy, and R. Narayan, "Router attack toward noc-enabled mpsoc and monitoring countermeasures against such threat," *Circuits, Systems, and Signal Processing*, vol. 34, no. 10, pp. 3241–3290, 2015.

[62] A. R. B. Patil and N. V. Thakur, "Mitigation against denial-of-service flooding and malformed packet attacks," in *Third International Congress on Information and Communication Technology*. Springer, 2019, pp. 335–342.

[63] M. Bykova, S. Ostermann, and B. Tjaden, "Detecting network intrusions via a statistical analysis of network packet characteristics," in *Proceedings of the 33rd Southeastern Symposium on System Theory (Cat. No. 01EX460)*. IEEE, 2001, pp. 309–314.

[64] N. Security, "Protecting our routers," https://www.nanolocksecurity.com/protecting-our-routers-why-a-password-change-or-software-update-is-just-not-enough/, 2020.

[65] R. Shinohara, T. Kamimoto, K. Sato, and H. Shigeno, "Cache control method mitigating packet concentration of router caused by interest flooding attack," in *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016, pp. 324–331.

[66] L. Daoud and N. Rafla, "Detection and prevention protocol for black hole attack in network-on-chip," in *Proceedings of the 13th IEEE/ACM International Symposium on Networks-on-Chip*, 2019, pp. 1–2.

[67] S. Specht and R. Lee, "Taxonomies of distributed denial of service networks, attacks, tools and countermeasures," *Technical Report CE-L2003-03*, 2003.

[68] M. Ring, D. Landes, and A. Hotho, "Detection of slow port scans in flow-based network traffic," *PloS one*, vol. 13, no. 9, p. e0204507, 2018.

[69] G. Conti and K. Abdullah, "Passive visual fingerprinting of network attack tools," in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*. ACM, 2004, pp. 45–54.

[70] M. Dabbagh, A. J. Ghandour, K. Fawaz, W. El Hajj, and H. Hajj, "Slow port scanning detection," in *2011 7th International Conference on Information Assurance and Security (IAS)*. IEEE, 2011, pp. 228–233.

[71] 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 Systems*, vol. 38, no. 3, pp. 538–550, 2018.

[72] M. López-Vizcaíno, F. J. Novoa, D. Fernández, V. Carneiro, and F. Cacheda, "Early intrusion detection for os scan attacks," in *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2019, pp. 1–5.

[73] M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, "Detecting slow port scan using fuzzy rule interpolation," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*. IEEE, 2019, pp. 1–6.

[74] 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, pp. 256–260.

[75] G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proença, "Artificial

immune systems and fuzzy logic to detect flooding attacks in software-defined networks," *IEEE Access*, 2020.

[76] R. Ritchey, B. O'Berry, and S. Noel, "Representing tcp/ip connectivity for topological analysis of network security," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.* IEEE, 2002, pp. 25–31.

[77] M. Kaushik and G. Ojha, "Attack penetration system for sql injection," *International journal of advanced computer research*, vol. 4, no. 2, p. 724, 2014.

[78] A. Sumalee and F. Kurauchi, "Network capacity reliability analysis considering traffic regulation after a major disaster," *Networks and Spatial Economics*, vol. 6, no. 3-4, pp. 205–219, 2006.

[79] M. Dubinsky, "The good and bad of 3 common ip white listing scenarios," https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/good-and-bad-3-common-ip-whitelisting-scenarios, 2020.

[80] Y. Kim, S. Ahn, N. C. Thang, D. Choi, and M. Park, "Arp poisoning attack detection based on arp update state in software-defined networks," in *2019 International Conference on Information Networking (ICOIN)*. IEEE, 2019, pp. 366–371.

[81] Z. Trabelsi and K. Shuaib, "Spoofed arp packets detection in switched lan networks," in *International Conference on E-Business and Telecommunication Networks*. Springer, 2006, pp. 81–91.

[82] D. Adamitis, "Sea turtle keeps on swimming, finds new victims, dns hijacking techniques," https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html, 2019.

[83] G. Al Sukkar, R. Saifan, S. Khwaldeh, M. Maqableh, and I. Jafar, "Address resolution protocol (arp): spoofing attack and proposed defense," 2016.

[84] S. Singh, D. Singh, and A. M. Tripathi, "Two-phase validation scheme for detection and prevention of arp cache poisoning," in *Progress in Advanced Computing and Intelligent Engineering*. Springer, 2019, pp. 303–315.

[85] T. Sanguankotchakorn and S. K. Arugonda, "Hybrid controller for securing sdn from switched ddos and arp poisoning attacks," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2019, pp. 1–6.

[86] A. M. Amin and M. S. Mahamud, "An alternative approach of mitigating arp based man-in-the-middle attack using client site bash script," in *2019 6th International Conference on Electrical and Electronics Engineering (ICEEE)*. IEEE, 2019, pp. 112–115.

[87] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in ipv6 link-local network," *IEEE Access*, vol. 8, pp. 27 122–27 138, 2020.

[88] B. Harris and R. Hunt, "Tcp/ip security threats and attack methods," *Computer communications*, vol. 22, no. 10, pp. 885–897, 1999.

[89] R. Chirgwin, "Firewalls snuffed by 'blacknurse' ping of death attack," https://www.theregister.com/2016/11/14/its_2016_and_a_ping_of_death_can_still_be_a_thing/, 2016.

[90] S. J. Templeton and K. Levitt, "A requires/provides model for computer attacks," in *Proceedings of the 2000 workshop on New security paradigms*. ACM, 2001, pp. 31–38.

[91] K. Hussain, S. J. Hussain, V. Dillshad, M. Nafees, and M. A. Azeem, "An adaptive syn flooding attack mitigation in ddos environment," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 16, no. 7, p. 27, 2016.

[92] D. Kshirsagar, S. Sawant, A. Rathod, and S. Wathore, "Cpu load analysis and minimization for tcp syn flood detection," *Procedia Computer Science*, vol. 85, pp. 626–633, 2016.

[93] P. Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, "Safety: Early detection and mitigation of tcp syn flood utilizing entropy in sdn," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, 2018.

[94] Y. Bae, I. Kim, and S. O. Hwang, "An efficient detection of tcp syn flood attacks with spoofed ip addresses," *Journal of Intelligent and Fuzzy Systems*, vol. 35, no. 6, pp. 5983–5991, 2018.

[95] X. Zhong and Y. Liu, "Detection and defense of syn flood attack based on winpcap," in *International Conference on Mechatronics and Intelligent Robotics*. Springer, 2018, pp. 249–257.

[96] K. Hussain, S. J. Hussain, N. Jhanjhi, and M. Humayun, "Syn flood attack detection based on bayes estimator (sfadbe) for manet," in *2019 International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2019, pp. 1–4.

[97] V. T. Dang, T. T. Huong, N. H. Thanh, P. N. Nam, N. N. Thanh, and A. Marshall, "Sdn-based syn proxy—a solution to enhance performance of attack mitigation under tcp syn flood," *The Computer Journal*, vol. 62, no. 4, pp. 518–534, 2019.

[98] S. Evmorfos, G. Vlachodimitropoulos, N. Bakalos, and E. Gelenbe, "Neural network architectures for the detection of syn flood attacks in iot systems," in *Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments*, 2020, pp. 1–4.

[99] R. R. Kompella, S. Singh, and G. Varghese, "On scalable attack detection in the network," in *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. ACM, 2004, pp. 187–200.

[100] J. Haggerty, T. Berry, Q. Shi, and M. Merabti, "Diddem: a system for early detection of tcp syn flood attacks," in *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.*, vol. 4. IEEE, 2004, pp. 2037–2042.

[101] M. Bogdanoski, T. Suminoski, and A. Risteski, "Analysis of the syn flood dos attack," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 5, no. 8, pp. 1–11, 2013.

[102] P. Nicholson, "Five most famous ddos attacks and then some," https://www.a10networks.com/blog/5-most-famous-ddos-attacks/, 2020.

[103] M. Masdari and M. Jalali, "A survey and taxonomy of dos attacks in cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, 2016.

[104] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet computing*, vol. 10, no. 1, pp. 82–89, 2006.

[105] Z. Yu, L. Yang, and T. Fu, "Network attack defense policy sending method and apparatus, and network attack defending method and apparatus," Nov. 22 2018, uS Patent App. 16/050,313.

[106] S. B. Venugopal and S. B. Venugopal, "Automatic generation of access control list on mellanox switch for ddos attack mitigation using ddos fingerprints," Master's thesis, University of Twente, 2019.

[107] D. L. Ponemon, "Opus and ponemon institute announce results of 2018," https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-of-2018-Third-Party-Data-Risk-Study-59-of-Companies-Experienced-a-Third-Party-Data-Breach-Yet-Only-16-Say-They-Effectively-Mitigate-Third-Party-Risks, 2018.

[108] S. Kumar, "Impact of distributed denial of service (ddos) attack due to arp storm," in *International Conference on Networking*. Springer, 2005, pp. 997–1002.

[109] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown ddos attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.

[110] Z. Liu, Y. Cao, M. Zhu, and W. Ge, "Umbrella: Enabling isps to offer readily deployable and privacy-preserving ddos prevention services," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1098–1108, 2018.

[111] S. Y. Mehr and B. Ramamurthy, "An svm based ddos attack detection method for ryu sdn controller," in *Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies*, 2019, pp. 72–73.

[112] J. David and C. Thomas, "Efficient ddos flood attack detection using dynamic thresholding on flow-based network traffic," *Computers and Security*, vol. 82, pp. 284–295, 2019.

[113] R. Saxena and S. Dey, "Ddos attack prevention using collaborative approach for cloud computing," *Cluster Computing*, pp. 1–16, 2019.

[114] M. Wang, Y. Lu, and J. Qin, "A dynamic mlp-based ddos attack detection method using feature selection and feedback," *Computers and Security*, vol. 88, p. 101645, 2020.

[115] D. Shree, "A review on cryptography, attacks and cyber security," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[116] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, "Phishing

attacks and defenses," *International Journal of Security and Its Applications*, vol. 10, no. 1, pp. 247–256, 2016.

[117] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019.

[118] A. K. Jain and B. Gupta, "Phish-safe: Url features-based phishing detection system using machine learning," in *Cyber Security*. Springer, 2018, pp. 467–474.

[119] M. A. Adebowale, K. T. Lwin, E. Sanchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of images, frames and text," *Expert Systems with Applications*, vol. 115, pp. 300–313, 2019.

[120] R. S. Rao and A. R. Pais, "Jail-phish: An improved search engine based phishing detection system," *Computers and Security*, vol. 83, pp. 246–267, 2019.

[121] M. T. Suleman and S. M. Awan, "Optimization of url-based phishing websites detection through genetic algorithms," *Automatic Control and Computer Sciences*, vol. 53, no. 4, pp. 333–341, 2019.

[122] S. W. Liew, N. F. M. Sani, M. T. Abdullah, R. Yaakob, and M. Y. Sharum, "An effective security alert mechanism for real-time phishing tweet detection on twitter," *Computers and Security*, vol. 83, pp. 201–207, 2019.

[123] J. Mao, J. Bian, W. Tian, S. Zhu, T. Wei, A. Li, and Z. Liang, "Phishing page detection via learning classifiers from page layout feature," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 43, 2019.

[124] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 2015–2028, 2019.

[125] K. L. Chiew, C. L. Tan, K. Wong, K. S. Yong, and W. K. Tiong, "A new hybrid ensemble feature selection framework for machine learning-based phishing detection system," *Information Sciences*, vol. 484, pp. 153–166, 2019.

[126] A. Orunsolu, A. Sodiya, and A. Akinwale, "A predictive model for phishing detection," *Journal of King Saud University-Computer and Information Sciences*, 2019.

[127] H. Y. Lam, R. E. Ashley, P. T. Mathison, Q. Li, and T. Ettema, "Outbound/inbound lateral traffic punting based on process risk," Mar. 21 2019, uS Patent App. 15/705,516.

[128] E. Mulyana and U. Killat, "Optimizing ip networks for uncertain demands using outbound traffic constraints," in *Proceedings of INOC*, vol. 2005. Citeseer, 2005.

[129] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *2012 IEEE symposium on security and privacy*. IEEE, 2012, pp. 95–109.

[130] C.-S. Chang, "On deterministic traffic regulation and service guarantees: a systematic approach by filtering," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1097–1110, 1998.

[131] Y. Sawa, R. Bhakta, I. G. Harris, and C. Hadnagy, "Detection of social engineering attacks through natural language processing of conversations," in *2016 IEEE Tenth International Conference on Semantic Computing (ICSC)*. IEEE, 2016, pp. 262–265.

[132] K. Y. Abeywardana, E. Pfluegel, and M. J. Tunnicliffe, "A layered defense mechanism for a social engineering aware perimeter," in *2016 SAI Computing Conference (SAI)*. IEEE, 2016, pp. 1054–1062.

[133] A. Dan and S. Gupta, "Social engineering attack detection and data protection model (seaddpm)," in *Proceedings of International Ethical Hacking Conference 2018*. Springer, 2019, pp. 15–24.

[134] M. Lansley, N. Polatidis, S. Kapetanakis, K. Amin, G. Samakovitis, and M. Petridis, "Seen the villains: Detecting social engineering attacks using case-based reasoning and deep learning," in *Workshops Proceedings for the Twenty-seventh International Conference on Case-Based Reasoning: Case-based reasoning and deep learning workshop*, 2019.

[135] F. Mouton, A. Nottingham, L. Leenen, and H. Venter, "Finite state machine for the social engineering attack detection model: Seadm," *SAIEE Africa Research Journal*, vol. 109, no. 2, pp. 133–148, 2018.

[136] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *2014 Information Security for South Africa*. IEEE, 2014, pp. 1–9.

[137] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and applications*, vol. 22, pp. 113–122, 2015.

[138] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys (CSUR)*, vol. 48, no. 3, p. 37, 2016.

[139] S. K. Sahay, A. Sharma, and H. Rathore, "Evolution of malware and its detection techniques," in *Information and Communication Technology for Sustainable Development*. Springer, 2020, pp. 139–150.

[140] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for android," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 15–26.

[141] A. Saracino, D. Sgandurra, G. Dini, and F. Martinelli, "Madam: Effective and efficient behavior-based android malware detection and prevention," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 83–97, 2016.

[142] A. Dinaburg, P. Royal, M. Sharif, and W. Lee, "Ether: malware analysis via hardware virtualization extensions," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 51–62.

[143] A. Moser, C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," in *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*. IEEE, 2007, pp. 421–430.

[144] P. Mishra, K. Khurana, S. Gupta, and M. K. Sharma, "Vmanalyzer: Malware semantic analysis using integrated cnn and bi-directional lstm for detecting vm-level attacks in cloud," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*. IEEE, 2019, pp. 1–6.

[145] D. Maiorca, B. Biggio, and G. Giacinto, "Towards adversarial malware detection: Lessons learned from pdf-based attacks," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–36, 2019.

[146] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical propagation model of malware for cloud computing security," *IEEE Access*, 2020.

[147] M. Alazab, M. Alazab, A. Shalaginov, A. Mesleh, and A. Awajan, "Intelligent mobile malware detection using permission requests and api calls," *Future Generation Computer Systems*, 2020.

[148] P. Mishra, I. Verma, and S. Gupta, "Kvminspector: Kvm based introspection approach to detect malware in cloud environment," *Journal of Information Security and Applications*, vol. 51, p. 102460, 2020.

[149] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," 2008.

[150] A. Karasaridis, B. Rexroad, D. A. Hoeflin *et al.*, "Wide-scale botnet detection and characterization." *HotBots*, vol. 7, pp. 7–7, 2007.

[151] S. Amina, R. Vera, T. Dargahi, and A. Dehghantanha, "A bibliometric analysis of botnet detection techniques," in *Handbook of Big Data and IoT Security*. Springer, 2019, pp. 345–365.

[152] A. Praseed and P. S. Thilagam, "Ddos attacks at the application layer: Challenges and research perspectives for safeguarding web applications," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 661–685, 2018.

[153] J. M. Ceron, K. Steding-Jessen, C. Hoepers, L. Z. Granville, and C. B. Margi, "Improving iot botnet investigation using an adaptive network layer," *Sensors*, vol. 19, no. 3, p. 727, 2019.

[154] R. Swami, M. Dave, and V. Ranga, "Software-defined networking-based ddos defense mechanisms," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, p. 28, 2019.

[155] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the iot edge based on sparse representation," in *2019 Global IoT Summit (GIoTS)*. IEEE, 2019, pp. 1–6.

[156] M. Banerjee and S. Samantaray, "Network traffic analysis based iot botnet detection using honeynet data applying classification techniques," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 8, 2019.

[157] S. Dange and M. Chatterjee, "Iot botnet: The largest threat to the iot network," in *Data Communication and Networks*. Springer, 2020, pp. 137–157.