International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 6; November 2017; Page No. 1253-1258

Review of different security threats in communication networks

[1] Karuna S Bhosale, [2] Maria Nenova, [3] Georgi Iliev
[1] Research Student, Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria
[2] Assoc. Prof., Research Guide, Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria
[3] Prof., Research Guide, Faculty of Telecommunication, Technical University of Sofia, Sofia, Bulgaria

Abstract
With the advances in Internet reliable operation of network based systems plays a major role. The ability to detect intruders in computer systems is important as computers are increasingly united to the systems that we depend on. Internet security is a critical factor in the performance of an enterprise which affects everything from business to cost management. Internet attacks can cause interruption in business operations and hence security is very valuable. In current research, it is shown that attacks on are hysterically increasing hence study on security threats in communication treats is necessary. In this paper, we are studying the different attacks in Internet and its behavior. There are different attacks present in today's era in Internet which include Denial of service attack, allotted Denial of service attacks, faraway to local attack, User to Root Attack etc. The behavior and effects of different attacks are different on Internet. These attacks are always harmful for network as well as application resources, which can also results in loss of incomes, loss of customers, harm to logo and robbery of essential records.

Keywords: denial of service attack, distributed denial of service attacks, remote to local attack, user to root attack

1. Introduction
Now a days, Internet usage and resources have shown tremendous growth. Along with Governments use the net to deliver data to citizens and they may more and more use the internet for their offerings. Business Company uses to trade statistics with their partners, divisions, providers, and customers for effective and easy records exchange. Research and academic institutes rely more on the internet as a platform for cooperation and as a medium for circulating their research find rapidly. Even the online social networking sites have become the main communication medium of the 21st century. Thus Internet is now transformed into a global information path for running government organizations, online businesses, banking enterprises, transportation, health, and education, emergency services etc [1].

With the increasing use of Internet, computer attacks are also increasing and which causes financial loss to an organization or an individual. The targeting internet banking transactions using malicious applications has been increased recently. This causes problems for not only to the customers who use such facilities, but also to the banking institutions which offer them. The undisrupted accessibility of the net may be very vital for the socio-monetary achievement of society. However, the inherent vulnerabilities of the internet emerge as opportunities for a number of attacks [2].

The net was designed through retaining functionality in mind now not protection and was indeed a success up to a few limitations. It offers speedy, clean and cheap communiqué mechanism, enforced with diverse better-level protocols that make certain dependable and well-timed shipping of messages with sure level of first-class of provider, Technically internet design follows the end-to-end paradigm. Such design opens up various protection hassles that offer possibilities for diverse kinds of attacks on the internet because intermediate network can be exploited by the attackers to send malicious traffic without being policed. On the Internet, Anyone person can send any packet that comes to the furnished provider. This loss of authentication means that attackers can generate a faux identification, and transfer malicious traffic with impurity through abundant and witless resources available in the intermediate network. Moreover the operating systems and protocols installed at end systems are advanced without applying safety engineering which outcomes in providing attackers quite more insecure machines on Interne. Thus vast number of vulnerable hosts can be exploited by attackers to attack victims which have deficient resources [4].

Usurpation is known as a series of associated movements accomplished by using a malicious adversary those outcomes within understanding of a target system. It's far considered that the actions of the intruder violate a given safety policy. The life of a security policy that states which movements are assumed malicious and should be prevented is a key needful for an intrusion identification machine. Violations can be detected whilst movements may be compared against given regulations. Intrusion detection (id) is the manner of calculating out and responding to malicious participates aimed at computing and network resources. This definition establishes the perception of intrusion detection as a procedure, which entails technology, humans, and tools. Intrusion identification is a method this is complementary with appreciates to mainstream techniques to security, including get admission to manage and cryptography. Intrusion detection structures (IDSs) are software program applications devoted to hit upon intrusions in opposition to a

target network [5].

If the laptop is left unattended, any one intruder can try to get right of entry to and try to misuse the device. The hassle is a lot more if the laptop is jointed to a network, specifically the internet. Any person from around the arena can reach the computer remotely. Intruder may also try and get admission to vital personal or exclusive records or release a shape of attack to deliver the system to a halt or give up to function efficiently. An intrusion to a system device does no longer need to be done manually through a person. It may be completed remotely and mechanically with engineered software. In this paper, our motive is to study the different types of security threats communication networks. We have presented the study on attacks characteristics, their behaviors and their impact. Additionally, we present the recent works on conducted on different security threats. In section II, we are presenting the study on different types of attacks. In section III,

2. Types of attacks

A. DOS Attack

DoS attacks these days are a part of every net person's existence. They are occurring all of the time, and all of the internet users, as a network, have a few element in growing them, affected by them or even loosing time and money due to them. DoS attacks do no longer have something to do with breaking into computer systems, taking control over far flung hosts at the internet or stealing privileged data like credit card numbers. Using the net manner of speaking DoS is neither a Hack nor a Crack. It is an all new and unique concern.

The only cause of DoS attacks is to disturb the services supplied with the aid of the victim. Even as the attack is in vicinity, and no activity has been taken to fix the hassle, the sufferer would not be capable of provide its services on the internet. DoS attacks are clearly a shape of vandalism towards internet offerings. DoS attacks take gain of weaknesses inside the IP protocol stack with the intention to disturb net services. DoS attacks can take various forms and may be classified according to numerous parameters. Especially, in this study we differentiate denial of carrier attacks based on in which the origin of the attack is being generated at.

"Ordinary" DoS attacks are being created by using a single host. The handiest real way for DoS attacks to force an actual risk is to exploit some software or layout flaw. Such flaws can contains, as an instance, incorrect implementations of the IP stack, which crash the complete host while receiving a non-preferred IP packet (as an instance ping-of-loss of life). Such an attack might commonly have decrease volumes of information. Except a few exploits exist on the sufferer hosts, which have no longer been fixed, a DoS attack need to not pose a actual danger to excessive-quit offerings on now day's internet.

Those attacks interrupt services on a bunch by using stopping it from managing certain requests. That is a step in multi levels attack which is damaging that crash a number or prevents it from functioning satisfactorily. There are 3 kinds of DoS attacks:

- Errors in trusted programs can be used by an attacker to achieve not authorized get right of entry to a computer system. Particular examples of implementation errors are buffer overflows, race situations, and mishandling of non-permanent files.
- Creation of malformed packets that confuse the Transmission Control Protocol/Internet Protocol (TCP/IP) stack of the system that is attempting to reconstruct the packet.
- Fooling a system by misrepresenting oneself and giving access.

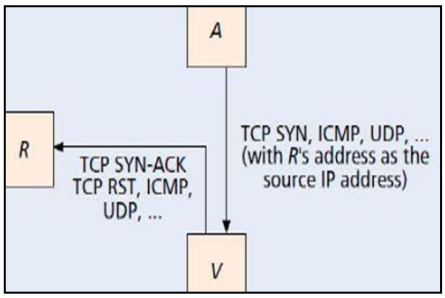

Fig 1: DOS Attack

In above fig, the attacking system sends out packets directly to the victim but hides its original IP address. It adopts the IP address of some other host which is R in this below diagram. The victim would have its further correspondence with host R assuming it was the source

B. DDOS Attack

DDoS (allotted Denial of provider) attacks could, usually, be created by a completely big quantity of hosts. Those hosts might be amplifiers1 or reflectors2 of some type, or maybe might be "zombies" (agent application, which connects lower back to a pre-described master hosts) who have been planted on far off hosts and had been anticipating the command to "attack" a sufferer. It is pretty common to look attacks created by using loads of hosts, producing masses of megabits per second floods.

Types of attacks or DDoS attack classification: In phrases of the variety of malicious entities concerned in an attack, we distinguish:

- Uni-source attacks – released by and originating from a only one supply;
- Distributed attacks – originating from a more than one of coordinated sources, although no longer necessarily involving more than one malicious stop consumer.

A DoS attack substantially threatens the community, especially if such an attack is distributed. A disbursed DoS (DDoS) attack is released by means of a mechanism called Botnet via a network of controlled computer systems. Software program software controls the computers and for particular capabilities, called ―bots. Bots are tiny scripts which can be designed to perform precise, automatic capabilities.

These attacks are a awful dream for little and separate web page as they can be overflowed by using a touch machine of botnet motion. They do no longer have the belongings and the inspiration to deal with the difficulty. DDoS attack is appreciably ordered into magnificence arrange layer attack and application layer attack [2]. The number one factor of the

layer 3 DDoS attack is to overpower the server and spent the information transmission with surges. The intentions of the utility layer attack are smashing the server with the aid of low and slight Institutions.

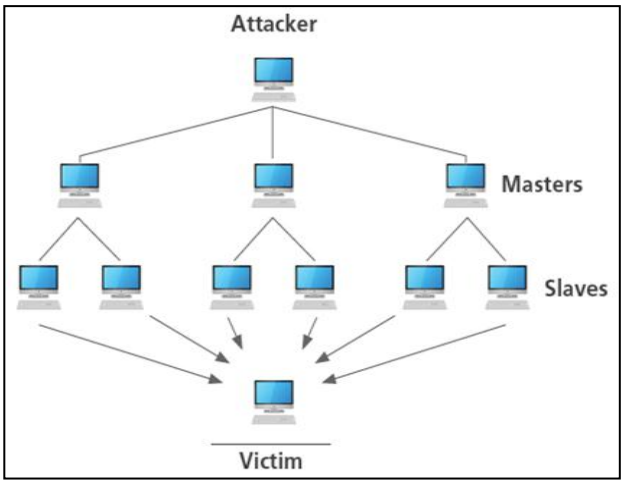

Fig 2: DDOS Attack

In Fig 2, it shows general DDOS attack architecture. The attacker first goes to master system and from that it goes to slaves systems then it attacks on victim system.

C. User to Root (U2R)

These attack are exploitations wherein the hacker starts off evolved off on the system with a easy consumer account and tries to misuse vulnerabilities inside the machine so one can obtain remarkable consumer privileges e.g. xterm, perl. Those attacks exploit vulnerabilities in operating systems and software program to gain root or administrator get admission to the system. As an example, recollect the buffer overflow attack. A buffer overflow occurs when this system writes greater statistics into the buffer area than the memory it has allotted. This permits an attacker to overwrite a record that controls this system execution path and seize the manager of the program to execute the attacker's code as an alternative the manner code. Bad programming practices and software insects are the fundamental threat elements. A powerful solution to the buffer overflow trouble is to hire reliable coding. While no safety measure is best, keeping off programming mistakes is continually the first-rate solution.

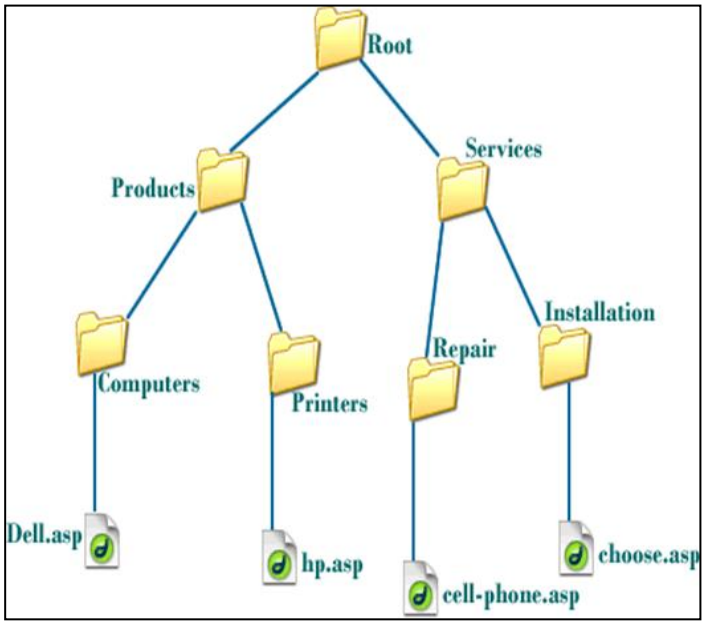

Fig 3: User to Root Attack

This show from a normal user pages attacker goes to root of the system to attack main systems.

D. Remote to Local Attacks

There are some equal things among this magnificence of intrusion and U2R, as similar kind of attacks may be carried out. In this situation the attacker does not have an account on the host and tries to obtain local access across a network connection. To acquire this, the attacker can execute buffer overflow attacks and exploit configurations. With this the attacker may obtain data by misguiding a human operator, rather than targeting software flaws. These classes may be used in IDS for classifying intrusions, rather than only differentiating between 'normal' and 'intrusion'. This will give more information about the kind of intrusion, which may additionally affect the selected method of reporting and acting on the suspected detection. Some known events may be classified as an intrusion while other event needs to be observed in the context of one or more events. This could lead to repetition of the same occasion or a very distinctive occasion but nevertheless IDS should be able to recognize simple, single event, attacks as well as complex, multiple event attacks. As an example, Ping of Death attack may cause the system to crash by sending large ping packets to a host.

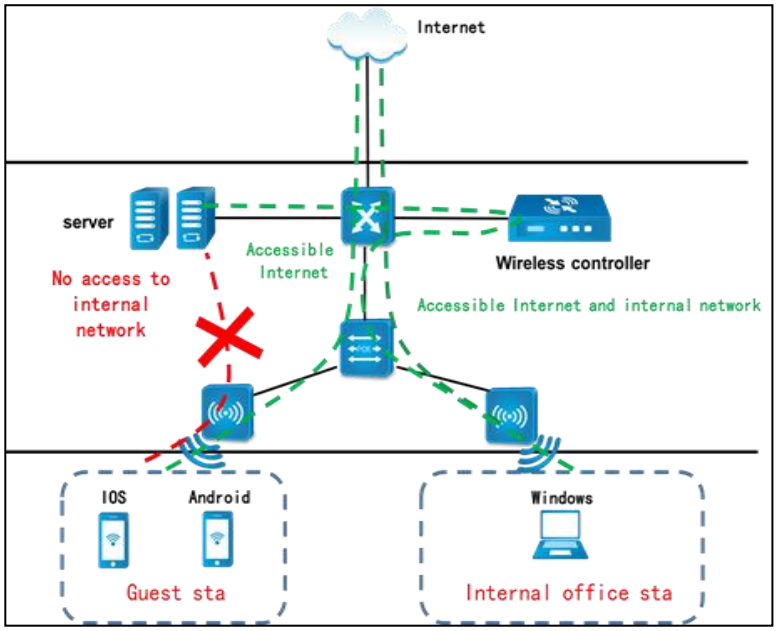

Fig 4: Remote to Local Attack

This above figure shows how attacker's attacks local machines remotely without having access.

Table 1: Different Attacks and Its Behaviour

S. No	Attack Name	Behaviour
1.	DOS	Attacker tries to prevent legitimate users from using a service.
2.	DDOS	The attacker will start by building network of infected machine
3.	U2R	Attacker has local access to the victim machine and tries to gain super user privileges
4.	R2L	Attacker does not have an account on the victim machine, hence tries to gain access.

Related Works

Khundrakpam Johnson *et al.* (2015)
In [1], to guard and shield web server from the attack, it is critical to know the nature and the conduct of genuine and ill-conceived customers. It is additionally critical to give access to the genuine customers and give a barrier framework against ill-conceived customers. The disbursed Denial of carrier (DDoS) attack is a primary risk to the net. By using its application layer convention DDoS can cause a huge pulverization by quietly making a passageway to the web server as it go about as one of the honest to goodness customers? The paper utilizes parameter of the system parcel like http GET, POST ask for and delta time to parent the precision in coming across the manageable attack. We utilize distinctive classifiers like Naive Bayes, Naive Bayes Multinomial, Multilayer Perception, RBF organize, Random Forest and so on to group the attack produced dataset. We look at the precision, genuine positive rate, false positive rate of every calculation by finding the perplexity grid.

Esraa Alomari *et.al* (2012)
In [2], A Botnet-based DDoS attack is without a doubt a genuine Internet issue that difficulties the development rate and the general population acknowledgment of online government and business destinations. In this paper, an unmistakable perspective of the Botnet construct DDoS attack with respect to the application layer, specifically at the web server, is shown. Incident around the world and income misfortunes of popular organizations and government Web locales are additionally portrayed, showing that extraordinary care ought to be taken and a further report ought to be directed to evaluate the span of the issue and afterward infer an ideal arrangement.

Qijun Gu *et al.* (2012)
In [3], Denial of service (DoS) attacks has turned into a noteworthy danger to current systems. To have a superior comprehension on DoS attacks, this article gives a review on existing DoS attacks and real resistance innovations in the Internet and remote systems. Specifically, we depict organize based and have based DoS attack strategies to outline attack standards. DoS attacks are arranged by their real attack attributes. Ebb and flow counterattack advances are additionally audited, incorporating real resistance items in arrangement and agent safeguard approaches in inquire about. At last, DoS attacks and protections in 802.11 based remote systems are investigated at physical, MAC and system layers.

Subramani rao *et.al* (2011)
In [4], among different online attacks hampering IT security, Denial of Services (DoS) has the most pulverizing influences. It has moreover placed giant weight over the security professionals of past due, in bringing out feasible shield preparations. Those attacks will be executed otherwise with an assortment of gadgets and codes. For the reason that there is

not a solitary solution for DoS, this attack has found out a way to win on internet for about decade. Thus, it ends up noticeably basic to complete these attacks in little proving ground conditions with a specific end goal to comprehend them better. Unlike other theoretical studies, this project lays down the steps involved in implementing these attacks in real time networks. These real time attacks are measured and broke down utilizing system activity screens. Notwithstanding that, this venture additionally subtle elements different safeguard methodologies that could be empowered on Cisco switches keeping in mind the end goal to relieve these attacks. The discovery and relief components planned here are successful for little system topologies and can likewise be reached out to practically equivalent to expansive areas.

Khaled M. *et al.* (2013)
In [5], A denial of service attack (DOS) is any form of attack on a structures management structure to impair a server from adjusting its clients. Attacks run from transferring a huge variety of solicitations to a server looking to back it off, flooding a server with large bundles of invalid information, to sending demands with an invalid or copied IP Address. On this paper we display the usage and analysis of three number one types of attack: Ping of death, TCP SYN Flood, and distributed DOS. The Ping of Death attack will be reproduced against a Microsoft Windows 95 System. The TCP SYN Flood attack can be mimicked towards Microsoft windows 2000 IIS FTP Server. Circulated DOS will be exhibited by re-enacting a dispersion zombie program with a view to carry the Ping of dying attack. This paper will display the potential harm from DOS attacks and destroy down the outcomes of the damage.

SANS Institute (2001)
In [7], Senior administrators are shrewdly focusing on Distributed Denial-of-Service (DDoS) attacks, since the budgetary results can be huge. An exhaustive examination of the monetary effect of a Ddos attack ought to incorporate both immediate and backhanded costs, remembering that the price of a DDoS attack is firmly solving to the period and sort of attack itself. This paper famous a version that can be utilized to valuation charges and quantifiable income (ROI) in mild of the specifics of each condition. Payback for DDoS confidence organizes can postpone from brief to underneath a half yr, contingent upon the highlights, value and execution of the picked organizes. In light of the way that complete scale patterns point to a proceeding with ascends in the recurrence and damage from DDoS attacks, a model, as an example, this seems to be steadily critical.

Adrien Bonguet *et.al* (2017)
In [8], Cloud computing it is a processing model that allows comprehensive, high quality and on-request get admission to a normal pool of notably configurable property (e.g., structures, servers, packages, stockpiling, and administrations). Denial-of-service (DoS) and disbursed Denial-of-provider (DDoS) attacks aren't kidding risks to the Cloud administrations' accessibility because of various new vulnerabilities offered via the idea of the Cloud, as an instance, multi-tenure and asset sharing. In this paper, new types of DoS and DDoS attacks in Cloud Computing are researched; especially the XML-DoS and HTTP-DoS attacks, and a few attainable discovery and relief structures are analyzed.
This study additionally gives a diagram of the current resistance arrangements and examines the analyses and measurements that are typically planned and used to assess their execution, which is useful for the future research in the space.

Zhang Chao-yang (2011)
In [9], Denial of Service (DoS) and circulated dissent of a service attack (DDoS) is presently a typical method for attack that influences truly arrange security and the nature of online administrations. This paper breaks down the DoS (DDoS) attacks anticipation standards and gives an intensive examination of existing avoidance strategies, proposed to forestall DoS (DDoS) attacks in three ways: utilizing a switch DoS attack counteractive action; increment the confided in stage module; increment framework guards.

Swati Paliwal *et.al* (2012)
In [10], These days it is vital to keep up an abnormal state security to guarantee sheltered and confided in correspondence of data between different associations. In any case, secured information correspondence over web and some other system is constantly under danger of interruptions and abuses. To control these dangers, acknowledgment of attacks is basic issue. Examining, Inspecting, Denial of facility (DoS), remote to user (R2L) attacks are a part of the attacks which affects enormous number of computers on this planet each day. Location of these attacks and anticipation of PCs from it is a noteworthy research subject for scientists all through the world. In this paper notion for usage of a Genetic algorithm (GA) based totally approach for age of standards to discover Probing, DoS and R2L attacks at the framework is proposed.

3. Conclusion
On reviewing and investigating the different DDoS attack location and relief plans we have reached a conclusion that the DDoS attack has an exceptionally awesome risk to the mutual and web conveyed frameworks and it is imperative to shield our framework from such sorts of attacks. Despite the fact that there are a great deal of answer for discovery and alleviating of the DDoS attack the significant downside in all the framework is that the framework recognizes the honest to goodness clients with extensive transmission capacity of information as an assailant. This paper investigates the DoS (DDoS) attack standards and gives an intensive examination of existing counteractive action procedures, proposed to avert DoS (DDoS) attacks in three ways: utilizing a switch DoS attack anticipation; increment the put stock in stage module; increment framework resistances. These are powerful techniques to Distributed DoS (DDoS) attacks from the edge of down to earth application. These days it is essential to keep up an abnormal state security to guarantee protected and confided in correspondence of data between different associations. Be that as it may, secured information correspondence over web and some other system is constantly under risk of interruptions and abuses. To control these dangers, acknowledgment of attacks is basic issue. Checking

out, Denial of service (DoS), far flung to consumer (R2L) attacks are a portion of the attacks which affects vast wide variety of computers on the earth every day.

4. References

1. Khundrakpam Johnson Singh, Tanmay De. An Approach of DDOS Attack Detection Using Classifiers. In Emerging Research in Computing, Information, Communication and Applications, 2015.
2. Esraa Alomari, Selvakumar Manickam, Gupta BB, Shankar Karuppayah, Rafeef Alfaris. Botnet-based on Distributed Denial of Service (DDOS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications. 2012; (0975-8887)49-7.
3. Qijun Gu, Peng Liu. Denial of Service Attacks, 2012.
4. Subramani rao Sridhar rao. Denial of Service Attacks and mitigation techniques: Real Time Implementation with Detailed Analysis SANS Institute Reading Room site, 2011.
5. Khaled M. Elleithy, Drazen Blagovic, Wang Cheng, Paul Sideleau, Denial of Service Attack Techniques: Analysis, Implementation and Comparison, Systemics, Cybernetics and Informatics, 2013.
6. Karami Park, McCoy. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services, 2015.
7. SANS Institute. The Changing Face of Distributed Denial-of-Service Mitigation, 2001.
8. Adrien Bonguet, Martine Bellaiche. A Survey of Denial of Service and Distributed Denial of Service and Defence in Cloud Computing, Future Internet. 2017; 9(43). doi:10.3390/fi9030043, 2017.
9. Zhang Chao-yang. DOS attack analysis and study of new measures to prevent. International Conference on Intelligence Science and Information Engineering, 2011.
10. Swati Paliwal, Ravindra Gupta. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm. International Journal of Computer Applications. 2012; (0975-8887):60.
11. Botha M, Solms R. Utilizing Neural Networks For Effective Intrusion Detection, ISSA, 2004.
12. Christoph L. Schuba, *et al*. Analysis of a Denial of Service Attack on TCP, IEEE Symposium on Security and Privacy. 1997, 208.