Distributed denial-of-service attacks

Author: Adriana Silva

Email: as1344829@gmail.com

University of Algarve, Portugal

Abstract:

Distributed Denial-of-Service (DDoS) attacks are the intimidation trials on the Internet that deplete the network bandwidth. Researchers have introduced various defense mechanisms including attack prevention, traceback, reaction, detection, and characterization against DDoS attacks, but the number of these attacks increases every year, and the ideal solutions to this problem have eluded us so far. A classification of detection approaches against DDoS attacks is presented with the aim of giving deep insight into the DDoS problem.

Introduction

Denial-of-service attacks are designed in order to make a machine or network resource unavailable to its users. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of attacks are possible, where the attack comes from a large number of points—and defending against them is thus much more difficult. Such attacks can originate from “zombie bot computers.” An alternative technique involves innocent systems (which are referred to as “botnets” from the word robot) being fooled into sending traffic to the victim.

Figure 1 DoS Attack

A Denial-of-Service attack DoS is such kind of attack which targeting the accessibility of network system resources for other legitimate users [1]. In other kinds of attacks, the information is stolen or changes the data but DoS attack aim is slow down or takes down system resources for other users. The attackers' goals are diverse; he does that for simple fun or financial gain and ideology. The first step in denial of service (DoS) attack is generating high rate malicious traffic [2]; direct that malicious traffic flow towards victim network or resources' and consuming computing resources of target exhaustively. Therefore legitimate users are not able to access the system resources [3].

DoS attacks influence all organizations of the world. They can target all 7 layers of OSI model from physical layer a to the application layer. The difficult part of DoS attack is detection because traffic type seems legitimate traffic to the system resources [4].

There are two types of DoS attacks. A (non-distributed) DoS attack and distributed DoS attack. In non-distributed DoS attack, an attacker uses a single machine's to overwhelm another machine. If target machine powerful then this type of attack doesn't affect target system. While in distributed DoS case, the attacker originates from multiple computers simultaneously, focus on single or multiple machines, therefore, causing the victim's resources exhaustion [5].

How does an attack work?

1) The first attacker chose to find the goals and system for the attack. Then he discovers the target network and calculated all the limitations of network and system resources.
2) After first phase an attacker floods company’s network or system with useless and malicious information [6].
3) Since Network and system can only handle a limited amount of traffic and an attacker overloads the targeted system with the unlimited amount of traffic.
4) Denial-of-service attacks disable the computer or the network partially or completely depending on the nature of the enterprise [7].

For example in authentication flood, the users send an authentication request to AP, AP respond with approval if there is space for approving. If the user has malicious

intention then he can flood the AP by sending the flood of authentication request which causes AP to respond and hence others nodes of the network face DoS [8].

Attack Types

1. Packet Internet or Inter-Network Groper (Ping) Flood Attack or (ICMP echo)
2. (synchronization)SYN Flood Attack (DoS attack)
3. DDoS Attack (Distributed SYN Flood)
4. Land Attack (Local Area Network Denial)
5. Authentication request flood
6. Association request flood
7. CTS Flood attack
8. RTS DoS Attack
9. Beacon Flood

1.1.1 *3.1 Ping Flood Attack (ICMP echo)*

In Ping flood attack, the attacker focus is network bandwidth. An attempt by an attacker on a network focus is bandwidth, fill a network with ICMP echo request packets in order to slow or stop legitimate traffic going through the network. As shown in fig 2.

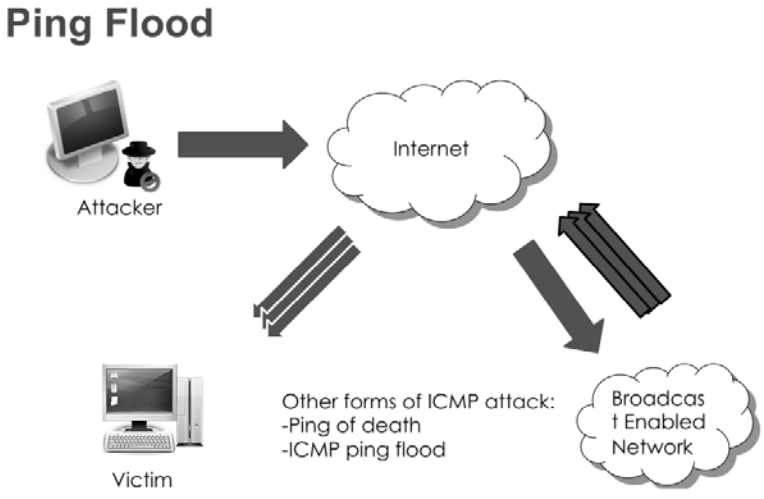


Figure 2Ping Flood Attack

Ping is a basic network program, which used for checking that system is alive to receive data or not. When a system receives the Ping message, the system must reply if it alive and active. Ping flood is also known as ICMP flood, To create DoS in the network, the attacker sends thousands of ping messages to victim node and victim node just only busy with responding that he is alive. At that time victim system are not able to process the other nodes information. Victim system is even not able to receive other data in worst case scenario. [10]

1.1.2 *3.2 SYN Flood Attack*

SYN messages are exchanges when a client needs to connect to a server in TCP. The user sends an SYN message, in response server send back SYN-ACK message [11]. In SYN flood attacker sends so many SYN requests that the system is notable for other nodes to respond. Since the server is busy with the reply to malicious SYN message and legitimate users are in the waiting stage. As explained in fig 3. [9]

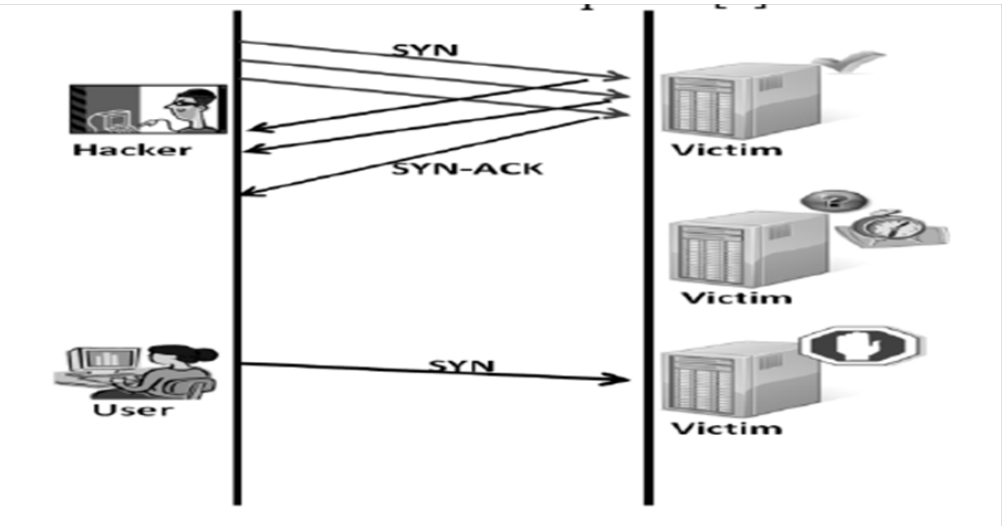


Figure 3 SYN Flood Attack

1.1.3 *3.3 DDoS Attack*

Distributed Denial of Services (DDoS) is such kind of DOS attack there are many step stone systems are used for generating malicious traffic and after that directed the flow of malicious traffic to the victim system and that cause a Denial of Service (DoS) attack. As shown in fig 4

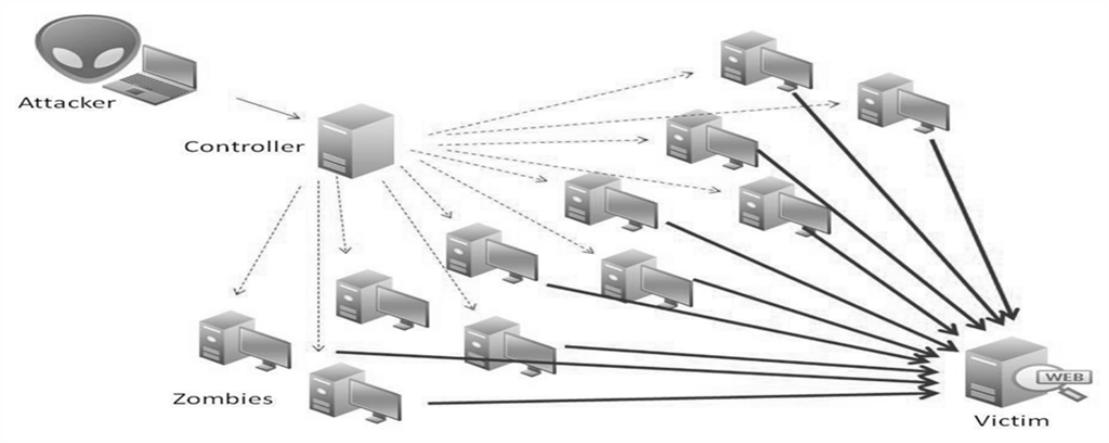


Figure 4 DDoS Attack Flow of traffic

3.3.1 How DDoS Attacks Work

There are three steps to launch the DDoS attack [12]. The main goal of the attacker is launching a large traffic and makes that flow direction towards victim system. For that, he first compromised many other systems called zombies. They are compromised using Trojans, infected system with malicious software and getting control of that zombie system. Using zombies having many advantages for the attacker, it's become impossible to block all zombies IPs addresses after detection. Each zombie generated traffic and direct that flow towards the victim. Even zombies detected attacker ID can't be detected. [13]

To handle zombies there is a controller in the second step. This may be also a compromised system or a system used by attacker temporarily. Controller, take instruction from an attacker, like how many zombies would be involved and for how much time, also malicious traffic format. Even victim find the controller, attackers ID are still hidden from the victim. The zombies and controller are used as step stone in the above two phases. The third step is traffic directed towards the victim [14].

3.3.2 Types of DDoS Attacks

There are many types of DDoS attacks. Common attacks include the following:

- **Traffic attacks:** In traffic attacks, the DDoS traffic is legitimate traffic like TCP, UDP, and ICMP. It's impossible for the victim to distinguish among ma-

licious traffic and legitimate traffic because traffic pattern is same as like legitimate traffic. That's preventing legitimate user to access the system or network [15].

- **Bandwidth attacks:** In that kind of attack attacker's aim is bandwidth only. So he fills the bandwidth with junk data. Traffic can be easily distinguished by victims but the amount of traffic is so much that it can't be handling [16].
- **Application attacks:** In application attack, the attacker exploited the application layer and resource unavailable for legitimate users after malicious traffic. Application layers distributed data to system resources.

1.1.4 *3.3.3 Land Attack (Local Area Network Denial)*

- It's an old kind of attack. In land attack, the attackers send malicious packets such that it has the same source and destination address. Both host and source addresses are victim addresses. It's mostly used in local area networks. The victim system is lock up after getting that packets and response to itself and loop continue until system detected or shutdown. As shown in fig 5.

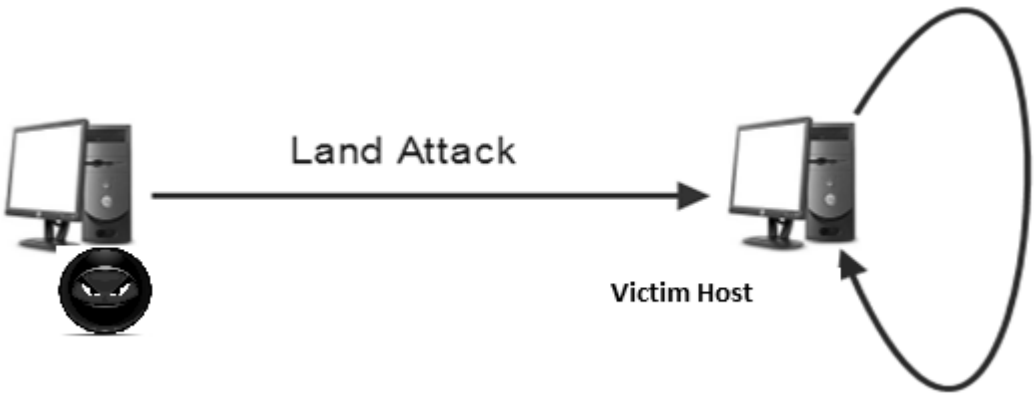


Figure 5 Land Attack (Local Area Network Denial)

1.1.5 *3.3.4 Authentication request flood*

- A node after listening bacon sends authentication request to AP, to associate itself with AP.
- AP maintains a state table, where there is the list of authenticated nodes.
- There are two kinds of effects of such DoS attack, First AP affected, because commit its normal operation and serve the request, when the request is too

much, AP only will do the job maintaining the state table. The second effects are legitimate users when state table is filled by malicious requests, there would be no space for accepting more legitimate requests. State table also has limitations. Shown in fig 6.

- In that kind of attack attacker first, need to spoof the MAC of others node. So it's little difficult to launch if there is the proper mechanism of protection for MAC addresses. [17]

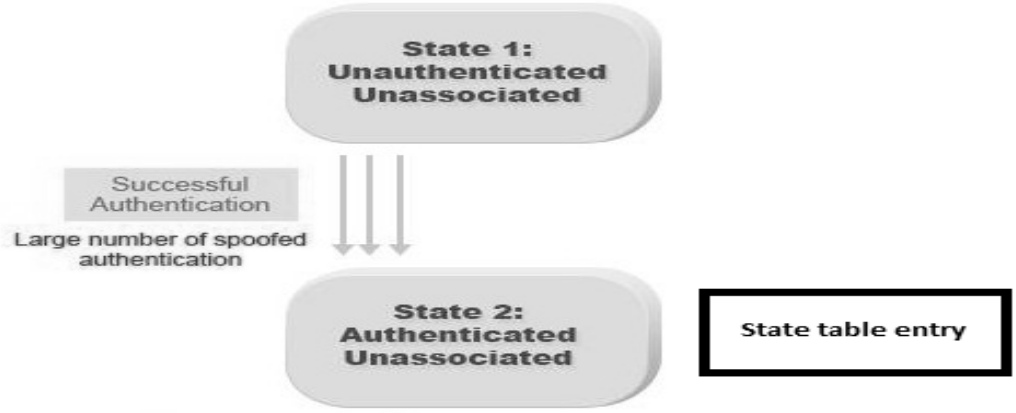


Figure 6 Authentication request flood

1.1.6 *3.3.5 Association request flood*

- After authentication, there is association step, in association step AP associate a client and make the entry in the association table. But this association is also vulnerable to DoS. There is de-authentication packet after authentication from AP if that de-authentication packet is spoofed and an attacker crack passwords then he can also reach to the association table. As shown in fig 7.
- That table also has limits and if requests are beyond the limit of an associated table, there would defiantly a DoS attack.
- It's harder to launch, because of the authentication step. An attacker must cross the authentication step [18].

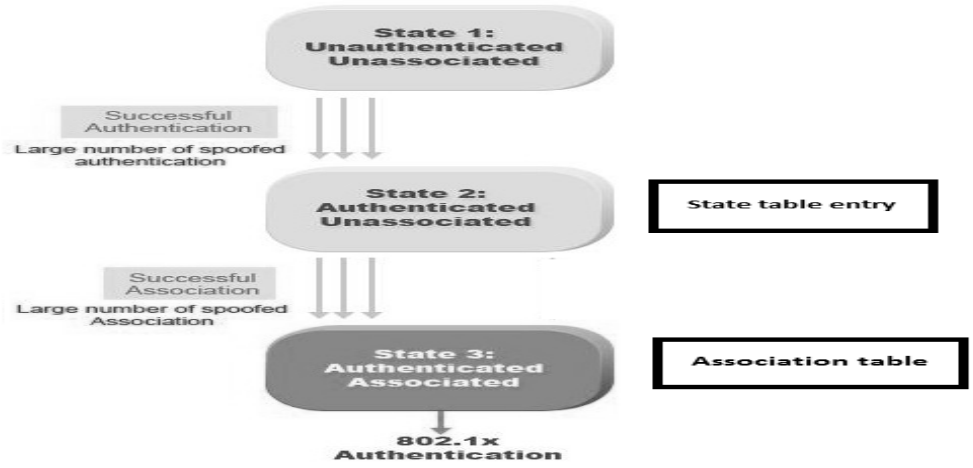
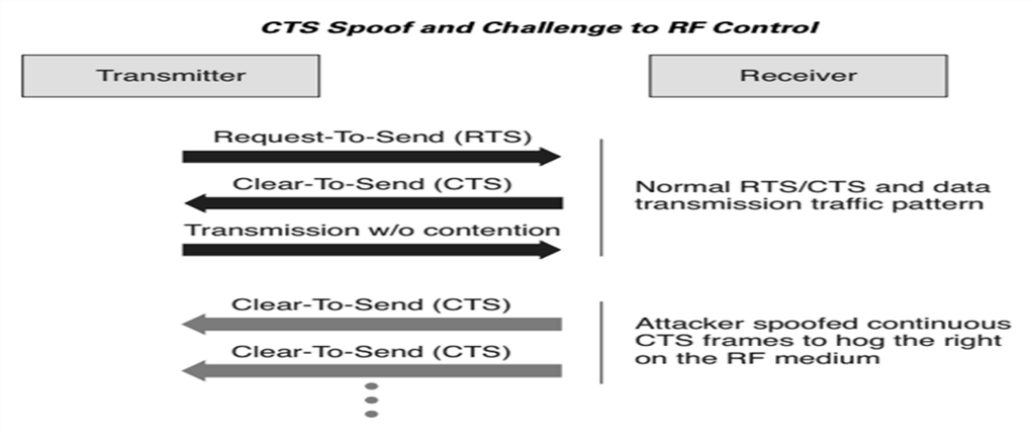


Figure 7 Association request flood

1.1.7 *3.3.6 CTS Flood attack*

- IEEE 802.11 set standard for wireless networks. As we discussed in the previous chapter, first there is RTS, followed by CTS, then DATA and ACK frame.
- Other nodes after listening CTS just update NAV and stay in quite a mood and start sensing media after CTS maintained time duration.
- This behavior can be exploited by an attacker, if an attacker sends CTS to others after the interval to others node, other nodes would be in quite a state after receiving.
- If the sending malicious CTS are back to back, no other node is able to send data. As shown in fig 8.
- There is also possible that CTS sender node increase the duration and nodes goes in the quiet state for the extra time.[17]



1.1.8 *3.3.7 RTS DoS Attack*

- RTS frame includes Frame Control, Duration, RA, TA, and FCS. By sending RTS frames mentioning large transmission duration, an attacker reserves the wireless medium for the overdue time and forces others wireless stations sharing the RF medium to delay their transmissions. As shown in fig 9.[18]

Figure 8CTS Flood attack

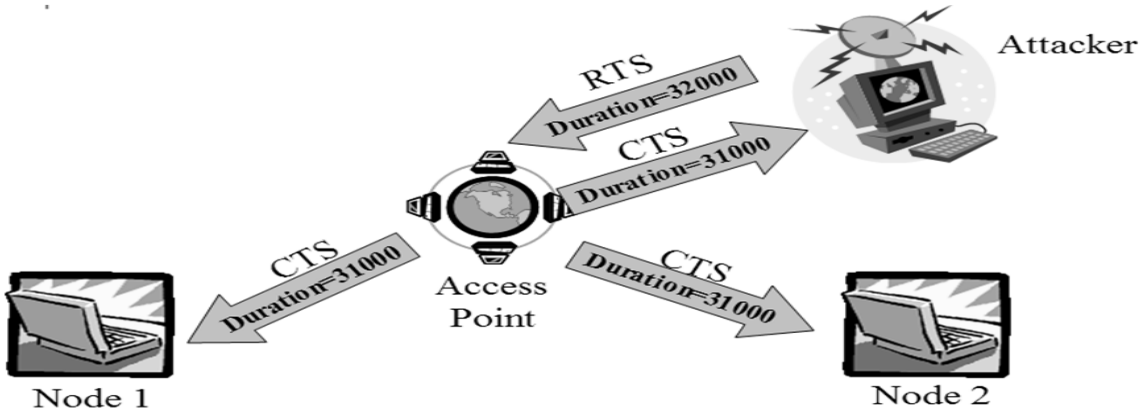


Figure 9 RTS Flood

1.1.9 *3.3.8 Beacon Flood*

Wireless clients can detect the presence of access points by listening for the beacon frames transmitted from APs. Beacon flood is launched by an attacker in such way, that first he generates thousands of malicious beacons around legitimate [20] AP that made difficult for the individual station to find the legitimate AP for the association. As shown in fig 10.

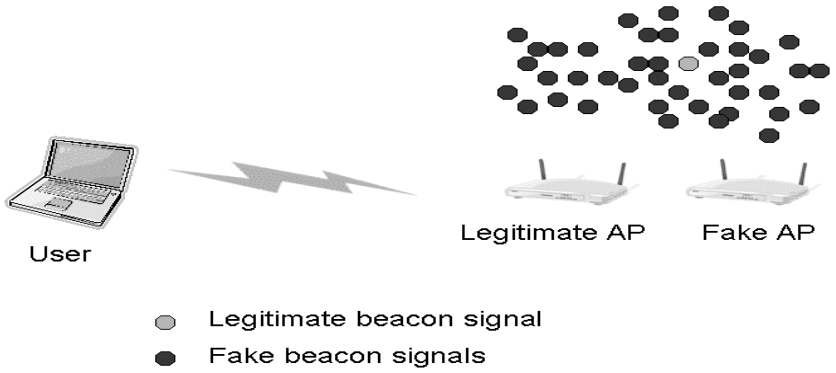


Figure 10 Beacon Flood

Damage & Costs

1. **Other affecting:** There are many costs associated with denial-of-service attacks. Like an attacker target the server, when server down, it does not only effect the server but also other users and sites associated with that victim server [19].
2. **Bandwidth wastage:** Network resources are shared among many stations. Like bandwidth. If attacker launches DDoS attack it does not only affect the target because of wastage of bandwidth and that also slow down the activity of non-victim systems [21].
3. **Extra network channels:** To detect the attack users must use extra resources only to handle and prevent their system from such kind of attacks. Like emailing, making logs etc.
4. **Insurance& Bandwidth cost:** As in international market we pay per byte. In DoS attack case the traffic is very high from normal traffic and that also increases the bandwidth cost.

How to handle DoS

- **Protecting:** The first step should be protected in such kind of attack, protection mechanism should be installed by ISP, and there should be an agreement between ISP, an insurance policy. Most of the people do that after learning a lesson.

- **Detecting:** If you detect properly then you would be able to respond accurately. For detection, there should be proper check and balance on log system, traffic pattern, updated blacklist and all updated detection software [28]. The attacker use different mechanism to launch the attack. So maybe detection not helps out in some kind of attacks [22].
- **Reacting:** Reaction step comes when there is no proper protection and detection mechanism. In that step there would some technical steps which are mostly implemented, are informing ISP, start backup system and moving data to the backup system, decreasing the incoming traffic, applying available data content filters on incoming traffic, redirecting traffic, shut downing after data is moved. [30][23]

Available Solutions

- The DoS attacks at the MAC layer discussed here are very common in the IEEE 802.11 standard networks.
- The attacker exploited mostly the non-implementation of the authentication method for management and control frames.
- Mostly available solutions are cryptographically protecting of management and control frames. In that method first step is finding the vulnerability on the basis of cryptography and then the possible solution to mitigate these attacks.
- IEEE made an amendment to the original standard IEEE 802.11 and releases a new standard 802.11w.It included the security features for management frames like data confidentiality, data origin authenticity, and replay protection [27].
- But for control frames, there are still no cryptographic protection schemes at the MAC layer. So control frames are still vulnerable to DoS attack. An attacker can easily exploit the control frame by spoofing them and then use for resource exhaustion.
- The de-authentication vulnerability, in particular, can be fixed by authenticating control frames explicitly [26][31].

- De-authentication flooding, in particular, can be mitigated by delaying the effect of requests [33][34].
- In RTS DoS attack, the network performance can be restored back by Reevaluate RTS Duration (RRD) technique [25].
- MAC address spoofing can be protected if there is incrimination mechanism implanted in firmware in each node [32]. When a node sends its MAC address there would incrimination after next frame by sender node. Since firmware functionality of wireless card can't be changed by an attacker. The receiver will only accept and response such frames which have incremented MAC [24] [29].

References

1. M. Naeem, Jorge Diaz-Martinez, Shariq Aziz Butt and Nicolo Montesano, “Trends and Future Perspective Challenges in Big Data”, in Proc. Of The Sixth Euro-China Conference on Intelligent Data Analysis and Applications (ECC2019) Arad-Romania, March 2020.
2. Z. Haider and M. Saleem,"Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.
3. A Khalid, SA Butt, and S Gochhait, “Agile Scrum Issues at Large-Scale Distributed Projects: Scrum Project Development At Large”, in International Journal of Software Innovation (IJSI), Vol 8, Issue 2, Pages: 85-94, IGI Global 2020.
4. S Gochhait, SA Butt, and A Ali, “Cloud Enhances Agile Software Development” Book Chapter in Cloud Computing Applications and Techniques for E -Commerce, Pages: 28-49, IGI Global, 2020.
5. M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.
6. T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.
7. S. A. Butt, and M. Shoaib, "IoT Smart Health Security Threats," in proc. of 19th International Conference on Computational Science and Its Applications (ICCSA), Saint Petersburg, Russia, 2019, pp. 26- 31. doi: 10.1109/ICCSA.2019.000-8.
8. M. Asam and Z. Haider, "Security Issues in WBANs", in proc. of Arxiv, Volume arXiv:1911.04330 [cs.NI], November 2019.
9. M. Asam and Z. Haider, "Novel Relay Selection Protocol for Cooperative Networks", in proc. of Arxiv, Volume arXiv: 1911.07764 [cs.NI], November 2019.

10. Zeeshan Haider, Muhammad Asam, Shariq Butt and Aleena Ajaz, "Mitigation of Wireless Body Area Networks Challenges using Cooperation", International Journal of Security and Its Applications (IJSIA), ISSN: 1738-9976(Print); 2207-9629(Online), NADIA, (2020), Vol. 14, No. 1, pp. 15-30.
11. SA Butt and M. Ajmal Azad, "A multivariant secure framework for smart mobile health application", in Transactions on Emerging Telecommunications Technologies, Aug. 2019.
12. M. Asam and A. Ajaz, “Challenges in Wireless Body Area Network”, in Proc. of International Journal of Advanced Computer Science and Applications, Volume 10, No. 11, Nov. 2019.
13. SA Butt and A. Ali, "Predictive Variables for Agile Development Merging Cloud Computing Services", in Proc. of IEEE Access, Volume 7, 2019. DOI: 10.1109/ACCESS.2019.2929169.
14. P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.
15. P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.
16. SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.
17. SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.
18. P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.
19. P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.
20. SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.
21. SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.
22. Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.
23. T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.
24. T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.
25. Fawad, U., et al. "Proton, UV, and X-ray Induced Luminescence in [Tb.sup.3+] Doped Lu[Gd.sub.2][Ga.sub.2][Al.sub.3][O.sub.12] Phosphors." Crystals, vol. 10, no. 9, 2020.

26. Fawad, U.; Kim, H. J.; Gul, Ibrahim; Khan, Matiullah; Tahir, Sajjad; Jamal, Tauseef; Muhammad, Wazir. 2020. "Proton, UV, and X-ray Induced Luminescence in Tb3+ Doped LuGd2Ga2Al3O12 Phosphors" *Crystals* 10, no. 9: 844.