# IoT Smart Health Systems

Author: **Dr. Abbas Khurum**

**Kiramat and Silva**

Email: abbaskhurram98@gmail.com

## Abstract:

This article is about an architectural hardware-software model creation—home-based smart health model—to boost healthcare to a higher position within society. As an emerging field, smart health modeling is still insufficient. Current smart health services are hospital centered, data are scattered and application dependent, and health service provision presents attention delays. Analyses of Internet of things, Internet of medical things, and smart health applications potentials are the bases for the proposed home-based smart health model.

In addition, the model should aim for an IoT-assisted cloud-based health monitoring system, using different physiological and environmental signals to provide DLA contextual information. The proposed infrastructure at the same time could include health care providers to monitor older or lonely people health status and behavioral changes, as well as monitoring rehabilitation and recovery processes.

# 1. Introduction

**The initial information and communication technology (ICT) adoption in the healthcare sector main contribution was cost reduction and efficiency. The mobile devices arrival with positioning capabilities set up m-health, which added leverages to e-health, such as global availability, immediacy, and monitoring. Another evolving concept is smart health (s-health), which is based on both smart city and Internet of things (IoT) use. "Smarter cities make their systems instrumented, interconnected and intelligent."[1] IoT allows connecting identifiers, sensors, devices, and computers through wired and wireless networks.[2,3]**

# 2. CHALLENGES IoT smart health

Only five years ago there was a breeze of IoT everywhere, and people were talking about vision 2020 where 20 billion IoT devices would be online. Now in 2019, we are close to that reality, and IoT is rapidly evolving into the atmosphere in various fields. All the tech giants are now considering the IoT as it finds a lot of applications in smart homes, vehicular networks, healthcare, big data, etc.

A recent survey in the US shows more than 50% population willing to spend $500 on smart home devices and appliances. IoT is most widely deployed in smart homes to automate various home tasks. These smart homes devices are transforming TV, refrigerators, doors, and that makes life easier for the residents. This also allows business to offer IoT devices and services to their customers.

3. **Threats to smart home IoT**

While IoT promises a lot of convenience for the end-users as apparent in the smart homes, the security and privacy issues are growing concerns because not much work is done in this regard, talking about security by design. From WannaCry incident it is apparent that IoT devices are an open opportunity for hackers to launch excessive attacks and undermine a lot of commercially available devices such as Belkin WeMo motion sensor, Nest Smoke Alarms, Withings Smart Body Analyzer lack security features to prevent the device against any malicious users. Security researchers have analyzed the devices in great depth and found them vulnerable to various security threats. These devices communicate in plain-text, which can be eavesdrop by a malicious entity. In addition to security, privacy issues are also apparent. These sensors, used in abundance have a lot of personal information that an attacker can use to track, as found by researchers in the widely used motion sensors. These issues will continue to persist and demand attention and awareness from technology innovators and consumers.

### 3.1.1. EXPOSED NODE PROBLEM

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes because of a neighboring transmitter [2]. Consider an example of 4 nodes labeled R1, S1, S2, and R2, where the two receivers (R1, R2) are out of range of each other, yet the two transmitters (S1, S2) in the middle are in range of each other (see figure 7).

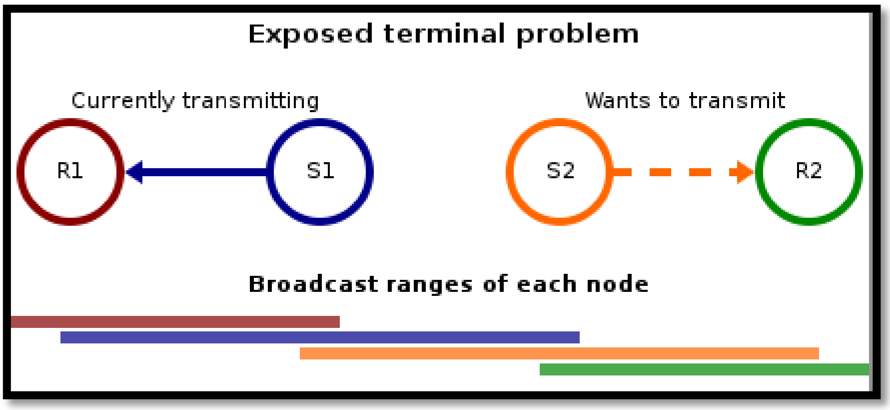



**Figure 7 Exposed Terminal Problem**

Here, if a transmission between S1 and R1 is taking place, node S2 is prevented from transmitting to R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor S1. However note that R2 could still receive the transmission of S2 without interference because it is out of range of S1.

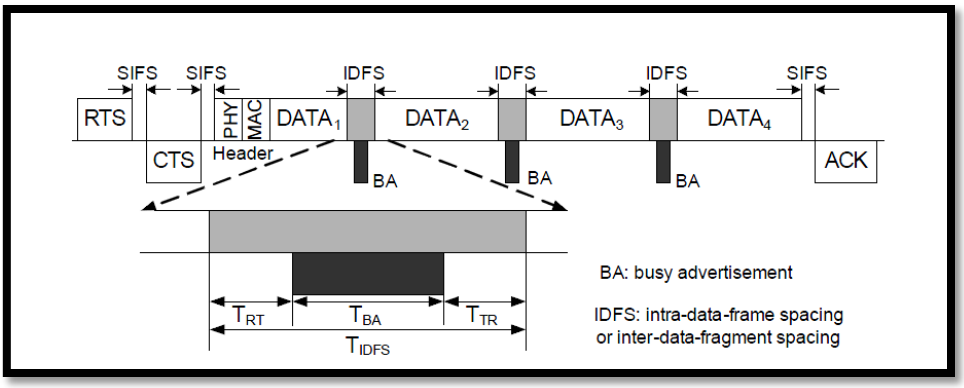



**Figure 9** Four-way handshake with busy advertisement signals

## 4. 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

## 4.1. 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.

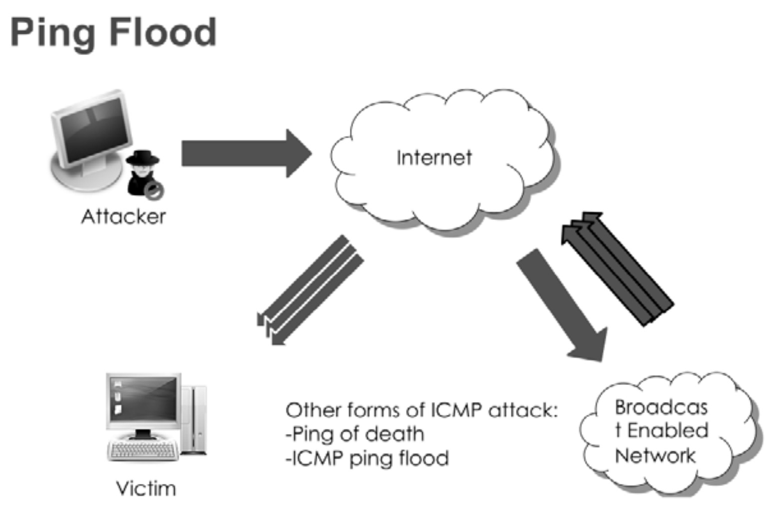



Figure 1Ping Flood Attack

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]

## 4.2. 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]

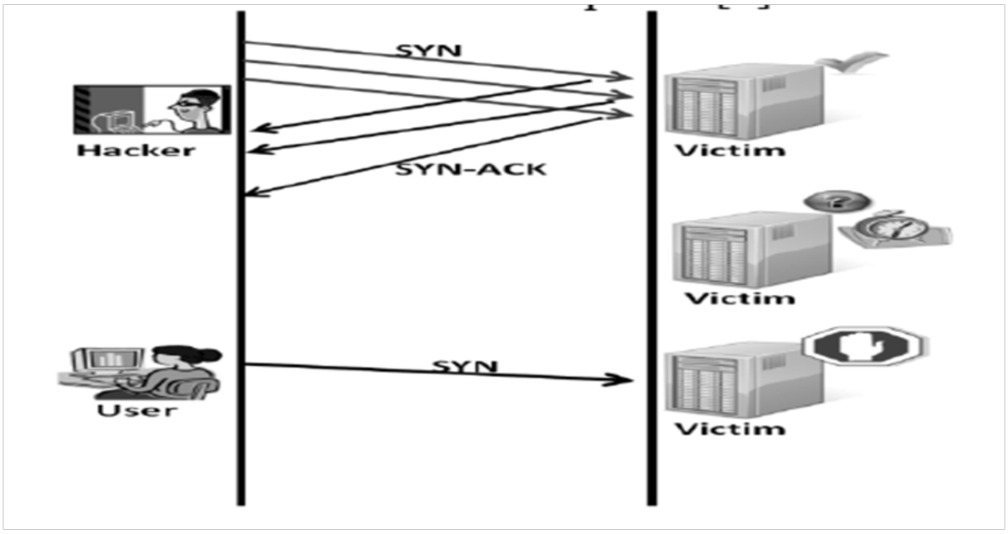



Figure 2 SYN Flood Attack

## 4.3. 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

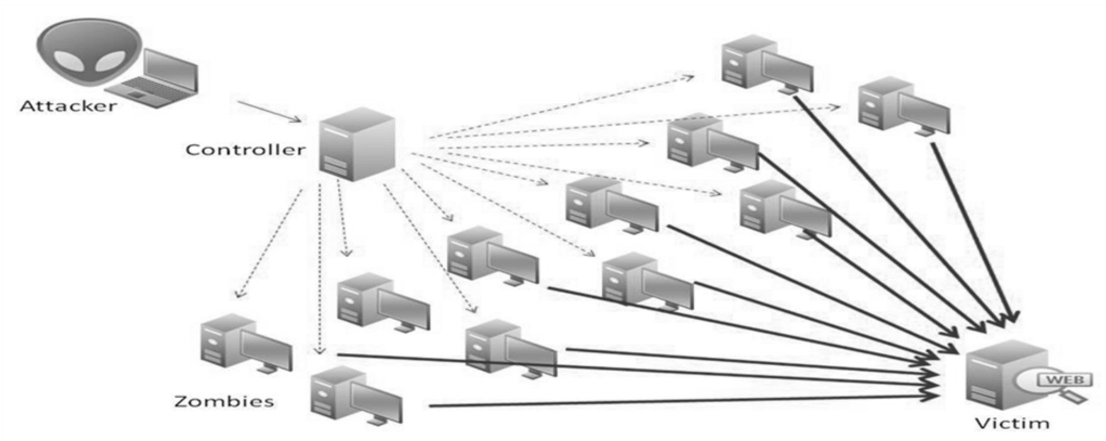



Figure 3 DDoS Attack Flow of traffic

### 4.4. 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].

## 5. 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 malicious 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.

## 5.1. 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.

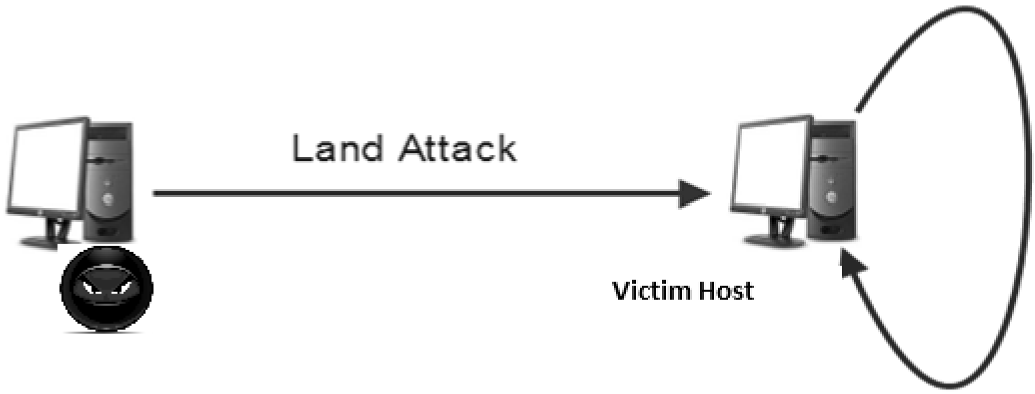



Figure 4 Land Attack (Local Area Network Denial)

### 1.1.1 *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]

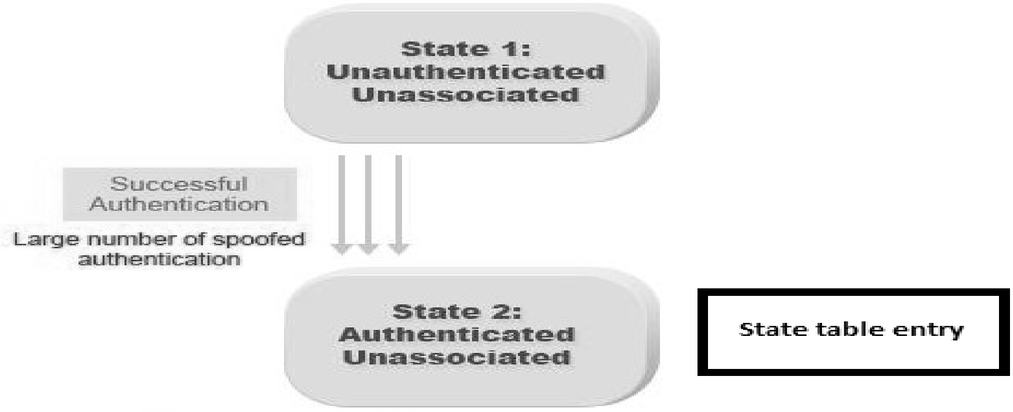



Figure 5 Authentication request flood

### 1.1.2 *Association request flood*

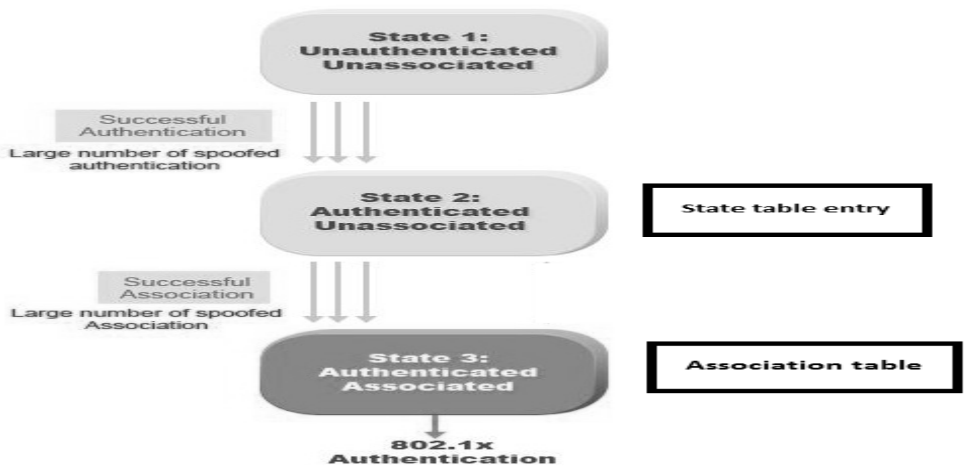
- After authentication, there is association step, in association step AP associate a client and make the entry in the association table. But this association is also vulnerable to DoS. There is de-authentication packet after authentication from AP if that de-authentication packet is spoofed and an attacker 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 6 Association request flood

•

### 1.1.3 ***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]

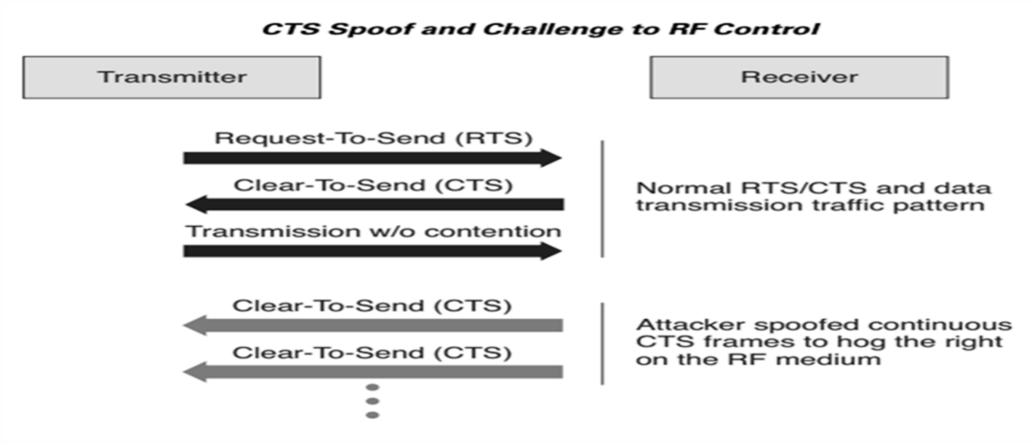



Figure 7CTS Flood attack

### 1.1.4 ***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]

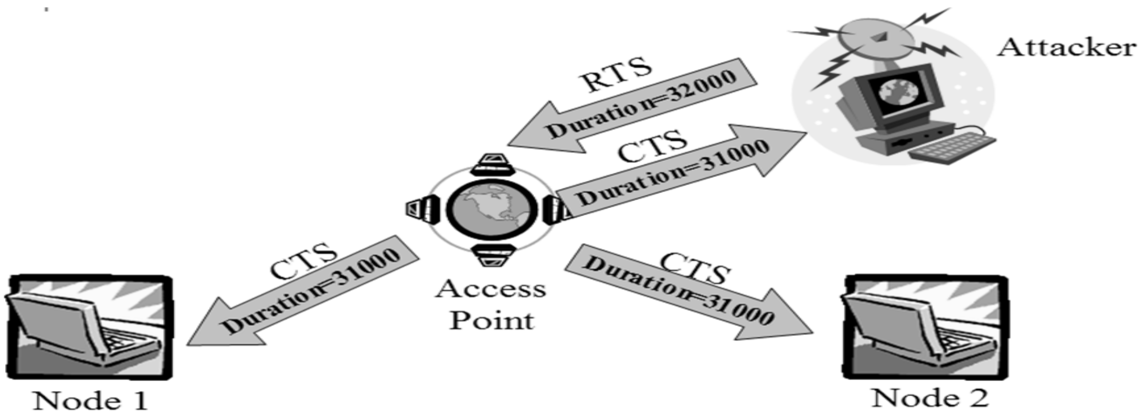



Figure 8 RTS Flood

### 1.1.5 ***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.

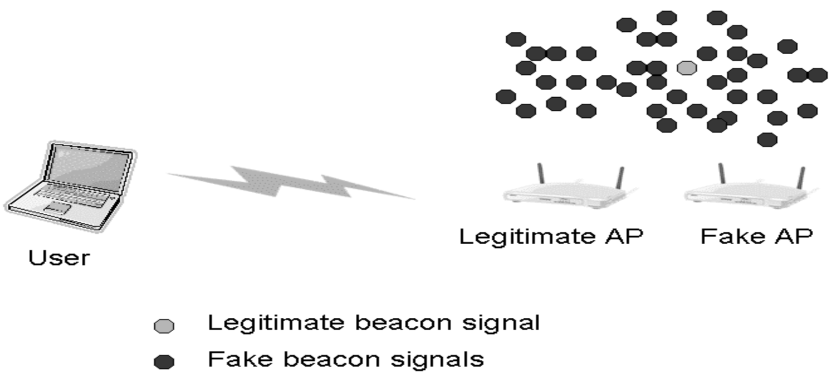



Figure 9 Beacon Flood

## 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]

# 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 $Tb^{3+}$ Doped $LuGd_2Ga_2Al_3O_{12}$ Phosphors" *Crystals* 10, no. 9: 844.