Tutorials for Internet of Things(IoT)

Khurum Abbas, Wajih un Nabi, Shah Hassan, Dawood Sher Jan, Muhammad Haris Khan Abbasi, Kiramat Ullah

wajihunnabi@hotmail.com, shahhasssan472@gmail.com.

muhammad.haris.abbasi97@gmail.com, alpha72784@outlook.com

Abstract: We're entering a new era of computing technology that many are calling the Internet of Things (IoT). Machine to machine, machine to infrastructure, machine to environment, the Internet of Everything, the Internet of Intelligent Things, intelligent systems—call it what you want, but it's happening, and its potential is huge. . The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. As a result, huge volumes of data are being generated, and that data is being processed into useful actions that can "command and control" things to make our lives much easier and safer—and to reduce our impact on the environment.

I. INTRODUCTION

IoT stands for "Internet of things". It is a network of physical objects or things embedded with electronics, sensors, software and network connectivity, enabling them to collect and exchange data.

It refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data. IoT further means adding a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate without a human being involved, and merging the digital and physical worlds.

II. Applications

Applications of Internet of Things

Internet of things has a wide applications range from industry and farms to cars and homes. It can help the human kind in everyday tasks and also cover the manufacturing needs. Through IoT we can make the machines smart enough to reduce human labor to almost nil.

According to HP, by 2025 number of connected devices will be 1.0 trillion [1]. The impact IoT will have on the economy then for your information as per the Cisco report IoT will generate $14.4 trillion in value across all industries in the next decade [2].

2.1 Smart Home

Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels

Smart home enables you to turn on air conditioning before you reach home, switch of the lights even after you have left the house, temporarily lock and unlock the doors, update you with the status of the all the expensive appliances at home and etc.

An equipment tracking app provides an airline's engineers with a live view of the locations of each piece of maintenance equipment. By increasing the efficiency of engineers, this IoT application is not only generating significant cost savings and process improvements, but also impacting the customer experience in the end through more reliable, on-time flights.

Figure 2.1 a connected home

2.2 Airlines

2.3 Pharmaceutical

A medication temperature monitoring app uses sensors to detect if the medication's temperature has gone outside of the acceptable range and ensures medical supplies still meet quality standards upon delivery. The handling temperatures of medications, vaccines for examples, is critical to their effectiveness. IoT based smart applications can be used to monitor that medications are kept within the proper handling temperature range, but also to remind patients when it is time to take their medication.

Figure 2.2 IoT in healthcare

2.4 Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to relieve real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied.

2.5 Connected Cars

A connected car is a vehicle which is able to optimize its own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity.

Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, and Google are working on bringing the next revolution in automobiles.

Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet. But it seems we are getting there.

2.6 Agriculture

With the continuous increase in world's population, demand for food supply is extremely raised. Governments are helping farmers to use advanced techniques and research to increase food production. Smart farming is one of the fastest growing field in IoT.

Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT.

2.7 Energy Engagement

Power grids of the future will not only be smart enough but also highly reliable. Smart grid concept is becoming very popular all over world.

The basic idea behind the smart grids is to collect data in an automated fashion and analyze the behavior of electricity consumers and suppliers for improving efficiency as well as economics of electricity use.

Smart Grids will also be able to detect sources of power outages more quickly and at individual household levels like nearby solar panel, making possible distributed energy system.

Figure 2.3 smart power grid

History:

The Internet of Things (IoT) has not been around for very long. But human are wishing for machines to communicate with one another since the early 1800s. Machines have been providing direct communications since the telegraph was developed in the 1830s and 1840s.

The Internet, itself a significant component of the IoT, started out as part of DARPA (Defense Advanced Research Projects Agency) in 1962, and evolved into ARPANET in 1969. In the 1980s, commercial service providers began supporting public use of ARPANET, allowing it to evolve into our modern Internet [3].

The Internet of Things was officially named in 1999. One of the first examples of an Internet of Things is from the early 1980s, and was a Coca Cola machine, located at the Carnegie Melon University. Local programmers would connect by Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip.

Till 2013, the Internet of Things had evolved into to a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems. The traditional fields of automation including the automation of buildings and homes, wireless sensor networks, GPS, control systems, and others, all support the IoT [4].

III. Security.

3.1 Definition:

Iot Security is the area of effort concerned with safeguarding connected devices and networks in the internet of Things.

Fig 3.1: Iot Security

3.2 Explanation:

It has be found that the IoT is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary[5]. Most of the technical security concerns are similar to those of conventional servers, workstations and smartphones, but security challenges unique to the IoT continue to develop, including industrial security controls, hybrid systems, IoT-specific business processes, and end nodes.

3.3 Security- The biggest Concern in IoT:

Security is the biggest worry in adopting Internet of things technology. In particular, as the

Internet of things spreads widely, cyber attacks are likely to become an increasingly physical

(rather than simply virtual) threat. In a January 2014 article in Forbes, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and

thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators[6].

3.4 IoTSF:

As a response to increasing concerns over security, the Internet of Things Security Foundation(IoTSF) was launched on 23 september 2015. IoTSF has a mission to secure the

Internet of Things by promoting knowledge and best practice. It’s founding board is made from technology providers and telecommunication companies including BT,

Vodafone, Imagination Technologies and Pen Best Partners.

3.5 Mirai Malware:

In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites. The Mirai Botnet had infected roughly 65,000 IoT devices within the first 20 hours[7]. Eventually the infections increased to 200,000 to 300,000 infections. Brazil, Columbia and Vietnam made up of 41.5% of the infections. The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers. Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik. In May 2017, Junade Ali, a Computer Scientist at Cloudflare noted that native DDoS weaknesses exist in IoT devices due to a poor implementation of the publish subscribe pattern. These sorts of attacks have caused security experts to view IoT as a real threat to Internet services.

3.6 Security Measures:

Figure 3.2: Security Measures

While security is a concern there are many things being done to protect device. Device Data is following cryptographic standards and encryption is being used in end-to-end scenarios. The overall understanding of Iot is essential for basic user security. Keeping up with current antivirus software and strengthening updates will help mitigate cyber attacks. In 2017, Mozilla launched the Project Things, which allows to route Iot devices through a safe Web of Things gateway[8].

IV. ATTACKS ON IOT.

4.1 Introduction:

Internet of things (IoT) is a group of interconnected devices and people in which devices can communicate with each other without human involvement. But these devices are greatly exposed to hackers, malwares and other kinds of cyber-attacks.

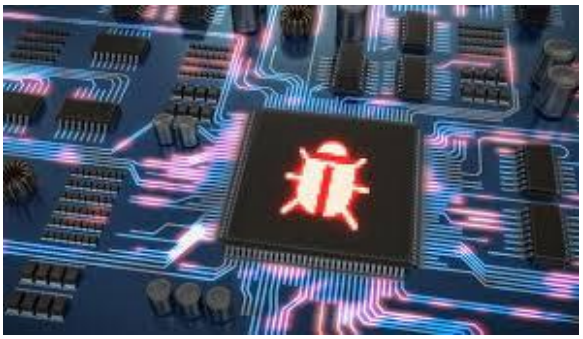

Figure 4.1: Representation of IoT Attacks

4.2 Rapid Increase in IoT Attacks:

The Internet of Things (IoT) continues to grow as a big target for cybercriminals to exploit, according to a new threat report from security firm Symantec. According to this report the number of IoT attacks increased from about **6,000 in 2016 to 50,000 in 2017—a 600% rise in just one year**[9].

The majority of IoT attacks in 2017 (**21%)** originated from **China**, the report found, followed by the **US (11%), Brazil (7%), and Russia (6%)**[10]. More than half of the attempted attacks against IoT devices targeted the Telnet service.

Cybercriminals are also increasingly turning to cryptocurrency mining. Detection of **cryptocurrency miners** increased **8,500% in 2017**[11] alone. Often, these attackers install miners on sufferers' computers or IoT devices without their knowledge.

4.3 How do such Attacks happen?

The DDoS-attackers know the **default passwords** for many IoT devices and used them to get in. It's a bit like leaving your house keys under a flowerpot for anyone to find. Anyone putting an IoT router, camera, TV or even refrigerator online without first changing the default password is enabling attacks of this type. Recent ESET research suggests at least **15% of home routers** are unsecured – that's an estimated **105 million potentially rogue routers**[12].

And while threats are increasing, the problem is made worse by the fact that many consumers and businesses continue to use **older operating systems**. On Android in particular, only **20% of devices**[13] were running the newest major version.

4.4 Some big Attacks of IoT:

4.4.1 The Miraj Botnet Attack:

In **October of 2016**, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including **Twitter, the Guardian, Netflix, Reddit, and CNN**[14].

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for exposed IoT devices and then use known **default usernames and passwords to log in**, infecting them with malware. These devices were things like digital cameras and DVR players.

According to PC Magazine, these are four straightforward IoT security lessons that businesses can take from the incident:

- "Devices that cannot have their software, passwords, or firmware updated should never be implemented.

- Changing the default username and password should be mandatory for the installation of any device on the Internet.
- Passwords for IoT devices should be unique per device, especially when they are connected to the Internet.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities."

The Mirai Botnet had infected roughly **65,000 IoT devices within the first 20 hours**. Eventually the infections increased to **200,000 to 300,000 infections**. Brazil, Columbia and Vietnam made up of **41.5% of the infections**[15]. The Mirai Botnet had singled out specific IoT devices that consisted of DVRs, IP cameras, routers and printers. Top vendors that contained the most infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik. In May 2017, Junade Ali, a Computer Scientist at Cloudflare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the publish subscribe pattern.

4.4.2 The Hackable Cardiac Devices from St. Jude:

Recently, CNN wrote, "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could **deplete the battery or administer incorrect pacing or shocks**, the FDA said.

The devices, like pacemakers and defibrillators, are used to monitor and control patients' heart functions and prevent heart attacks."

The article continued to say, "The vulnerability occurred in the transmitter that reads the device's data and remotely shares it with physicians. The FDA said hackers could control a device by accessing its transmitter."[16]

4.4.3 The TRENDnet Webcam Hack:

Figure 4.2: TRENDnet Webcam Hack

TechNewsWorld reports, "TRENDnet marketed its SecurView cameras for various uses ranging from home security to baby monitoring and claimed they were secure, the FTC said. However, they had faulty software that let anyone who obtained a camera's **IP address** look through it — and sometimes listen as well.

Further, from at least April 2010 [until about January 2012], TRENDnet transmitted user login credentials in clear, readable text over the Internet, and its mobile apps for the cameras stored consumers' login information in clear, readable text on their mobile devices, the FTC said.

It is basic security practice to secure IP addresses against hacking and to encrypt login identifications or at least **password-protect** them, and TRENDnet's failure to do so was surprising."[17]

4.4.3 Types of Attacks:

4.4.3.1 Distributed denial-of-service attack (DDoS attack):

A DoS attack can be done in a several ways. The basic types of DoS attack include:

- Flooding the network to prevent legitimate network traffic
- Disrupting the connections between two machines, thus preventing access to a service
- Preventing a particular individual from accessing a service.
- Disrupting a service to a specific system or individual
- Disrupting the state of information, such resetting of TCP sessions

4.4.3.2 Eavesdropping Attack:

5 An **eavesdropping** attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

4.4.3.3 Clickjacking:

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. Clickjacking is an instance of the confused deputy problem, a term used to describe when a computer is innocently fooled into misusing its authority.

4.4.3.4 Phishing:

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. The word, phishing, is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim.

4.4.3.5 Spoofing:

Spoofing is a malicious practice employed by cyber scammers and hackers to deceive systems, individuals, and organizations into perceiving something to be what it is not. Communication is initiated by the spoofer to the victim or system from an unknown source but disguised to present itself as an authentic and safe sender. If you have ever received an email from a seemingly familiar source asking you to update your profile details because some funny system upgrade was necessary, then you have experienced spoofing.

V. IOT HEALTH

When it comes to healthcare the IoT devices, can refer to a wide variety of devices such as heart monitoring implants, infusion pumps that are used in hospitals to deliver a pre-programmed level of fluids into a patient. There are also millions of other devices like pacemakers, insulin pumps, and cochlear implants. Some of these devices only send information via a wireless connection like a pace maker, while others can send and receive information. There are also devices know as wearable, like the Apple watch or the Fitbit, that can track vital information including your daily activity information, including the number of steps taken or calories burned. This data is synced with the watch or another device for data analysis and keep a history.

Figure 5.1 Medical IoT devices

When it comes to healthcare the IoT devices, can refer to a wide variety of devices such as heart monitoring implants, infusion pumps that are used in hospitals to deliver a pre-programmed level of fluids into a patient. There are also millions of other devices like pacemakers, insulin pumps, and cochlear implants. Some of these devices only send information via a wireless connection like a pace maker, while others can send and receive information. There are also devices know as wearable, like the Apple watch or the Fitbit, that can track vital information including your daily activity information, including the number of steps taken or calories burned. This data is synced with the watch or another device for data analysis and keep a history.

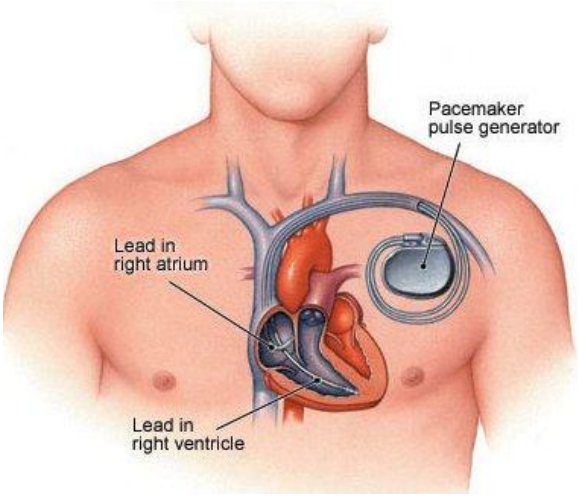

Figure5. 1 Pacemaker

Poor cybersecurity in IoT medical devices potentially poses risks to both the health of patients as well as to the organization that is using these IoT devices.

It is possible that hackers could tamper with medical devices to harm individuals, but we haven't seen anything like that yet. Devices are usually hacked so attackers can get into larger medical systems and steal protected health information. This type of hacking is usually called "medjacking". The following are a few cases of medjacking in three different hospitals.

In the first case, a blood gas analyzer infected with two different types of malware was used to steal passwords for other hospital systems, and confidential data was being sent to computers in Eastern Europe. At another hospital, the radiology department's image storage system was used to gain access to the main network, sensitive data was retrieved and sent to a location in

China. In the third case, hackers used the vulnerability in a drug pump to gain access to the hospital network.

Figure 5.3 Insulin Pump

Insulin pumps are medical devices that patients attach to their bodies that injects insulin through catheters. The Animas OneTouch Ping, was launched in 2008, is sold with a wireless remote control that patients can use to order the pump to deliver a dose of insulin, which is typically worn under clothing and can be awkward to reach. Johnson & Johnson recently informed patients that it has learned of a security vulnerability in one of its insulin pumps that a hacker could exploit to overdose diabetic patients with insulin. This system is vulnerable because communications are not encrypted, to prevent hackers from accessing the device.

VI. Conclusions

The pervasiveness of embedded processing is already happening everywhere around us. At home, appliances as mundane as your basic toaster now come with an embedded MCU that not only sets the darkness of the piece of toast to your preference, but also adds functional safety to the device. Your refrigerator has started talking to you and keeping track of what you put in it. There are energy-aware HVAC systems that can now generate a report on the activity in your house and recommend ways to reduce your energy consumption. The electrification of vehicles has already started happening, and in just a few years from now, each car will contain >50 percent more electronics than it did just five years ago.
Connecting those smart devices (nodes) to the web has also started happening, although at a slower rate. The pieces of the technology puzzle are coming together to accommodate the Internet of Things sooner than most people expect. Just as the Internet phenomenon happened not so long ago and caught like a wildfire, the Internet of Things will touch every aspect of our lives in less than a decade.

VII. References.

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] 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.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] 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.

[8] T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and 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] T. Jamal, 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.

[18] 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.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: LivingExamples, Challenges, Advantages”, Tech. Rep. SITI-TR- 11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP- Tele Workshop, Porto, Portugal, Dec. 2009.

[25] 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.

[26] T. Jamal, and 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.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE- SW-13-05, 2013.

[28] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.

[29] Zeeshan Haider, Kiramat Ullah and T. Jamal, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.