Security Threats, Attacks & Challenges to Internet of Medical Things Operating Systems

Mudasir Mahmood [1]*, Muhammad Ijaz Khan[1]

[1]*Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan 29050*
*Corresponding Author: mudasir@gu.edu.pk

Abstract: *The challenge of ensuring robust security and privacy (S&P) is growing as more devices are connected to the Internet of things. The S&P in the medical industry presents a severe problem that is only going to get worse because to the widespread usage of medical things. The (S&P) of the Internet of medical things (IoMT) is a challenge because of the importance and sensitivity of the data in the healthcare industry. Patients' privacy will be at stake, and their lives could be at risk, if IoMT lacks sufficient S&P. IoMT serves both machines and humans by creating a connection between them. It is expected that billions of IoMT medical things would cover the whole world by 2025.In healthcare systems, as the sensitive and crucial data is unstructured and noisy, it needs extra power to be computed, so that better analysis is done and reliable results are achieved. But, IoMT devices use less power to compute, low memory & battery life and limited resources to achieve more efficient and effective results. The data is collected and processed for making critical decisions which is the main target of cybercriminals. In the current research, this work is proposed to cope with all these challenges including Security threats & attacks on IoMT. In this study, we will discuss the most important security threats, security attacks and security challenges that IoMT operating Systems may encounter through Routing Protocol for Low-Power and Lossy Networks "RPL" and 6LoWPAN (IPv6 over low-power WPAN) protocols and possible solutions related to IoMT security challenges. To improve the security issues of the internet of medical things, this study will be beneficial for the researchers who would be willing to improve existing models as well as for those who want to develop new security models for IoMT.*

Keywords: IMOT, Low Power Wireless Personal Area Networks, Malware, Ransom ware, Spoofing, Replay Attack

1. Introduction:

IoMT is based on IoT for monitoring healthcare-related important and relevant signs through electrocardiography, Heart rate, BP, Body Temperature, Pulse Rate, Oxygen Saturation, Blood Glucose Testing, Cholesterol Testing, Infections, and Pregnancy testing it is primarily responsible for providing quality life to patients without their need to be hospitalized. It ensures the care of patients inside and outside the hospital environment. (See Figure-1)

Figure 1: Internet of Medical Things

The network is the key component of IoMT having all IoMT-enabled devices which continuously oversee patients' health digitally e .g they can access their health status simply using a mobile phone or radio-frequency identification "RFID". These devices of IoMT include smart watches or smart shoes and also ECG sensors, airflow sensors etc.

Cybercriminals have left no stone unturned to disrupt the security in healthcare e. g. In 2021, Cybercriminals heavily targeted the institutional servers of 1 CF Witting Hospital in Bucharest by ransomware attack. Similarly, the same attacks happened in 2019 at four other hospitals in Romania. In Italy, similar attacks were recorded that disrupted the vaccination schedule of several tertiary care hospitals in 2021.

Therefore, we will discuss the most important security threats, security attacks and security challenges that IoMT operating

Systems may encounter through Routing Protocol for Low-Power and Lossy Networks "RPL" and 6LoWPAN (IPv6 over low-power WPAN) protocols and possible solutions related to IoMT security challenges.

IoMT environment consists of wireless sensors and applications and uses less power of computation with limited resources and this way overrules the regular operating system. For resource constraints, IoMT needs a lightweight operating system. There are many well-equipped operating systems with key communication and networking protocols, and security features with many implementation flaws, some protocol flaws make the network defenseless to differentiate the attacks like Black-hole attacks, fragmentation attacks & denial of service attacks. The section area describes the security issues related to RPL and 6LoWPAN.

Selection Area:

Section No.1 Describes the Introduction, Section No. 2 Contains the Literature Review, Section No. 3 Deals with the Different Environments of the Operating System for the Internet of Medical Things, Section No. 4 represents RPL, many kinds of attacks in RPL and solution recommended for improving the Security Issues, Section No. 5 Describes 6LoWPAN and Security Issues related to 6LoWPAN.Section No.6 Describes SDN-Based Architecture for IoMT, and Section No. 7 is based on the Conclusion of this paper.

2. Literature Review:

Huang, X., & Nazir, S. (2020) [1] Internet of Medical thing plays the most important role in Medical Industry .The Communication between the different devices e. g smart sensors, wearables devices, handheld and many other devices are connected in the network is possible because of the successful Internet of things. For efficient and smooth function of healthcare, the security of different devices connected is very compulsory. An effective and strong security system is the need of the hour to cope with the different attacks, threats and challenges. There are many security issues for IoMT that are directly proportional to the heath of patients. Farahat, I. S. et al.2018. [2]. Through the use of data encryption and authentication, a wireless system for transferring medical data must be safe. By encrypting data using a rotated key before it is transferred over the network, a new data encryption scheme is introduced. The doctor uses his access information and digital signature to restore the encrypted data. Alsubaei, et al.2019 [3]. Presented tool for IoMT Solutions that provides security recommendations, An IoMT scenario with details on the architecture, solution, and stakeholder types serves as the tool's input. The program compiles a list of security concerns based on the scenario and suggests security ways to solve them. It also suggests a set of security characteristics that can be used to gauge the degree of security offered by the measures. Based on their security goals, adopters of IoMT can use this study to help them choose and enforce security in IoMT systems. System administrators are occasionally the only ones in charge of making security-related decisions, but this study informs other stakeholders about security in IoMT, enticing them to participate more. Additionally, this technology encourages responsibility and openness among IoMT stakeholders and aids in raising security awareness. Solution providers, on the other side, can use this technology to evaluate and confirm the security of their products. Additionally, it facilitates their transparent competition with other providers. Elhoseny M et al. [4] discussed some security requirements i-e authentication, integrity, and confidentiality Atamli A et al. [5] Introduced privacy & security threats in the architecture of the Internet of Things through a systematic approach for analyzing the threats at various levels of the architecture. The suggested cloud based health management system by Rathnayake, R. M. P. H. K et al. 2018 [6] increase data accessibility, storage requirements, and processing power. Three encryption methods Advanced Data Encryption, Attribute-Based Encryption, and Proven Data Possession are trusted with security in the cloud-mobile architecture. Turabieh H et al. [7] inquired about the missing data for medical data sets. Tree-Based Models (TBMs) were applied for recovering missing data based on the surrogate approach (SUR). They proved that putting the missing data will raise the performance of medical applications.

A thorough hierarchical model for trusting of things in the IoT is provided by Hashemi, S. Y. et al. in 2019 [8]. This has a multifaceted understanding of trust. We classify the collection of metrics and necessary countermeasures under the computation of the trust level. When used in a mobile context and while being subjected to significant routing attacks, DCTM-RPL performs better than the traditional RPL protocol. When it comes to the identification and isolation of assaults, DCTM-RPL outperforms the normal RPL protocol. Yang Z et al. [9] enfolded the major security and privacy issues in IoT. They addressed a holistic cyber security concept that was required to present different security and privacy threats at all abstraction levels e. g security in platform, engineering, management, identity, and industrial rights management. Alabady, S. A. et al 2020 [10] gives the foundational components of a secure networking system, such as a firewall, router, AAA server, and VLAN technology. In the IoT Era, it introduces a revolutionary security approach to protect the network from risks and attacks from both inside and outside the system.

3. Different Environments of Operating System for the Internet of Medical Things:

IoMT and different objects interact through software i-e "WSN" (wireless sensor network) & "RFID" (Radio Frequency Identification) technologies. It is the Operating System which makes this interaction possible. The Internet of Medical Things performs easier because of the flexible features of the Operating System. IoMT Operating System consists of a few kilobytes of memory and operator on low power consumption. Operating Systems are not built to compromise features like security, networking and communication like in traditional Operating Systems TOS e. g Fedora, SUSE, Red hat and Windows. Operating System for IoMT deals with several different security features to avoid compromise on usability and stability. Just because of security issues, the operating system for IoMT is different from the regular operating system. The efficient platform for the exchange of information in the IoMT environment among different devices uses very limited resources. However, the IoMT environment and Operating

Systems are vulnerable to third-party attacks. Encryption, intrusion detection [11] and data hiding techniques [12] have dominant importance in IoMT infrastructure.

3.1. **Contiki:** (See Figure-2)

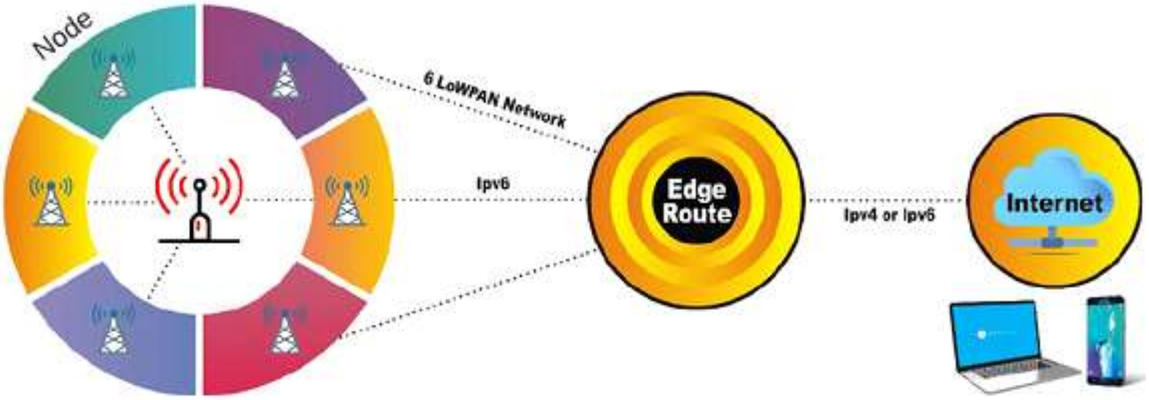

Figure-2: Communication Component in Contiki Operating System

It was developed by Adam Dunkels and revised by different organizations like Cisco, SAP, Atmel, Sensinod etc. [13]. It supports different microcontroller devices such as Atmel ARM, Atmel AVR, STM32 w, TIMSP430 /CC2430 /CC2538 /CC2630 /CC2650, LPC2103, Free scale MC13224, Microchip dsPIC, Microchip PIC32. Contiki is also open source under Berkeley Source Distribution-licensed “BSD” license, it has features of Contiki nodes simulation and supports three types of nodes:

1. Emulated
2. Cooja
3. Javanodes

Supports CoAP, 6LoWPAN and RPL networking protocols Contiki is secure with the implementation of DTLS/TLS and Contiki Sec [14].

3.2. **Tiny OS:** (See Figure-3)

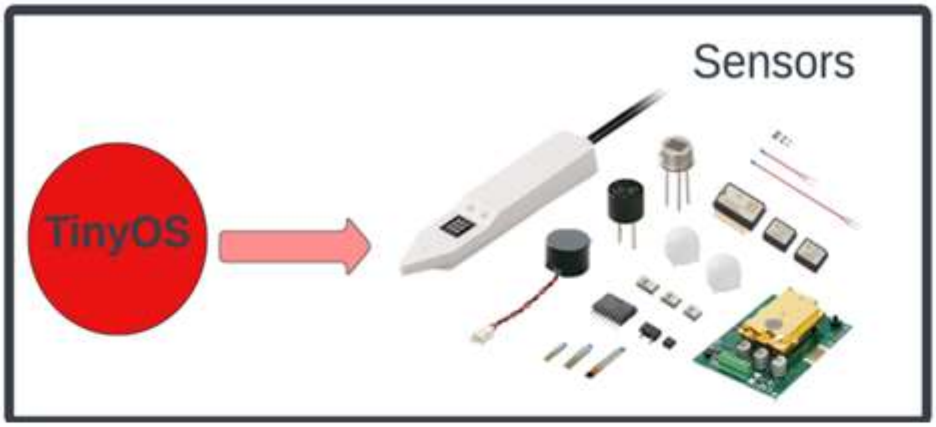

Figure-3: Tiny Operating System

TinyOS is an open source, “BSD” Berkeley Source Distribution-licensed operating system designed for low-power wireless devices akin to those used in smart meters, sensor networks, smart buildings, ubiquitous computing, personal area networks and others. ”SDK” software development kit for Tiny OS is a combination of TinyDT, TinyOS Eclipse Plugin – YETI 2 and Eclipse Editor plugin. The tinyOS supports TDMA base Routing, Geographical Routing, Multi-Path Routing, Broadcast based Routing & Reliability based Routing. TinySec made TinyOS architecture Secure [15].

3.3. Mbed: (See Figure-4)

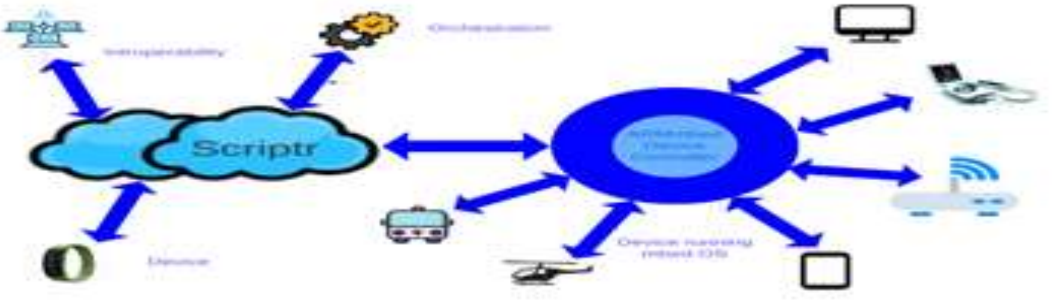

Figure-4: ARM mbed Operating System

Mbed Operating Systems are developed by ARM with the alliance of technological partners.

Mbed provides a free open-source IoMT Operating System with Connectivity, Storage, Device Management, Security, and Machine Learning. Mbed is 32 bits ARM Cortex M Microcontroller. This operating system is an open source under Apache License 2.0 “SDK” Software Development Kit for Mbed offers a framework for developing different firmware for IoMT devices.

The main libraries consist of the below-mentioned components.

1. Build tools
2. Microcontroller peripheral drivers
3. Debug Scripts
4. Networking
5. Test scripts
6. RTOS and runtime environment

By using Mbed Online IDEs “Integrated Development Environments” Mbed applications are developed. Web browsers are used to write the code ArmCC: ARM C/C++is complier.

Mbed supports following technologies:

1. Bluetooth
2. Cellular
3. 6LoWPAN
4. Wi-fi
5. Zigbee IP /LAN

Mbed is use to provide (IPv4 and IPv6) “E2E” End to End security through “DTLS” Datagram Transport Layer Security & “TLS” Transport Layer Security.

“DTLS” uses “UDP” user datagram protocol and TLS uses “TCP” Transmission control protocol. Nonetheless, a lightweight protocol “OMA” Open Mobile Alliance is used for management in this environment.

3.4. RIOT (Radical Image Optimization Tool): (See Figure-5)

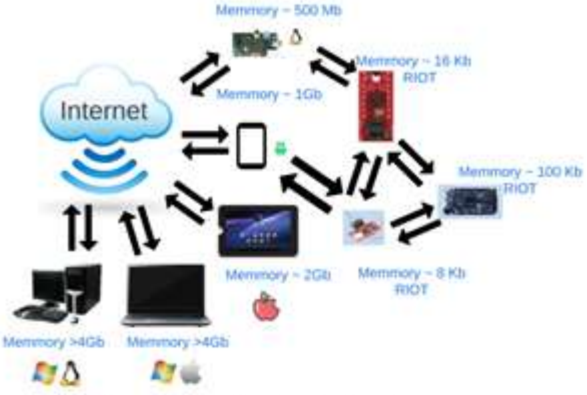

Figure 5: Riot Architecture

Riot Architecture was developed in 2008, as an Operating System for wireless sensor nodes. Later, it was applied to IoT and IoMT systems. It is compatible with AVR at mega, TI MSP430 and ARM Cortex-M3/ M4 this is also open source under LGPL V 2.1 licensed and develops in C++ / C. “SDK” Software Development Kit for RIOT OS are GDB, Valgrind and GCC.

Following communication and networking protocols supported by RIOT are as under:

1. IPv6
2. 6LoWPAN
3. RPL
4. CoAP
5. UDP
6. TCP
7. CBOR
8. CCN-lite
9. Open WSN
10. UBJSON

The Operating System has properly been developed and maintained and no new programming environments are there. C or C++ can be used directly with already available tools like GCC, GDB and others. (See Table-1)

Table 1: Comparative Analysis of Operating Systems for IoMT Devices [16]

OS Properties	Contiki	TinyOS	Mbed	RIOT
Rom	Less than 30Kb	Less than 4Kb	Less than 37Kb	5Kb
Ram	Less than 2Kb	Less than 1Kb	Less than 8Kb	1.5Kb
Kernel	Modular	Monolithic	Layered	Microkernel
Real-Point Sustain	Partial	Nope	Definitely	Yes
Dev. Terminology	C(partial)	NesC	C,C++	C,C++
Scheduling	Preemptive	Preemptive FIFO,EDF	Priority –Based	Priority -Based,Tickles
Efficient Energy	Yes	Yes	Yes	Yes
Event Driven	Yes	Yes	-	-
Reliability	Yes	Yes	-	Yes
Programming Model	Proto-Threads	Multi-Threading	Event-Driven	Multi-Threading
Open Source	Positively	Positively	Positively	Positively

4. RPL (Routing protocol for low-power and lossy networks): (See Figure-6)

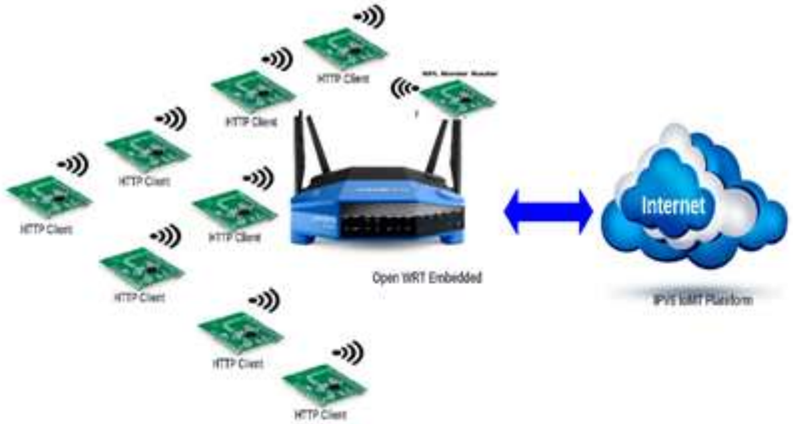

Figure-6: IoMT Network: IEEE 802.15.4, IPV6, and RPL

RPL stands for Routing Protocol for Low Power and lossy network. It communicates from multipoint to point, point to multi-point and also point to point. RPL consumes low power and is usually prone to packet loss while acting as a routing protocol for wireless networks. This protocol is proposed for a wide range of network environments such as hospital automation, urban automation and smart grid.

RPL is known as a proactive protocol which is dependent on distance vectors and functions on IEEE 802.15. 4, its topology contains 1 root known as a sink node. RPL is used to form a Destination Oriented Directed. A cyclic Graph tree structure, Topology formations start with the root node broad casting "DODAG information objects" (Destination Oriented Directed Acyclic Graph). The rank value is calculated PRV (parent rank value) and some other parameters when any node receives a DIO message. Rank Value "RV" also depended on the distance between the root node and the Parent node. The network owner decides the parameter calculations.

Network devices are mostly resource-constrained, IoMT devices are Hospital appliances, smart meters and sensor nodes etc. thousands of devices are available which can connect to IoMT. 6LoWPAN allows controlled devices to communicate with the IPv6 network. 6LoWPAN is a compression protocol that can easily attack. IoMT devices are limited in resources, so a new protocol is designed for network routing called RPL. RPL doesn't have routing like traditional routing protocol. Here we have to discuss different kinds of attacks [17].

4.1. **Smurf Attack:** (See Figure-7)

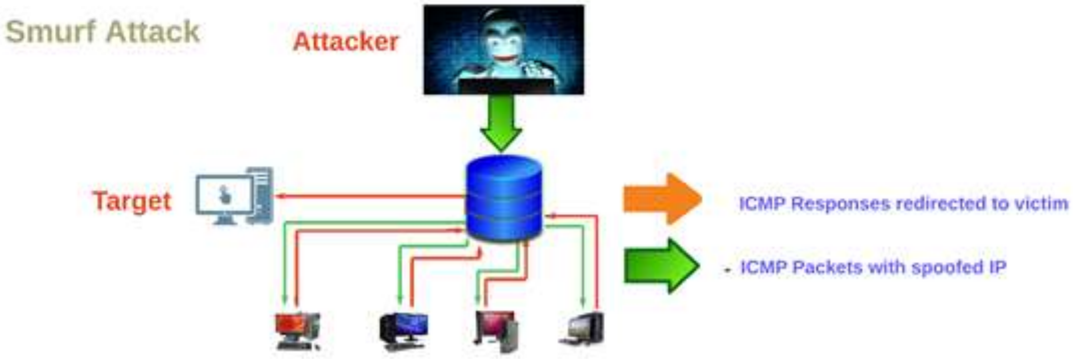
Smurf Attack
Attacker
Target
ICMP Responses redirected to victim
ICMP Packets with spoofed IP

Figure 7: Smurf Attack

Smurf Attacks area kind of DDOS (distributed denial-of-service) attacks which lie on the network layer. It causes DoS in the network to make the network incurable. We have to understand the basics of Internet Control Message Protocol "ICMP" to unveil the areas open to attack.

ICMP is a network layer protocol which is used by network devices. These devices diagnose network communication issues. This controls network nodes and the network administrator can be able to change the information of ICMP. The status of IoMT nodes is also monitored by ICMP. If it returns ping then it means they are operating [18].

"Configure OS in the PaaS layer and Router in the IaaS layer".

4.2. **Black hole Attack:** (See Figure-8)

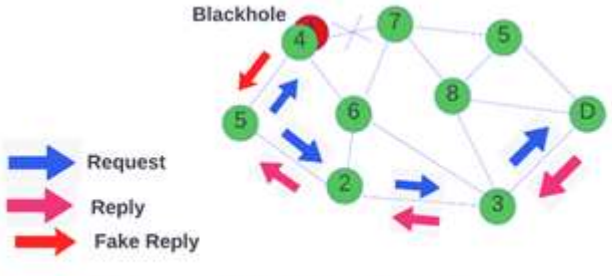

Figure- 8: Black hole Attack

A black hole attack is a form of a denial-of-service attack, in computer networks, wherein a router functions to relay packets, not to discard them. It generally happens out ofa router which becomes compromised because of multiple causations. It is also called a packet drop attack Heterogeneous Communication Protocols are abbreviated as "HCP". These protocols are defenseless to different types of attacks like network sniffing, modification, Dos etc. some types of attacks are documented in [19]. This kind of attack acts, whenever a conciliator gets and re-programs nodes or a set of nodes in the network, so that block/drop the packets may be blocked and creates false messages towards the base station in a wireless sensor network. Black hole attack work on the network layer and target RPL implementation of the Contiki operating system [20], Black hole attacks can easily be hidden and the targeted network can pretend to be the health network. Only Contiki OS-based devices are defenseless to this type of attack. The good defense against black hole attacks in RTL protocol is "To implement RIOTOS, TinyOS which are not defenseless to this type of attack".

4.3. Wormhole attack detection: (See Figure-9)

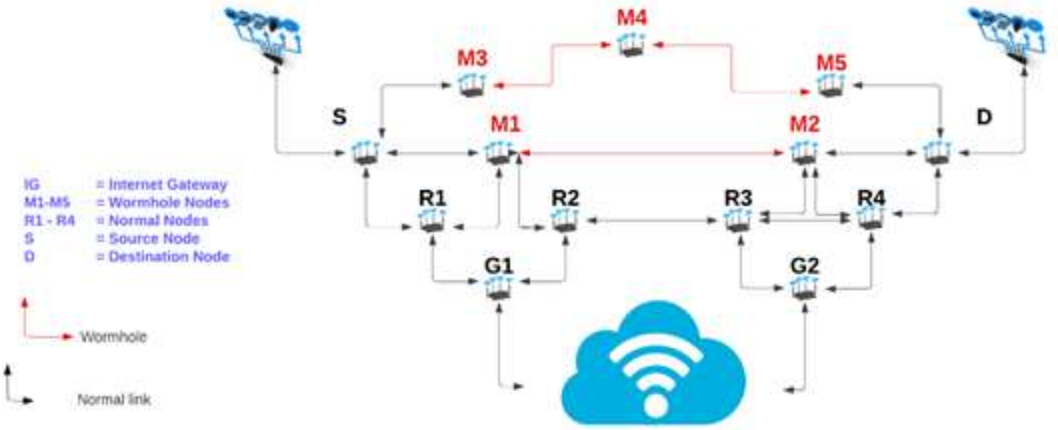

Figure-9: Wormhole attack detection

In this type of attack, packets or bits are recorded at a location/place in the network, and packets or bits ate recorded at one location in the network. Then, the attacker forces them very selectively to some other location& re-transmits the same into the network. Herein [21]. The author describes how to detect wormhole attacks in a wireless network. This type of attack causes great damage to nodes and networks. To prevent form such type of attack we use a special timer WAPT, by using timer nodes which do not require synchronization of the already present clock when the node ends an RREQ packet. This will travel between the nodes back & forth. If WAPT is large then it is very difficult to detect. For sensor nodes WAPT is:

WAPT = 2 * Transmission Range /Propagation Speed of packet

Monitors neighbor nodes for hidden attack detection. When wormhole nodes are legitimate nodes then it is very difficult to detect by only monitoring mechanisms. In wormhole attacks, while keeping the same hop count, the delay is undoubtedly greater than the normal path. That is why these nodes can be ignored if such long delays do not opt. "In adhoc network wormhole detection is still big challenging."

4.4. The Sybil Attack: (See Figure-10)

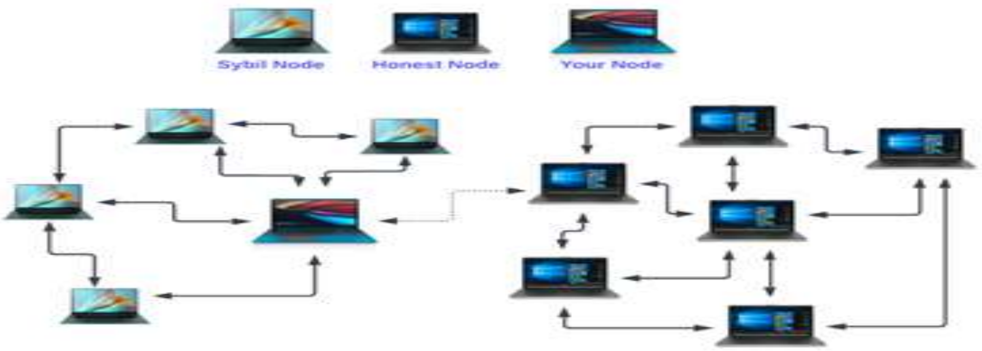

Figure-10: Sybil Attack

A Sybil attack is when a single malicious identity can show multiple identities and gain control of the network. This kind of attack undermines the authority or power in a reputable system that is outrun by achieving the majority of influence in the network. RPL protocol is not defensive against Sybil attacks. In the Sybil attack, the attacker is presented as a lot of people acting at the same time and this becomes the greatest issue when connected to a P2P network. These nodes cause a consuming large amount of resources. In [22] author explains the way of preventing over WSNs networks from Sybil attack; which is detected through a propagation model. This is the technique where "The received signal power from a sending node is matched with its claimed position. By using this method, received signal power can be used to calculate the position of the node" (See Figure-11)

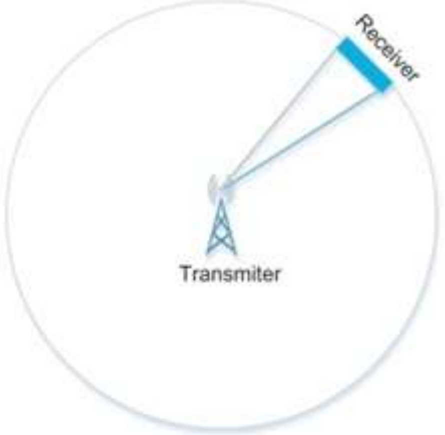

Figure-11: Propagation Model

4.5. Clone ID Attack: (See Figure-12)

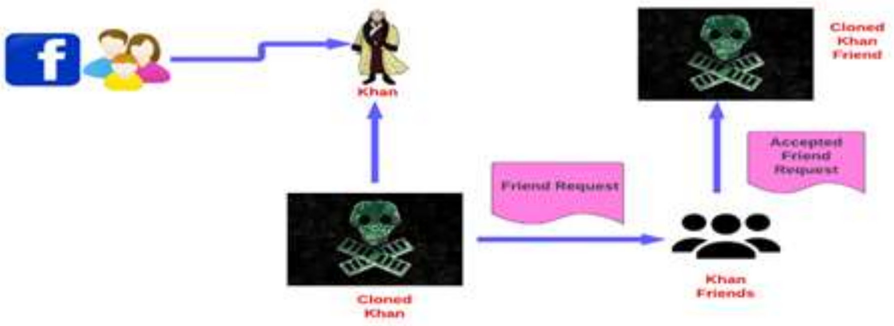

Figure 12: Clone ID Attack

This kind of the attack is found in RPL protocol where the node's ID in the network is cloned by the attacker. A Clone ID detection system is constructed for IoMT.

In RPL Network Clone ID attacks are possible [23]. In the case of geographical location nodes identify store in 6BR, by using this "we can recognize clone or original node". In these types of attacks, the attacker nodes clone the identity of another. These attacks are minimized with "Tracking no of every identity".

4.6. Hello Flooding Attack: (See Figure-13)

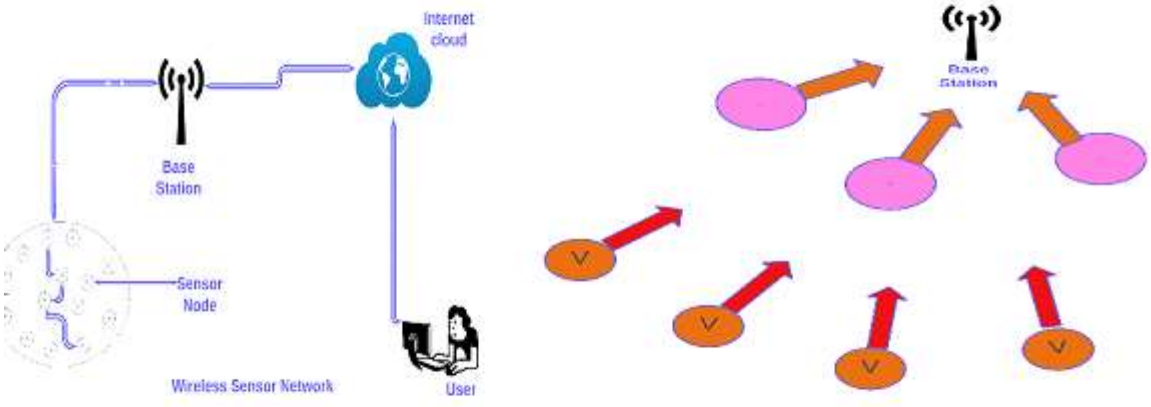

Figure 13: Hello Flooding Attack

The main attack in the network layer is Hello Flooding Attack. The node, which broadcasts a Hello packet using very high power, causes this kind of attack. Very high power is used to make it easy for a lot of very far nodes to opt for it as a parent node.

This type of attack can be avoided by using the link layer metric in the default route [24]. This kind of attack is unable to survive long enough in RPL's Local and Global repair mechanism. If multiple attackers combine then RPL's Local & Global repair cannot remove it. "Another solution of this attack is to use geographical distance".

5. 6LOWPAN and Security Issues: (See Figure-14)

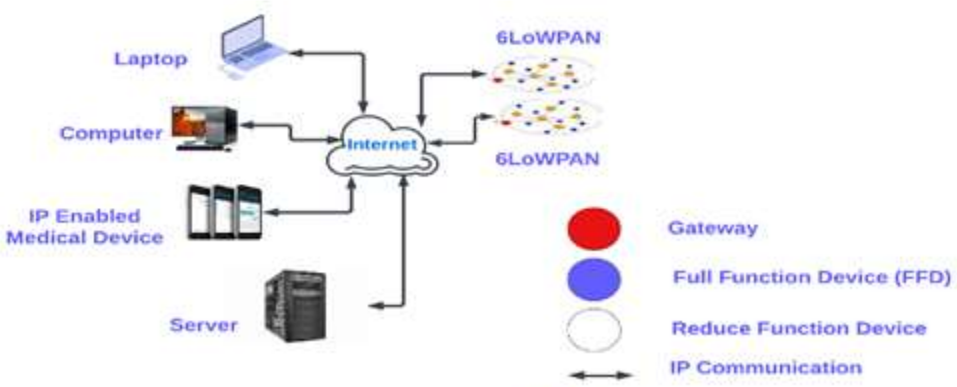

Figure-14: 6LOWPAN

It is a mesh network that is robust, scalable, and can heal on its own. It delivers low-cost and secure communication in IoMT devices. It is directly routed to the cloud platform and it uses the IPv6 protocol. It offers one-to-many and many-to-one routing.
6LoWPAN infrastructure is IP-Based and WSNs specify IPv6 packet routing in networks like IEEE 802.15.4. 6LoWPAN defines resemblance with data gram and fragmentation due to the link layer it has limited pay load size. 6LoWPAN connect to the internet with a 6LoWPAN Border Router that performs fragmentation, decompression and compression of IPv6 datagrams.

Attacks on 6LoWPAN are discussed as under:

5.1. Fragmentation Attack: (See Figure-15)

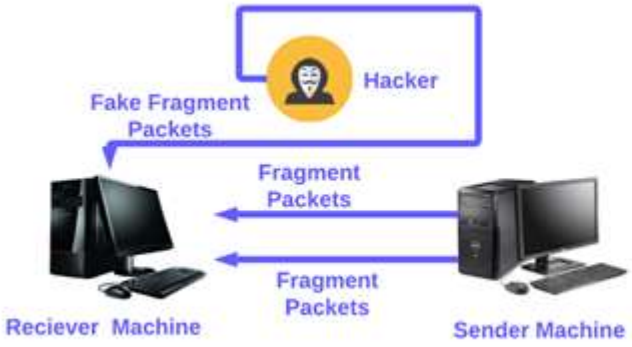

Figure-15: Fragmentation Attack

Fragmentation attack is also called teardrop attacks. This kind of attack aims at TCP/IP reassembly mechanisms and prevents them from coming close to the fragmented data packets. Resultantly, the data packets overlap& overwhelm very fast the server of the victim and leading them to be failed.

We have connected devices with an IPv6 network with 6LoWPAN protocol. Fragmentation is done in IPv6 because the minimum size of IPv6 MTU is 1280 bytes whereas nodes in IoMT or sensors have maximum 127 bytes MTU.

6LoWPAN does not support authentication is also a reason for fragmentation attacks. As there is no authentication in 6LoWPAN, the attack can put its fragment in the fragmentation chain. The chain is not spoofed to check the fragment hence the author proposes two mechanisms [25].
"First one is the split buffer approach that is to promote the competition between the reassembly buffer resource and the original sender and the second one is the content chaining, cryptographic approach to verify the fragment is in the same packet or not".

5.2. Confidentiality Attack : (See Figure-16)

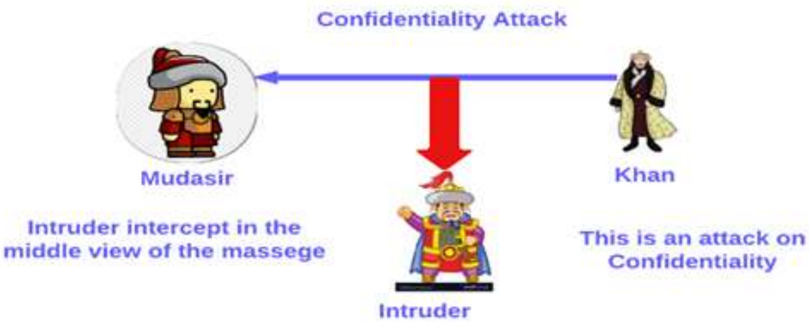
Confidentiality Attack
Mudasir
Khan
Intruder intercept in the middle view of the massege
This is an attack on Confidentiality
Intruder

Figure-16: Confidentiality Attack

Confidentiality ensures that the data is only readable by the proposed destination. 6LoWPAN gives IP-based sensors and traditional networks end-end secure communication.

6LoWPAN mitigate different attacks such as Man in the middle, spoofing, eavesdropping and other, by encryption. It supports both IP Sec's Authentication Header and encapsulating Security Payload. Crypto hardware is used for encrypting packets faster for 6LoWPAN with IEEE 802.15.4 [26]. The author examined MT6D "Moving Target IPv6 Defense" in 6LoWPAN [27]. In MT6D nodes change their addresses frequently and attackers are not able to attack the specific node or sensor. The main target of MT6D is to secure the network against the DoS and the Man in the Middle attacks. (See Figure-17)

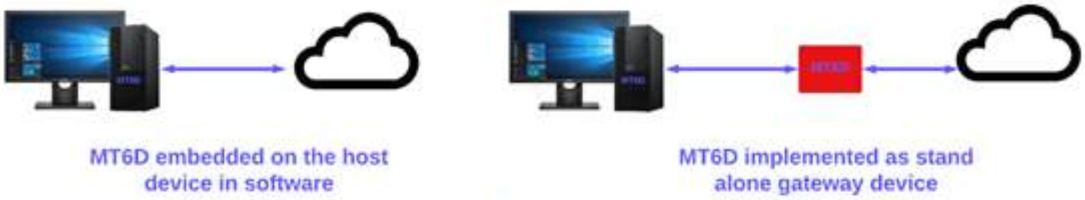
MT6D
MT6D embedded on the host device in software
MT6D
MT6D
MT6D implemented as stand alone gateway device

Figure-17: MT6D Diagram.

5.3. Authentication Attack : (See Figure-18)

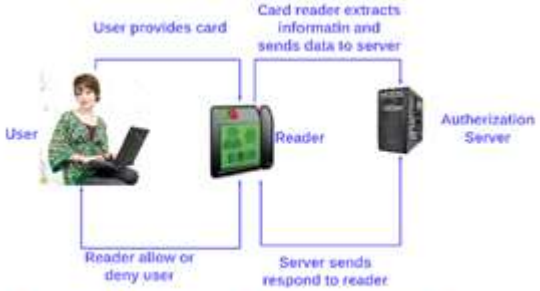
User provides card
Card reader extracts informatin and sends data to server
User
Reader
Autherization Server
Reader allow or deny user
Server sends respond to reader

Figure-18: Authentication Attack

Authentication is considered an important pillar of the Internet of Medical Things (IoMT). The identity of a device or a person is authenticated by security using a unique identification number. An intruder can easily get access and initiate attacks on IoMT if authentication is taken for granted.

When joining the IoMT 6LoWPAN cannot provide any authentication for nodes due to this reason any malicious node can join the network. In [28] the author describes the authentication mechanism for controlling nodes that have the access to the 6LoWPAN network. It is directly based on administrative approval that contains following four steps:

1. Authorized node list propagation
2. Data filtering
3. Node authorization
4. Node presence detection

A list of nodes with layer II addresses is saved in the border router, and the presence of nodes is verified with the help of these addresses. It also allows those nodes to connect with networks that are on the list. For the flow of data between nodes and data filtering this list is also used.

6. SDN-Based Architecture for IoMT : (See Figure-19)

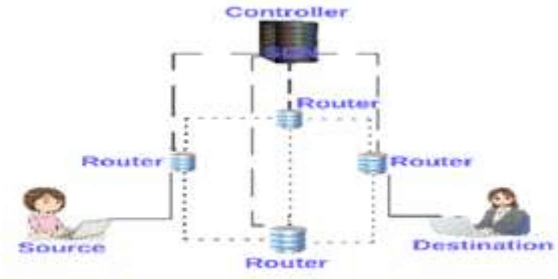

Figure-19: SDN Architecture

Software-Defined Networking (SDN) employs either software-based controllers or application programming interfaces (APIs) for communication with underlying hardware infrastructure as well as direct traffic on a network. Protocols and traditional equipment support high amounts of traffic, scalability and mobility.

The author proposed IoT architecture [29], here we will explain SDN architecture. In IoMT networks or sensor networks, every device is not compatible with SDN Controller or SDN embedded capability.

Let's we have two kinds of nodes, one is of that have enough resources and the second is a sensor or smart object that does not have enough resources. All traffic will be controlled by SDN in this domain. Here in this SDN domain, every domain has at least one SDN controller.

SDN does not only use for network management but also provides efficient security against both inside and outside attacks. SDN authenticate network devices to secure the network resources. Once the connection is established and secured between the controller and the switch then block all the ports that are directly connected to the user. We have to expend this process to each device, node connected with Open Flow "OF" and one of the nodes connected with domain controller [30].

7. Conclusion:

As per the above discussion, we have concluded that most of the IoMT operating systems are flexible and well organized, but there are many implementation problems and protocols, over networks, that are defenseless from different types of attacks. Hence many techniques are proposed against RPL and 6LOWPAN attacks. There are many types of attacks that have not been evaluated till now. Thus, it is a need of an hour to counter the weakness of RPL and 6LoWPAN. Sybil, Black Hole, Clone ID etc. and some other kinds of attacks that need IDS-based detection mechanisms. In the years to come, IoMT will grow more in to main stream technology and there will be standardization in IoMT operating systems and development environments.

References:

[1]. Huang, X. and Nazir, S. (2020) "Evaluating security of internet of medical things using the Analytic Network Process Method," *Security and Communication Networks*, 2020, pp. 1–14. Available at: https://doi.org/10.1155/2020/8829595.

[2]. Farahat, I.S. *et al.* (2018) "A secure real-time internet of medical smart things (IOMST)," *Computers & Electrical Engineering*, 72, pp. 455–467. Available at: https://doi.org/10.1016/j.compeleceng.2018.10.009.

[3]. Alsubaei, F., Abuhussein, A. and Shiva, S. (2019) "Ontology-based security recommendation for the Internet of Medical Things," *IEEE Access*, 7, pp. 48948–48960. Available at: https://doi.org/10.1109/access.2019.2910087.

[4]. Elhoseny, M. *et al.* (2018) "Secure Medical Data Transmission Model for IOT-based Healthcare Systems," *IEEE Access*, 6, pp. 20596–20608. Available at: https://doi.org/10.1109/access.2018.2817615.

[5]. Atamli, A.W. and Martin, A. (2014) "Threat-based security analysis for the internet of things," *2014 International Workshop on Secure Internet of Things* [Preprint]. Available at: https://doi.org/10.1109/siot.2014.10.

[6]. Rathnayake, R.M.P.H.K. *et al.* (2018) "Cloud enabled solution for privacy concerns in internet of medical things," *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)* [Preprint]. Available at: https://doi.org/10.1109/atnac.2018.8615361.

[7]. Turabieh, H., Abu Salem, A. and Abu-El-Rub, N. (2018) "Dynamic L-RNN recovery of missing data in IOMT applications," *Future Generation Computer Systems*, 89, pp. 575–583. Available at: https://doi.org/10.1016/j.future.2018.07.006.

[8]. Hashemi, S.Y. and Shams Aliee, F. (2018) "Dynamic and Comprehensive Trust Model for IOT and its integration into RPL," *The Journal of Supercomputing*, 75(7), pp. 3555–3584. Available at: https://doi.org/10.1007/s11227-018-2700-3.

[9]. Yang, Z. *et al.* (2020) "Faster authenticated key agreement with perfect forward secrecy for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, 16(10), pp. 6584–6596. Available at: https://doi.org/10.1109/tii.2019.2963328.

[10]. Alabady, S.A., Al-Turjman, F. and Din, S. (2018) "A novel security model for cooperative virtual networks in the IOT ERA," *International Journal of Parallel Programming*, 48(2), pp. 280–295. Available at: https://doi.org/10.1007/s10766-018-0580-z.

[11]. Ugendhar, A. *et al.* (2022) "A novel intelligent-based Intrusion Detection System approach using deep multilayer classification," *Mathematical Problems in Engineering*, 2022, pp. 1–10. Available at: https://doi.org/10.1155/2022/8030510.

[12]. Taleby Ahvanooey, M. *et al.* (2018) "A comparative analysis of information hiding techniques for copyright protection of text documents," *Security and Communication Networks*, 2018, pp. 1–22. Available at: https://doi.org/10.1155/2018/5325040.

[13]. "Kalnins, Rheinhold" (2011) *Benezit Dictionary of Artists* [Preprint]. Available at: https://doi.org/10.1093/benz/9780199773787.article.b00096883.

[14]. Wei, M. *et al.* (2022) "An intrusion detection mechanism for IPv6-based Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, 18(3), p. 155013292210779. Available at: https://doi.org/10.1177/15501329221077922.

[15]. Paramita, S. (2020) "IOT-based WBAN Health Monitoring System with security," *Internet of Things*, pp. 107–120. Available at: https://doi.org/10.1201/9781003032441-7.

[16]. Pongle, P. and Chavan, G. (2015) "A survey: Attacks on RPL and 6LoWPAN in IOT," *2015 International Conference on Pervasive Computing (ICPC)* [Preprint]. Available at: https://doi.org/10.1109/pervasive.2015.7087034.

[17]. Zeebaree, S.R., Jacksi, K.F. and Zebari, R.R. (2020) "Impact analysis of SYN flood DDOS attack on HAPROXY and NLB Cluster-Base web servers," *Indonesian Journal of Electrical Engineering and Computer Science*, 19(1), p. 505. Available at: https://doi.org/10.11591/ijeecs.v19.i1.pp505-512.

[18]. "Smart homes: Security challenges and privacy concerns" (2020) *International Journal of Computers*, 14. Available at: https://doi.org/10.46300/9108.2020.14.5.

[19]. D, S. (2021) "A data driven trust mechanism based on blockchain in IOT sensor networks for detection and mitigation of attacks," *March 2021*, 3(1), pp. 59–69. Available at: https://doi.org/10.36548/jtcsst.2021.1.006.

[20]. Gupta, C., Singh, L. and Tiwari, R. (2022) "Wormhole attack detection techniques in ad-hoc network: A systematic review," *Open Computer Science*, 12(1), pp. 260–288. Available at: https://doi.org/10.1515/comp-2022-0245.

[21]. Akshara Vemuri, S. and Krishna Chaitanya, G. (2022) "Insider attack detection and prevention using server authentication using Elgamal encryption," *2022 International Conference on Inventive Computation Technologies (ICICT)* [Preprint]. Available at: https://doi.org/10.1109/icict54344.2022.9850623.

[22]. Rajasekar, V.R. and Rajkumar, S. (2022) "A study on impact of Dis flooding attack on RPL-based 6LowPAN Network," *Microprocessors and Microsystems*, 94, p. 104675. Available at: https://doi.org/10.1016/j.micpro.2022.104675.

[23]. A. Almusaylim, Z., Jhanjhi, N.Z. and Alhumam, A. (2020) "Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP," *Sensors*, 20(21), p. 5997. Available at: https://doi.org/10.3390/s20215997.

[24]. Sheff, J.N. (2014) "Dilution at the patent and trademark office," *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.2410069.

[25]. Glissa, G. and Meddeb, A. (2019) "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, 82, pp. 100–112. Available at: https://doi.org/10.1016/j.adhoc.2018.01.013.

[26]. Finstad, R.K. (no date) "Implementation of Network Moving Target Defense in embedded systems." Available at: https://doi.org/10.31274/etd-20210114-44.

[27]. Berguiga, A. *et al.* (2021) "FPMIPv6-S: A new network-based Mobility Management Scheme for 6LoWPAN," *Internet of Things*, 13, p. 100045. Available at: https://doi.org/10.1016/j.iot.2019.02.005.

[28]. Aiello, M. (2022) "IOT architectures: From Data to Smart Systems," *Frontiers in the Internet of Things*, 1. Available at: https://doi.org/10.3389/friot.2022.959268.

[29]. Manguri, K.H. and Omer, S.M. (2022) "SDN for IOT environment: A survey and research challenges," *ITM Web of Conferences*, 42, p. 01005. Available at: https://doi.org/10.1051/itmconf/20224201005.

[30]. Andrade, R.O. *et al.* (2022) "Security Risk Analysis in IOT systems through factor identification over IOT devices," *Applied Sciences*, 12(6), p. 2976. Available at: https://doi.org/10.3390/app12062976.