# A Review of Different Types of Attacks in IoT's

[1]Er.Manveen Kaur
Research Scholar,
Department of Computer Science and Engineering,
Guru Kashi University, Talwadi Sabo,Bathinda,(PB).

[2]Er.Jashanpreet Kaur
Assistant Professor,
Department of Computer Science and Engineering,
Guru Kashi University, Talwadi Sabo,Bathinda,(PB).

***Abstract*****:** IoT, Internet of things, is the utility of internet for future and provides the ability of small networks to connect to the remote networks. Also, IoT platform provides the ability to share resources amongst each other to make cost-effective network. Because of this network to establish, no new infrastructure has to be built as existing infrastructure can be utilized. While sharing of the resources amongst remote computers by using the existing infrastructure imports various types of disadvantages of the existing system such as congestion and packet loss attacks by different types of attackers. Therefore, these problems must be addressed to have a successful IoT. Thus it is very important to review different types of attacks prevailing in the existing wireless networks. And also study different types of techniques to mitigate those attacks and improve the security standards.

**Keywords:** Internet of Things (IoT), Sybil, Energy harvesting, Attacks, Active Attacks, Passive Attacks, Security, Encryption Attacks, Networks, Wireless Network.

## I. INTRODUCTION

IoT is a vast platform or network which is connected to various embedded systems through Internet. It is a network of millions of private, public, academic, business, hospitals and government networks, from local to global in scope. IoT is a network which is used for development in the physical devices, vehicles, sensors ,mobiles, home devices etc which enable these objects to connect and share data with others devices. IoT objects create the infrastructure to control the devices wirelessly or through portable devices as well as smartly works like a human being requirements. It is depicted as a self-configuring wireless network of sensors which is intended for interconnecting all things. IoT gives us secure wireless communication and value added services as well as hardware implementation such as smart city, crop watering level system etc. Now a day, IoT does not have any boundaries for the development in hardware or only Information and Technology Sector. The enabling technologies of the IoT are:-

- RFID
- Sensor and actuator
- Miniaturization
- Nanotechnology
- Smart entities
- Wireless technology

IoT Infrastructure also improvised the security threats and developing user friendly applications in real world. IoT still works on security attacks or other threats.

Also, Cisco Internet of Things Group (IoTG) predicts that there will be around 50 billion users connected through IoT by 2020. The various application areas of IoT's are:-

1) Smart Home
2) Forestry Monitoring:
3) Intelligent transportation
4) Patient Monitoring Based System

### 1.1 TYPES OF ATTACKS IN IoT's

Any attack on IoT networks can be categorized as active and passive attacks based on Ad-hoc networks also. In an active attack, the misbehaving node actively disturbs the normal operation of the network with attempts to alter or destroy the data being exchanged in the network. It can also be classified into two categories, external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks. In passive attacks, the malicious entity only listens to the traffic without disturbing proper operation of the network. An attacker is also able to interpret the data gathered through snooping to violet confidentiality requirement [1].

#### 1.1.1 Sinkhole Attack

Sinkhole attack occurs when a malicious node attempts to make itself attractive to neighboring nodes so that packets are forwarded through the malicious node instead of the legitimate node. This type of attack can be combined with a Selective Forwarding attack for increased disruption of a network.

#### 1.1.2 DDOS Attack

In distributed denial of service attacks, an attacker node stops the other legitimate node to transfer the data and in place of legitimate node, attacker node declares itself as a legitimate node and starts sending and receiving the data on the behalf of other node.

### 1.1.3 Jamming

In physical layer, jamming is considered as the primary DOS attack. It has the ability to disturb the communication of an appliance or a network by a powerful jamming source like diffusing radio signals.

### 1.1.4 Jelly-fish Attack

Jellyfish attack affects the routing protocol. Jellyfish attack is an attack working in accordance with protocol rules and is difficult to detect. Attacker here intends to minimize good put of traffic by reordering the packet sequence, dropping or delaying the packets. In jellyfish delay variance attack, the malicious node disrupts the normal functioning of the protocol and introduces unwanted delays in forwarding data packets in the network [11]. This attack is one of the attacks that can be initiated from inside the network which makes it difficult to detect this attack.

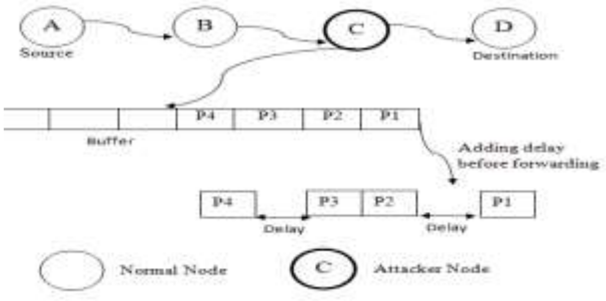

**Fig.1. Jellyfish delay variance attack**

## II. LITERATURE SURVEY

**Dave Eastman et al. (2017)** have studied different mechanisms to detect different types of attacks in Internet of Things (IoT). It is determined that packet drop and energy consumption parameters can become useful parameters for detecting those attacks in IoT. Current approaches to detect IoT attacks use many different parameters that require a great deal of overhead while this study aims to examine system parameters that can be utilized to detect the attacks in IoT effectively.

**Atinderpal et al. (2016)** reviewed the sinkhole attack and discussed the detection and prevention of sinkhole attack in IoT networks. Also implemented the AODV routing protocol's effectiveness and compare it with the previous methods.

**Stepen et al. (2016)** uses dynamic techniques to detect sinkhole attack in IoT infrastructure. Also identifies the mechanisms to prevent these kinds of attacks in IoT.

**Sudip Mishra et al. (2011)** considered a system model which is implemented on Layer of system model in IoT networks to prevent attacks like DDOS attack. This model automatically chooses path or action using system model procedure when a model detects the attack. This is based on Software networks.

**Chang and Wood and Stankovic et al.(2002**) in this determine the research on DDOS attack against wireless network. It is defined on specific interest at application layer known as Path-Based DOS attack. And implement the common approaches to detect attack with simple parameters of packet loss and reduce energy usage in IoT.

**Sana Benz arti et al. (2017)** Improving our world to be a better environment building a city of dreams which is called smart city is a trend field of research. In this context, objects will be connected to the Internet interacting with each other making the world smarter. The variety of networks building makes the IoT vulnerable. Smart home, smart grid, Smart transport, WSN, UASN, UWASN, etc make our lives easier by offering intelligent services that save time and effort.

**Prachi Shukla et al. (2017)** Due to the presence of unreliable internet and new routing protocols for low-power devices, IoT requires innovative security solutions. In this paper, authors present three new Intrusion Detection Systems (IDSs) for IoT: 1) Kmeans clustering unsupervised learning based IDS; 2) decision tree based supervised IDS; and 3) a hybrid two stage IDS that combines K-means and decision tree learning approaches.

**Neha and Aruna et al. (2013)** develop the jamming attack detection and prevention which models work on TCP and network model and detect jam attack when it exist using Triple DES techniques etc. They also considered the types of jamming attack i.e. internal and external but external jammer is not part of network.

**H. Suo et al. (2012)** compactly reviewed security in the IoT, and investigated security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application layer. At that point, the research status is talked about in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm. Finally several challenges are condensed. All things considered the development of the IoT will bring more serious security problems, which are always the concentration and the primary task of the research [1].

**J. Granjal, et al. (2015)** The Internet of Things (IoT) introduces a vision of a future Internet where clients, computing frameworks, and regular objects having sensing and actuating capabilities cooperate with unprecedented convenience and economical benefits [2]. Likewise with the current Internet architecture, IP-based communication protocols will play a key role in enabling the ubiquitous connectivity of devices in the context of IoT applications. Such communication technologies are being developed in line with the constraints of the sensing platforms liable to be employed by IoT applications, forming a communications stack ready to give the required power—efficiency, reliability, and Internet connectivity. As security will be a fundamental enabling factor of most IoT applications, mechanisms should likewise be designed to protect communications enabled by such technologies [2].

**S. Sicari, et al. (2015)** Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this situation, the fulfillment of security and privacy requirements plays a fundamental role. Such requirements incorporate data confidentiality and authentication, access control inside the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. More in subtle elements, a unified vision regarding the insurance of security and privacy requirements in such a heterogeneous environment, including different technologies and communication standards is as yet lost [7].

**J. Yun, et al. (2015)** The exceedingly fragmented and non-standardized landscape of the Internet of Things industry results in forcing both IoT developers and end-users to need to pick their restrictive consumer electronics by an organization, in the end turning into a barrier to construct an un-fragmented IoT ecosystem. [9]

## III. CONCLUSION

From above study it is clear that IoT is highly vulnerable to various kinds of attacks. These attacks are either active attacks or may be passive attacks. There are various techniques that had been followed by various researchers to identify and remove these attacks. Major research is being held by researchers to identify and remove active attacks. But few attacks are very hard to detect and remove. Because their nature almost similar to legitimate nodes. One of such attacks is delay tolerance attacks. These attacks are having very small delay which even legitimate node can produce. But they produce the delay unnaturally. In result will make various nodes to lose their energy more compared to the natural when there is no delay variance attacker.

## IV. FUTURE WORK

In existing researches various types of IoT attacks are being identified and removed. Major work has been done on Black hole, Sinkhole and Gray hole attack. There are highly efficient techniques which can address these types of attacks and implemented the detecting techniques. But very few works has been performed on delay variance attack or called Jelly Fish Attack. This type of attack is very hard to detect. Future work will be experiments in Delay variance attacks to detect and removal techniques. After detecting and removing compare parameters of performance analysis.

## REFERENCES

[1] Dave Eastman, Sathish A.P Kumar," A Simulation Study to Detect Attacks on Internet of Things",issue 113,2017.

[2] Vipindev Adat, and B. B. Gupta," A DDoS Attack Mitigation Framework for Internet of Things",issue 978,2017.

[3] Sana BENZ ARTI, Bayrem TRIKI and Ouajdi KORBAA," A Survey on Attacks in Internet of Things Based Networks",issue 978,2017.

[4] Atinderpal Singh, and Tejinderdeep Singh, "Review on Detection and Prevention of Sink Hole Attack In network", Global Journal of Computers & Technology, Vol.5, No.2, pp:289- 292. 2016..

[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," 2012, in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, no., pp. 648-651

[6] J. Granjal, E. Monteiro, and J. S´a Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," 2015, IEEE Communications Surveys & Tutorials Volume: 17, Issue: 3, pp. 1294-1312.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol.54, 2010, p. 2787-2805

[8] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen," Capillary Networks – Bridging the Cellular and IoT Worlds," 2015, IEEE 2nd World Forum on Internet of Things

[9] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, and D. Valletta, "Security implementation in heterogeneous networks with long delay channel," 2012, IEEE 1st AESS European Conference on Satellite Telecommunications, ESTEL 2012, Rome, Italy, p.1-5

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements and future direction”, 2013, Future Generation Computer Systems, Vol.29, p. 1645-1660

[11] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, Volume 76, 15 January 2015, Pages 146-164

[12Stephen .R, A. Dalvin Vinoth Kumar, and L. Arockiam, "Deist: Dynamic Detection of Sinkhole Attack for Internet of Things", International Journal of Engineering and Computer Science, International Journal of Electrical Electronics & Computer Science Engineering Volume 4, Issue 4 (August, 2017) | vol.5, issue. 12, pp. 19358- 19362, 2016.

[13] J. Yun, Il-Y. Ahn, N.-M. Sung, and J. Kim, “A Device Software Platform for Consumer Electronics Based on the Internet of Things”, 2015, IEEE Transactions on Consumer Electronics, Vol. 61, No. 4

[14] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji,” Access Features Analysis of Things in the Internet of Things”, 2016, IEEE, 978-1-5090-2534-3

[15] Archudha Arjunasamy, Thangarajan Ramasamy,” A Proficient Heuristic for Selecting Friends in Social Internet of Things”, 2016, ISCO, 3294794

[16] Minchul Shin, Inwhee Joe,” Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things”, 2016, IET Commun., Vol. 10, Iss. 12, pp. 1508–1521

[17] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues,” Toward Trustworthy Crowdsourcing in the Social Internet of Things”, 2016, IEEE, 1536-1284

[18] Dongsik Jo and Gerard Jounghyun Kim,” ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere”, 2016, IEEE Transactions on Consumer Electronics, Vol. 62, No. 3

[19] David Linthicum,” Responsive Data Architecture for the Internet of Things”, 2016, IEEE, 0018-91 62

[20] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong,” Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment”, 2016, IET Netw., Vol. 5, Iss. 5, pp. 107–113

[21] Haojun Huang, Jianguo Zhou, Wei Li, Juanbao Zhang, Xu Zhang, Guolin Hou,” Wearable indoor localisation approach in Internet of Things”, 2016, IET Netw., pp. 1–5

## Author Biography

Er. Manveen Kaur, Research Scholar, Department of Computer Science and Engineering, Guru Kashi University, Talwadi Sabo, Bathinda, Punjab. I completed B.tech in Computer Science and Engineering (cse) and Also I am pursuing M.Tech in Computer Science and Engineering .My research interests in Wireless Communication, Internet of Things(IoT), Security and Encryption.