Survey on Attacks in MANET Based Internet of Things System

Sana Zeba[1] Md Hussain Ahmad[2]
[1]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Jahangirabad Institute of Technology, Barabanki, Bangalore, India

Abstract— The rapid growth of technology has changed many things around us. If we talk about network a few years back it was just used for making the broad permanent network for sharing the resources and in communication and now we can make the network for any particular purpose. Internet of Things (IoT) system of many numbers of objects connected and it occurs on the digital environment. The major goal of the IoT is to allow the things or object to be linked anytime and at any location with using any digital device. Any wireless-based network technologies are used in the IoT system which is maybe wireless sensor technology or Mobile ad-hoc technology. These technologies are based on basically based on sensing concepts of sensors. Creation of IoT systems allows which may be based wireless or maybe IT-based IoT system. In the IoT System, Security and attacks have become major challenges due to network-based IoT system. In this survey paper discusses attacks in IoT system; categorize attacks and finding the most well-known attacks.

Keywords: Internet of Things (IoT), IoT Features, IoT Protocols, Attacks, Computing Devices, Communication, MANETs

I. INTRODUCTION

Internet of things (IoT) system is a framework that has been become more ordinary for current years. The most important objective of the IoT system is to allow the things to be connected at any location and anytime with any device. Internet of Things (IoT) system has newly received a great concentration due to its potential and capability of a complex system. The first network project Arpanet which sponsored by the U.S. Department of Defense designed the first protocol called as the network control protocol in organizing to join different machines and which used the packet switching for sharing the information. Later on, Arpanet became Internet project and other new standard protocol, which was developed on the basis of an open architecture philosophy. In this area, we can find other types of networks such as Underwater Acoustic Sensors Network (UASN), Mobile Underwater Wireless Sensors Network (MUWSN) and Underwater Acoustic Wireless Sensors Network (UAWSN).

In this paper, discuses about diverse IoT attacks with their many existing solutions. Also further these attacks are classified on the basis of vulnerabilities of the IoT attacks used to compromise the IoT network. That's why; some attacks are shortlisted as an unsafe attack from each category on the basis of their less opportunity of detection and capability to impact the IoT system network. These attacks are discussed in detail and compared with the same parameters. This paper is structured as follows. Section II is the literature survey on IoT system, MANET network, and IoT attacks. Section III gives an overview of IoT system devices and. In Section IV, explain different protocols of IoT system. Section V, reviews of different attacks of MANET based IOT system and Section VI, representing some concluding comments and identifying promising trends.

A. IoT System

Internet of Things (IoT) system is a topic used to discuss an environment where more than billions of objects (things), constrained in terms of resources, are connected with the different internet and interacting in parallels. The IoT system environment in which all objects are placed becomes smarter with so many types of objects in the IoT system. For recent years, the model of the IoT system has become more popular. The major objective of the IoT system is to permit the object to be connected at any location and anytime with any devices. The sensors and the meeting of information technologies such as wireless communication and the Internet, IoT is rising as an important technology for monitoring systems, as the quick development of sensing technologies in current time.

The environment of the internet of things (IoT) system is connected with devices, objects, mechanical and digital machines objects, animals or people object which are assigned with unique identifiers (UIDs). A thing or object in the internet of things (IoT) system can contain an object with a heart monitor machine embeds a farm animal by using a biochip transponder, an automobile which has suit-in sensors. Progressively more, organizations in a diversity of industries are using IoT system to function more efficiently, better recognize customers to deliver improved customer service, improve decision-making operation and raise the value of the business.

In IoT, environment devices are sharing the sensor information among devices. They collect data by connecting to an IoT system gateway. So many times, IoT system devices contact with other associated devices in the system and act on the gathered information which has to gain from one another devices. The devices of IoT system do the majority of the work without human interference, even though people can interact with the devices, for instance, to set them up, give them instructions or contact the data.

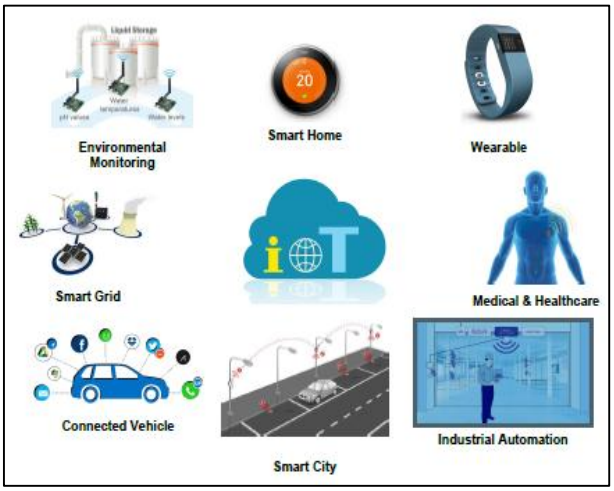

Fig. 1.1: Internet of Things System

B. IoT Application

Internet connectivity of the Internet of things (IoT) system is expanding into many physical devices and objects. It is embedded with electronics devices, Internet connectivity, and additional forms of hardware (such as sensors, actuators), and these devices can communicate and interact with other devices over the Internet, and these devices can be remotely controlled and monitored. With these web-enabled devices used the connectivity, networking and communication protocols which largely depend on the particular IOT application deployed.

IoT system has many applications; some applications are following which are as follows,

- Smart Home
- Wearable's
- Smart City
- Smart Grids
- Industrial Internet
- Connected Car
- Connected Health (Digital Health/ Telehealth/ Telemedicine)
- Smart Retail
- Smart Supply Chain
- Smart Farming

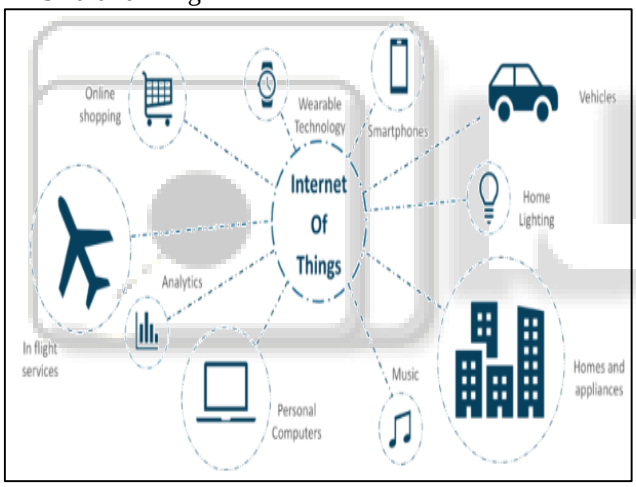

Fig. 1.2: Applications of IOT System

C. IoT Features

Internet of Things (IoT) system is growing quickly and dynamically. It is defined as a system of the connectivity of the device over the internet. It's similar to social networking or an email service, but instead of connecting different people, IoT system network actually connects smart devices which include, smart home appliances, your computers, smart phones, automation tools, and more. Important features of the IoT system are analyzing, connectivity between devices, active appointment, integrating different devices, etc. Some IoT system features are listed below:

1) Connectivity: Connectivity of the system defined as to establish a proper connection among the sensors of the device of the IoT system.
2) Analyzing: After connecting all the appropriate objects, it comes to real-time analyzing the data collected and use them to build valuable business intelligence.
3) Integrating: IoT system integrates the various models into the same environment for improving the user experience as well.
4) Artificial Intelligence: IoT system makes objects smart and enhances life during the use of different data.
5) Sensing: The sensor devices used in IoT system environment which are detected and calculate any change in the system and report on their status situation.
6) Active Engagement: IoT system makes the connected environment of the devices, product, or services to active appointment among objects of the system.
7) Endpoint Management: It is very essential to be the endpoint management of every device of IoT system otherwise; it gives the total failure of the IoT system.

D. MANET Network

Wireless sensor and actuator networks (WSAN) play a key role in the accomplishment of the Internet of Things (IoT) systems. It represents the interaction between computational systems and the physical environment in the world today. In a wireless sensor and actuator networks (WSAN), both actuators and sensors control the physical environment with their attributes like temperature, pressure, light intensity, and the sound level is constantly measured by devices joined to either a WSN or a WSAN network. Précised data are sent by wireless communications to processing IOT system devices for analysis and essential control data transmitted back to connected actuators of WSAN.

The wireless sensor network is similar to MANET because both are multi-hoped and self-configured networks. While the topology of MANET is extra changeable than WSN. MANET protocols can permit it to act as wireless sensor network backbone and exchange information with WSN about MANET starting entry points and as well as access wireless sensor network's nodes. Both two networks can allow more efficient and reliable cross-network protocol routing in the IoT system network.

II. LITERATURE REVIEW

In [1], the author has introduced safe routing for IoT systems based on MANET and it is not only an IoT security matter, but it is also a key Internet security problem because of the large and quickly growing number of such type of systems. In this paper presents a modern appraisal of communication architectures and topographies for MANET based Internet-of-Things (IoT) systems and also identifies some main research challenges in the emerging field of MANET based IoT connectivity.

In [2], the author tries to bring order on the IoT security scene and providing taxonomic monitoring from the point of view of the main key layers of IoT system model. It has also introduced about Social Internet of things (SIOT) as a new model where the Internet of things (IoT) merges with different social networks which allowing devices and people to facilitate information and interact.

In [3], the author has proposed "It Feature" concepts for the better recognize the necessary reasons for new threats and the challenges in recent research. In this paper also discussed security and privacy effects on IoT system on the

basis of different IoT features including the threats and different existing solutions.

In [4], this paper study the privacy defense problem in IoT system through a broad review of the state-of-threat by mutually considering three major dimensions, namely the state-of-the-art principles of privacy laws, the IoT system architecture and representative privacy-enhancing technologies (PETs).

In [5], the author has provided an overview of structural health monitoring (SHM) system implementation based on the combination of the wireless sensor network (WSN), IoT system, and big data tools. The rest of this paper introduces a framework model for structural health monitoring (SHM) by using different IoT technologies on smart and reliable monitoring.

In [6], the author discussed a variety of IoT attacks happening and classifies all attacks. Also, explain its countermeasures and finding the most important attacks in IoT. In this survey about the variety of attacks have been presented and compared different attacks on the basis of their efficiency and damage stage in IoT system.

In [7], the author has explained an AODV Routing Protocol for performance assessment of Energy Efficient for MANET network. To increase network lifetime, energy efficiency, throughput and decrease the end to end delay of networks are the main objective of this paper. In the route discovery phase, this scheme is applied to the AODV routing protocol. A recvRevrese () function is used at a certain threshold level to check out the energy level of the node. It enhances the remaining energy of the nodes in an ad-hoc network.

In this paper [8], the author presents a categorization of attacks from a variety of networks involved in IoT system. This categorization discriminates common and specific attacks from each network and uses several criteria like the congestion, security attributes, disturbance. Also, several existing security solutions are presented for the purpose to expose the security requirements to protect IoT.

In [9], the author has introduced paper of Comparing and Analyzing Reactive Routing Protocols (AODV, DSR, and TORA) in QoS of MANET. This research paper has been conducted using the OPNET modeler simulation. It has evaluated different QoS metrics of different reactive protocols like TORA, AODV, and DSR.

In this survey [10], the authors have presented the security and privacy problems in IoT applications and systems. They presented the restrictions of IoT devices in battery and computing assets and discussed different possible solutions for battery life expansion and lightweight computing. They also considered existing categorization approaches for IoT attacks and security mechanisms.

In [11], the author has shown a denial of service (DoS) attack to an IoT system. Different attacks tools have discussed in this paper for QoS attacks. As the Quality of service attack tool is Kali Linux, which is launched by using many different methods and also compare different methods.

In [12], the author has introduced a paper on Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks. In this security analysis, we take into consideration the network size, the mobility, the traffic load and finally the number of the attackers. Different attacks have been implemented in NS-2 based on AODV routing protocol. Then, they compared the performance of AODV under attacks with the original AODV in terms of Packet Delivery Ratio, Average End to End Delay and Average Throughput.

In [13], the author has introduced a survey paper on Security Issues in Mobile Ad-hoc Network. In this paper, we will study security problems and their existing solutions. In this survey paper, they try to analyze the reasons that cause security issues in MANET that disturbs the normal functioning of the network.

In [14], the author has proposed a paper on Effect of Pause Time on AODV and TSDRP Routing Protocol under Black Hole Attack and DOS Attacks in MANET. This paper study the impact of pause time of our proposed Trust-Based Secure on Demand Routing Protocol called "TSDRP". It evaluates performance on the basis of PDF, AED, AT and NRL. TSDRP protocol is capable of delivering packets to destinations even in the presence of malicious node while increasing pause time in MANETs. TSDRP protocol shows better performance in almost all parameters: PDF, AED, AT and NRL as compared to AODV.

In this paper [15], black hole attack is implemented on AODV protocol which reduces the performance parameters of the network by exploiting the packet sequence number included in any packet header. They can conclude that when the number of nodes is varied, AODV has the highest packet delivery ratio (PDR) and normalized routing load (NRL) while DSR has the highest throughput.

In [16], the author gives a complete survey and investigation of embedded security, especially in the field of IoT system. Based on this survey and investigation, in the paper, the author defines the security requirements taking into account computational time, energy utilization and memory needs of the devices. It also proposes an embedded security structure as a characteristic of software/hardware co-design methodology.

In this paper [17], the author has tried to provide a brief study about routing protocols on MANETs under the categories of basic, location aided and security-based protocols. It also focuses on the advantages and disadvantages of the protocols.

In [18], the author has introduced evaluated effects of different routing attacks against MANETs i.e. black hole, sinkhole, selfish behavior, RREQ flood, hello flood, and selective forwarding attacks.

In [19], the author has introduced a Performance Evaluation on Modified AODV Protocols. The paper evaluates some of the modified AODV protocols which is performance after examining the effectiveness in alleviating of the black hole attack. It further exams the effect of mitigation methods that are used on overhead.

In [20], this paper presents the survey about the common Denial-of-Service (DoS) attacks that are on the network layer. These are named as Wormhole attack; Black hole attack and Gray hole attack. These are serious threats for MANETs. This paper also shows a brief view about routing as well as security concerns of MANET.

In [21], the author has introduced a method for identification in Ad hoc Networks. This paper focuses on creating a complete security framework to address these

problems. We have identified three different aspects that need to be solved in order to secure MANETs: Identification, Secure Routing, and Prevention of Selfish Nodes.

III. COMPUTING DEVICES

Internet of Things (IoT) is a group of "things or objects" which have sensors, actuators hardware, software, electronic devices, and can be connected with the Internet to exchange and collect information with each other in the network. The IoT devices are prepared with sensors and processing power that used them to be deployed in many IOT based environments. IoT contains uncountable physical objects that have not been concerned in the usual Internet. An object of the IoT system enables their cooperation and interaction to provide a broad range of IoT applications [4]. A lot of services in the IoT system may involve analysis and investigation of data collected through a large number of physical devices and comprehensive understanding that challenges both private information privacy and the development of the IoT system.

IoT system involves expanding internet connectivity outside of the standard physical devices, such as laptops, smart phones, tablets, and desktops, to any range of usually dumb or without internet-enabled physical devices or nodes of the system and daily objects. Connected physical devices are part of circumstances in which every device talks to other associated devices in an environment to mechanize industry tasks and home. Examples of enterprises IoT devices and other industries are like monitor weather and traffic conditions, the security of the system and smart city technologies.

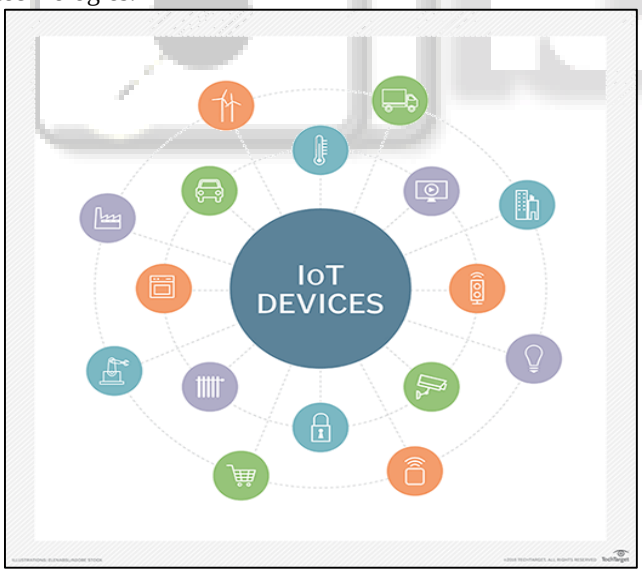

Fig. 1.3: Devices of IoT System

IV. IOT PROTOCOLS

The interaction between the IoT system and MANET network opens new customs for service requirement in smart system environments and challenging problems in its networking aspects. Since the IoT system mostly depends on lots of different wirelesses sensors and selection of sensors from MANET protocols focuses on the most capable and shortest routes. Appropriate utilization of battery power supply of sensors is a key role in maintaining the network connectivity of wireless nodes in the network. Due to sensors nodes, constraints like human interface with IoT devices, temperature, computational speed, sounds and network node density, wireless network protocols cannot be used openly. Hence, there is a requirement of complex solution for routing over MANET based IoT system, which can use node remaining energy professionally and expand the network lifetime.

The success of IP protocol and the use of radio and satellite networks made the Internet a global system with the capacity to access and collect information, communicate with people around the world through the Internet by using the TCP/IP architecture.

Nowadays, any objects able to sense the environment features like temperature, sounds, etc. and interchange digital data among connected nodes to the Internet using IP protocol. In some case, an IP proxy or software able to convert IP into dedicated wireless protocol is used to ensure continuity between a sensing object that cannot support IP and the Internet. Objects of the Internet in the IoT system may be mobile phones, cameras, any home appliances, city infrastructures, medical instruments, and plants or cars which have contain sensors. It uses IPs for communicating in the network and can also share information about their environment anytime from anyplace.

For routing protocols of multi-hop MANETs based system are analyzed with a focus on the consistent Routing Protocol for Low-power. In modern wireless-based routing, there are so many security threats, issues and exposures are described and these are increasing security in routing protocols. For supporting and enhancing secure routing in MANET based IoT system, there are many trust models and methodologies are presented. Routing protocols for wireless sensor-based IoT system nodes requires also network topology. Various routing protocols are in the wireless network. Routing protocols can be also differentiated into three types:

- Proactive routing protocol
- Reactive routing protocol
- Hybrid routing protocols

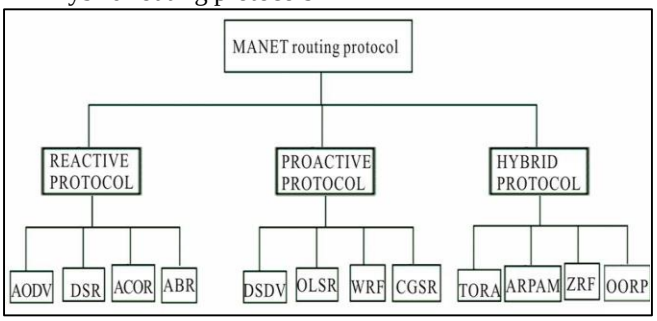

Fig. 1.4: Routing Protocols in MANET based System

V. ATTACKS IN MANET BASED IOT

In Networking the MANET or WSN based IoT system is used WSN routing principles, MANET routing protocols concept, and data handling, sensing, and processing. Networking of such type systems are very difficult and challenging regarding the routing. Routing protocols of these types of systems are limited in-network sensor and mobility resources.

MANET protocols are designed with mostly focus on QoS, efficient energy consumption.

With limited characteristics of the internet with different mobile ad-hoc network and wireless connection of different objects must be guaranteed connectivity, reliability, and connectivity of the IoT system. IoT system devices are susceptible to different attacks in many ways, some ways are:

- Device identity attacks: For the cloud to be able to understand or use your information, it has to trust that the device that is sending the information is legitimate and not a false one. Hence, the identity of the devices needed for protection.
- Device integrity attacks: Through this attack, the device itself could have its configuration changed by malware or a hacker.
- Lifecycle attacks: You could have a legitimate device but if you don't protect it with the right level of security, then that can invite hackers to install malware into your device.
- Communication attacks: This type of attacks refers to "man-in-the-middle" attacks or eavesdropping. It usually happens during the illegal usage of retail websites.

A. Physical Cyber-Attacks:

Physical cyber-attacks result from breaches to the IoT system device's sensors. Physical attacks are determined on hardware devices in the system.

1) Node Tampering Attacks:

In this attack attacker node physically alters the compromised node and it can also obtain sensitive information from a node such as encryption key [22].

2) RF Interference on RFIDs Attack:

By sending noise signals over signals, the attackers perform Denial of service (DoS) attack, any other routing attacks and signals are used in RFID's (Radio Frequency Identification) communication.

3) Node Jamming in WSNs:

By using jammer, the attacker nodes can disturb the wireless sensor-based communication in the system [22].

4) Malicious Node Injection Attack:

Attackers or intruder nodes are physically inserting a malicious node between the path of source and destination node. Then it modifies data and passes the wrong data to other nodes.

5) Physical Damage:

Many attackers physically damage components of the IoT system.

6) Social Engineering Attacks:

The attacker or intruder nodes directly work together with nodes in the network and also influence users for damaging networks of an IoT. The attacker nodes are finds out sensitive data to accomplish his target.

7) Malicious Code Injection Attack:

The attacker nodes or malicious node can acquire full monitoring and controlling of nodes in wireless IoT systems.

8) Sleep Deprivation Attack:

The target of this attack is using more power supply in the system for performing any operations.

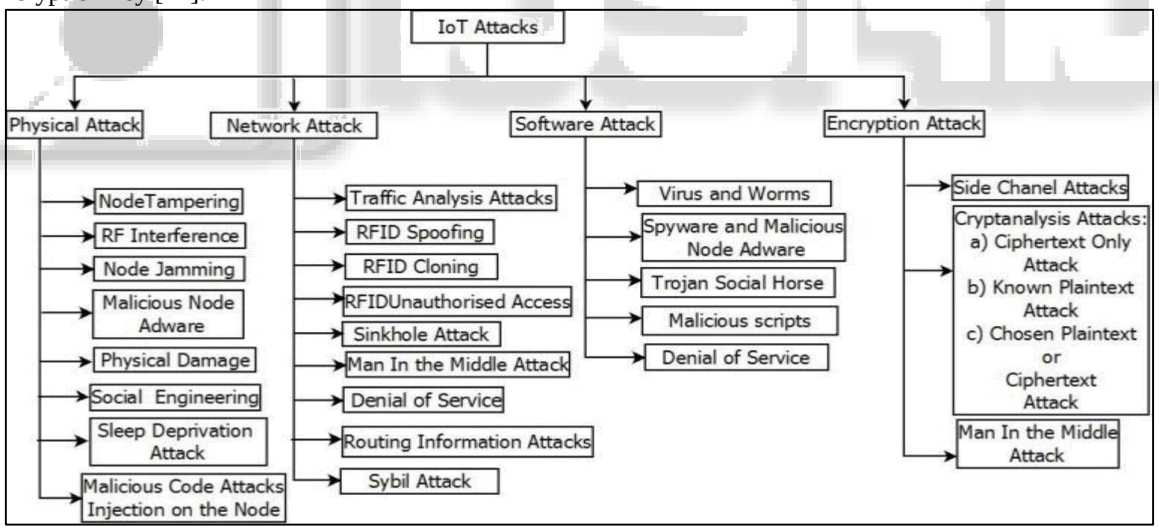

Fig. 1.5: Attacks in IOT System

B. Network cyber-attacks:

Attackers or intruders nodes insert themselves in the network (known as "Man in the Middle" or "MitM"), and it is creating duplicate identities and stealing data or information, and it can redirect data to their preferred location for accomplish goals which is away from network (also referred to as a "sinkhole" attack).

1) Traffic Analysis Attacks:

The attacker intercepts and checks data to obtain network information [22].

2) Sinkhole Attack:

By using compromises node sinkhole attack performs and this compromised node present inside the network.

3) Denial of Service:

Services of intended users are unavailable due to large traffic floods in the network.

4) Routing Information Attacks:

In this attack, the attacker node can make the network composite by sending information or spoofing, modifying.

5) Sybil Attack:

In this attack, malicious or attacker node that takes the identities of many nodes and acts as them.

C. Software Attacks:

Software attacks happen when malware software is installed into the network's program. This malicious software sends a worm, virus, and spyware which corrupts or steals data and can both disrupt and spy on the activities.

1) Phishing Attacks:

The intruder or malicious node finds the personal information like username, passwords by using fake email spoofing and fake websites.

2) Virus, Worms, Trojan horse, Spyware and Aware:

An opponent can spoil the system by using the malicious code.

By email attachments, downloading any files from the Internet, these malicious codes are spreads. Without human interference, worm can replicates itself.

3) Malicious Scripts:

By inserting the intruder or malicious script in the system, the attacker can acquire access to the system.

By email attachments, downloading any files from the Internet, these malicious codes are spreads. Without human interference, worm can replicates itself.

4) Malicious Scripts:

By inserting the intruder or malicious script in the system, the attacker can acquire access to the system.

D. Encryption Attacks:

Finally, in encryption attacks, attackers analyze and deduce encryption keys, to figure out how implementation works

Parameters	Classification Types		
	Spoofing Attack	Worm Attack	Sinkhole Attack
Attack type	Active -As the attacker nodes can modify data.	Active -As it modifies the files, documents.	Active -As it is provide wrong information to neighbor nodes in path.
Attacker Location	External, Internal	External, Internal	External
Damage Level	High -As it can modify the data and pass the wrong information to other nodes.	High -Because it can delete important files, emails, documents.	High -Because data or packets flowing through compromised node and attacker can do anything's with data.
Detection Chances of Attack	Low	Normal -By using Anti-virus	Difficult
Attack based parameter	Malicious Information or messages	Malicious Code	Routing
Threats of Attack	Availability, Integrity	Authenticity, Integrity, Availability	Availability, Confidentiality
Chances of Prevention	Yes -By provide nodes identity	Yes -By avoid suspicious sites and files.	Yes -By authentication of every nodes in the network
IOT Layer	Perception	Application	Network

Table 1: Comparison of Various IOT Attacks

VI. Conclusion

IoT is a latest and growing technology that has lured a significant amount of people attending from all around the world. With the help of several most important contributions, this technology has been made flexible into our daily life. With the development of the IoT system, various kinds of attacks have been invented to break the security of IoT devices in the system. So many researchers have proposed several solutions for the routing attacks of WSN and deal with it. Some attacks of WSN based IoT system has been discussed and classify it on the basis of some attributes. In this paper, the most important security concepts of IoT system were reviewed and analyzed widely. All kinds of security threats with respect to the field of IoT that may become an obstacle while implementing it or its development have been discussed and classified based on IoT system layers. Then finally, there has needed to find efficient and secure solutions of attacks which are known and difficult to detect are prevent.

References

[1] Jonny Karlsson "Secure Routing for MANET Connected Internet of Things Systems", 2018 IEEE 6th International Conference on Future Internet of Things and Cloud page 114- page 119

[2] Mario Frustaci, Pasquale Pace "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 4, AUGUST 2018 page 2483- page 2495

[3] Wei Zhou, Yuqing Zhang, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE https://ieeexplore.ieee.org/document/8386824

[4] Chao Li, Student Member, "Privacy in Internet of Things: from Principles to Technologies" 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See

http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

[5] C. Jr. Arcadius Tokognon, Bin Gao "Structural Health Monitoring Framework Based on Internet of Things: A Survey" 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information. page 619-page 635

[6] Jyoti Deogirikar, Amarsinh Vidhate "Security Attacks inIoT: A Survey " http://faratarjome.ir/u/media/shopping_files/store-EN-1520245543-1185.pdf

[7] Anjana Tiwari and Inderjeet Kaur "Performance Evaluation of Energy Efficient For MANET Using AODV Routing Protocol ", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017) page 1 – page 5

[8] BENZ ARTI, Bayrem TRIKI "A Survey on Attacks in Internet of Things Based Networks" 2017 IEEE https://ieeexplore.ieee.org/document/8273006

[9] Abdalftah Kaid Said Ali and Dr. U.V. Kulkarni "Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET", 2017 IEEE 7th International Advance Computing Conference page 345 - page 348.

[10] Lulu Liang, Kai Zheng "A Denial of Service Attack Method for an IoT System " 2016 8th International Conference on Information Technology in Medicine and Education

[11] HoudaMoudni and Mohamed Er-rouidi "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks", 2nd International Conference on Electrical and Information Technologies ICEIT'2016 IEEE.

[12] Yuchen Yang, Longfei Wu "A Survey on Security and Privacy Issues in Internet-of-Things" 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

[13] Vishnu Sharma and Akansha Vij "Security Issues in Mobile Adhoc Network: A Survey Paper " International Conference on Computing, Communication and Automation (ICCCA2016) IEEE page 561-page 566

[14] Nirbhay Chaubey "Effect of Pause Time on AODV and TSDRP Routing Protocol under Black Hole Attack and DOS Attacks in MANET ",2015 2nd InternationalConference on Computing for SustainableGlobal Development(INDIACom) IEEE page 1807-page 1812

[15] Sandeep Kumar Arora and Mubashir Yaqoob Mantoo "Performance Measurement in MANET " , 2014 5th InternationalConference- Confluence The Next Generation Information Technology Summit (Confluence) IEEE page 406-page 410

[16] Sachin Babar, Antonietta Stango, "Proposed Embedded Security Framework for Internet of Things (IoT) " 2014 https://www.researchgate.net/publication/252013823

[17] 17) Geethu Mohandas ,Dr Salaja Silas and Shini Sam" Survey on Routing Protocols on Mobile Adhoc Networks ",©2013 IEEE page 514-page 517.

[18] Ehsan, H., & Khan, F. A. (2012, June). Malicious AODV: implementation and analysis of routing attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 1181-1187). IEEE.

[19] Zaid Ahmad and J.A. Manan" Performance Evaluation on Modified AODV Protocols ",2012 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE 2012), December 11 - 13, 2012, Melaka, Malaysia page 158-page 163

[20] Rutvij H. Jhaveri and S.J.Patel "DoS Attacks in Mobile Ad-hoc Networks: A Survey ",2012 Second International Conference on Advanced Computing & Communication Technologies IEEE page 535-page 541

[21] Frank Kargl, Stefan Schlott, Michael Weber "Identification in Ad hoc Networks ",Proceedings of the 39th Hawaii International Conference on System Sciences – 2006 IEEE page 1-page 9

[22] Ms. Shilpa B. Sarvaiya "Study of Security Challenges in Multilayered Structure and Various Attacks on IOT" 61st IETE Annual Convention 2018 on "Smart Engneering for Sustainable Development" Special Issue of IJECSCSE, ISSN: 2277-9477 page 30- page 36

