



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

**Thesis for the Degree of  
Masters of Engineering**

**Novel Methodology for the Detection of Malicious Nodes  
from IoT**

The Graduate School  
University of Ulsan

Department of Global Smart IT Convergence

SAINI JYOTI

# **Novel Methodology for the Detection of Malicious Nodes from IoT**

Supervisor: Chong, UiPil

A Dissertation

Submitted to  
The Graduate School of the University of Ulsan  
In partial fulfilment of the Requirements  
For the Degree of

Master of Engineering

by

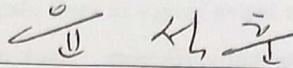
SAINI JYOTI

Department of Global Smart IT Convergence  
Ulsan, Korea

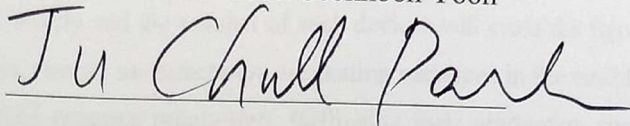
April 2021

# Novel Methodology for the Detection of Malicious Nodes from IoT

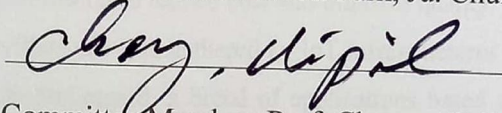
This certifies that the dissertation of Saini Jyoti is approved.



Committee Chair: Prof. Seokhoon Yoon



Committee Member: Prof. Park, Ju. Chull



Committee Member: Prof. Chong, UiPil

Department of Global Smart IT Convergence  
Ulsan, Korea

July 2021

## **Abstract**

The Internet of Things (IoT) is considered to be a rapidly evolving technological model that is continually drawing the consideration of research and the industrial sector. This perception makes a shift to IoT very attractive to individuals, the public sectors, and commercial organizations. It can affect individuals' lives to a great extent and upgrade different factors in many areas including transportation, energy, manufacturing, medical, smart cities, agriculture, and so on. According to an estimate, the number of devices connected by IoT will increase rapidly all over the world shortly and the number of such devices will cross the figure of 75 billion by 2025. Nowadays, several manufacturers are putting resources in the establishment of IoT set-up for improving resource monitoring, facilitating their production cycles, and enhancing their product distribution to reduce cost and improve quality. In addition to this, a significant number of providers use data gathered by IoT infrastructures to offer high-quality services or applications. In this regard, a breed of applications based on IoT uses location information to modify their properties concerning the client's location and the objects of interest. However, the presence of some obstacles considerably delays the further advancement and development of the IoT vision, for example, matters concerning privacy, security, and client acknowledgment. IoT has pulled the attention of malicious attackers who often attack IoT infrastructure to gain access to potentially useful information. This is for the reason that IoT has become an integral part of everyone's regular day-to-day life and has the potential to gather and distribute a massive volume of (generally sensitive) data.

The devices in the IoT are capable of producing, processing, and exchanging not only the enormous volume of data related to security and safety but the privacy-sensitive information also. Thus, several attacks are inclined towards these devices. The integrity of the underlying devices, especially their code and data privacy against the malicious modification is required for providing the precise and secure operation of Internet of Things systems. There are two types of privacy threats occurred in IoT. The first is the privacy threat which is based on data and the second is the privacy threat that takes place on location. Data privacy issues are generated when secret information is leaked in the process of data acquisition and transmission. In the IoT, the essential part to protect privacy is location privacy. This part is related to the location privacy of every node in the IoT and the location privacy of the IoT to provide different location services such as privacy of RFID reader location, its user location, sensor node location, and location-based privacy issues. The network, in which personal and

sensitive information about the condition of a person contains, often makes the collection, aggregation, and transmission of data. The location protection is the denial of service attack which reduce network performance. The technique is proposed in this research work is based on the threshold and monitor mode for the detection of malicious nodes. The proposed methodology is implemented in NS2 and results are analyzed in terms of throughput, packet loss, and delay.

## **Acknowledgments**

This thesis is based on the work done at the Department of Smart IT Convergence, the Graduate School, University of Ulsan, from March 2021 to June 2021 and supervised by Professor Chong, UiPil, to whom the author wishes to express his sincere gratitude for their continuous support and guidance.

I would like to express my gratitude to my supervisor Professor Chong, UiPil for the useful comments, remarks, and engagement through the learning process of this master thesis.

Furthermore, I would like to thank Prof Surinder Sharma for introducing me to the topic as well for the support on the way.

Also, I like to thank my friends, who have willingly shared their precious time during the coding process. I would like to thank my loved ones, who have supported me throughout the entire process, both by keeping me harmonious and helping me putting pieces together. I will be grateful forever for your love.

# Contents

|  |     |
|--|-----|
| <b>Abstract</b> .....                                      | iv  |
| <b>Acknowledgments</b> .....                               | vi  |
| <b>Contents</b> .....                                      | vii |
| <br>   |     |
| <b>Chapter 1</b>   |     |
| <b>Introduction</b> .....                                  | 1   |
| <b>1.1. Introduction to IoT (Internet of Things)</b> ..... | 1   |
| <b>1.2. IoT Layered Architecture</b> .....                 | 1   |
| <b>1.3. Security in IoT</b> .....                          | 3   |
| <b>1.4. Location Privacy in IoT</b> .....                  | 7   |
| <br>   |     |
| <b>Chapter 2</b>   |     |
| <b>2.1. Literature Summary</b> .....                       | 15  |
| <b>2.2. Literature Review</b> .....                        | 20  |
| <br>   |     |
| <b>Chapter 3</b>   |     |
| <b>Problem Formulation</b> .....                           | 35  |
| <b>3.1. Problem Formulation</b> .....                      | 35  |
| <b>3.2. Objectives</b> .....                               | 35  |
| <b>3.3 Research Methodology</b> .....                      | 36  |
| <br>   |     |
| <b>Chapter 4</b>   |     |
| <b>Result and Discussion</b> .....                         | 38  |
| <b>4.1. Tool and Technologies</b> .....                    | 38  |
| <b>4.1.1 Deployment of Network</b> .....                   | 39  |
| <b>4.1.2 Division of Network in Clusters</b> .....         | 39  |
| <b>4.1.3 Aggregation of sensed information</b> .....       | 40  |
| <b>4.1.4 Location Protection Number Attack</b> .....       | 40  |
| <b>4.1.5 Proposed Methodology</b> .....                    | 41  |



**Chapter 5**

**Conclusion and Future work**.....45

**5.1. Conclusion** .....45

**5.2. Future Work** .....46

**References**.....47

**List of Publications**.....47

# List of Figures

|  |           |
|--|-----------|
| <b>Figure 1.1: Five-layer architecture of IoT.....</b>                           | <b>2</b>  |
| <b>Figure 1.2: Classification of Location Privacy Attacks.....</b>               | <b>9</b>  |
| <b>Figure 2.1. Attacker capturing the data traveling from/to the server.....</b> | <b>17</b> |
| <b>Figure 2.2. A server acting as a malicious party.....</b>                     | <b>17</b> |
| <b>Figure 2.3. Our Proposed Web Services Architecture.....</b>                   | <b>20</b> |
| <b>Figure 3.1: Proposed Flowchart.....</b>                                       | <b>37</b> |
| <b>Figure 4.1: Deployment of Network.....</b>                                    | <b>39</b> |
| <b>Figure4.2: Division of the network in clusters.....</b>                       | <b>39</b> |
| <b>Figure 4.3: Aggregation of sensed information.....</b>                        | <b>40</b> |
| <b>Figure4.4: Location Protection Number Attack.....</b>                         | <b>40</b> |
| <b>Figure4.5: Proposed Methodology.....</b>                                      | <b>41</b> |
| <b>Figure 4.6: Energy Consumption.....</b>                                       | <b>42</b> |
| <b>Figure 4.7: Delay Analysis.....</b>   | <b>43</b> |
| <b>Figure 4.8:Throughput Analysis.....</b>                                       | <b>44</b> |

# Chapter 1

## Introduction

### 1.1 Introduction to IoT (Internet of Things)

The term Internet of Things (IoT) is considered to be a heterogeneous network comprising physical and virtual objects. This system is embedded with electronics, software, sensors and provides connectivity to allow objects to obtain better value and service by sharing data online with other linked objects. The word “Thing” in IoT, maybe a patient with a heart monitor implant, livestock with a biochip transponder, a field operating robot assisting in a hunt and rescue mission, or any other natural or artificial object provided with an IP address and ability to relay data and to interoperate within the present Internet system. The rapidly expanding technology of IoT (Internet of Things) into different application fields (e.g., building and home automation, smart transportation systems, wearable technologies for healthcare, industrial process control, and infrastructure monitoring and control) is driving the change in the elemental way of perceiving and managing the actual world [1]. Almost all IoT devices are intended to be pocket-friendly and based on the innovation of wireless communication with restricted abilities concerning storage and computation. The increasing trust in IoT frameworks due to their ability to sense and control extremely complicated ecosystems adds a question mark to the security and reliability of the data being transferred to and from the IoT devices.

### 1.2 IoT Layered Architecture

The worldwide researchers have never agreed on a single and general arrangement of IoT architecture. The most fundamental IoT architecture is three-layered consisting of perception layer, network layer, and application layer.

- i. Perception layer: This layer comprises physical objects being monitored/controlled by sensor & actuator devices. The main objective of these devices is to collect sensor data and control actuation [2].
- ii. Network Layer: This layer facilitates the data connectivity to the devices in the perception layer to realize the functioning of diverse applications in the application

- layer. As this layer acts as the connectivity provider for other layers, some security flaws may occur which could compromise the functionality of the overall IoT system.
- iii. Application layer: The application layer manages IoT applications globally. This layer relies upon the information processed in the middleware layer. Apart from this, this layer relies upon the details of the diverse enforced IoT applications, such as smart industry, smart health, etc.

Researchers have presented a five-layered architecture due to growing concerns regarding security and privacy in IoT. It is a new architecture to satisfy the security and privacy concerns of IoT. Figure 1 represents the five-layered IoT architecture.

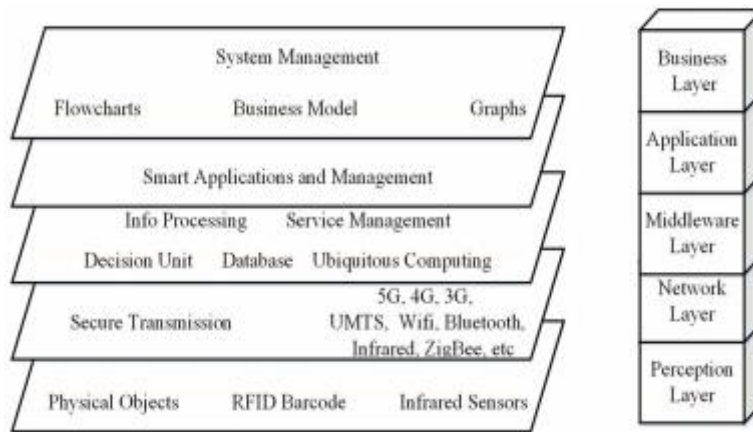


Figure 1.1: Five-layer architecture of IoT

The perception, transport (i.e., network layer), and application layers in five-layer architecture work the same as in the three-layer architecture. The remaining layers of this arrangement are [3]:

- i. Processing layer: This layer is also known as the middle-ware layer. This layer provides different sorts of services, especially stores, analyzes, and processes data in terms of computational results.
- ii. Business layer: The complete IoT system actions and functionality come under this layer. The application layer sends the data to the business layer which, in turn, builds business models, graphs, and flowcharts for analyzing data, and thus participates actively in decision-making concerning business plans and road-maps.

### 1.3 Security in IoT

Security refers to the process of upholding high confidentiality and integrity of the asset's information and making information concerning the object available as per the need to secure a resource against physical damage, illegal access, or stealing. IoT security is a research field related to the preservation of connected devices and networks in the IoT system. IoT holds great promise for many applications in diverse areas, for example, smart grids, smart cities, smart homes, medical, and industrial applications [4]. However, new security concerns originate due to limitedly able IoT devices and IoT technologies in such subtle applications. The major security challenges in IoT are authentication, authorization, integrity, confidentiality, non-repudiation, availability, and privacy. All these challenges have been summarized as:

- a. Authentication: It refers to the way of verifying an object's identity. The entity being verified could be both humans as well as machines. It is the primary stage of any access control system capable of determining the precise identity of the accessing party to make the system trustable.
- b. Authorization: It is the way of imposing restrictions and granting privileges to the verified objects. This process determines the abilities of an object in the framework.
- c. Integrity: Integrity is the process of maintaining the consistency, precision, and dependability of information throughout its life span. In IoT, any change in crucial information or even the infusion of illicit information may lead to major problems.
- d. Confidentiality: It is the way to ensure that merely authorized users can get access to the information [5]. The two main issues need to be considered regarding confidentiality. Primarily, establishing that the recipient of the data will not transfer these data to other entities and, next, paying attention to the management of data.
- e. Non-repudiation: This is the way of assuring that a task or episode has occurred (and by whom), and it can't be denied in the future. In simple terms, the entity cannot refute the legitimacy of an exact data moved.
- f. Availability: This process guarantees that the required service will remain available anywhere and anytime for the intended users. In IoT, this involves the availability of the entities themselves [6].
- g. Privacy: This is the way to ensure inaccessibility to private info by public or malevolent entities.

### 1.3.1 Security attacks in the Layered architecture of IoT

In IoT, an attack is considered to be an endeavor to abolish, disclose, modify, deactivate, thief or get illegal access to an asset. For instance, the role of cryptographic security protocols is crucial in offering security services for communication across networks. Evidence of a protocol flaw is commonly referred to as an "attack" on a protocol, and it is usually characterized by a sequence of actions conducted by an unscrupulous principal to accomplish protocol security goals through any hardware or software tool [7]. All layers of IoT with possible security attacks have been discussed below:

a) Perception Layer: This layer includes sensors with limited processing power and storage capacity. Following is the list of attacks that are generally noticed in this layer:

- i. Node Capture: The assailants can easily get control over nodes (base node or gateway). Capturing a node not only empowers an attacker to strongly obtain cryptographic keys and protocol states but also to clone and reallocate spiteful nodes in the network, affecting the security of the overall system.
- ii. Denial of Service (DoS) Attack: This assault completely blackouts the framework or network and stops illegal users to get access to it. To do this, the attacker floods the network with a huge number of fake requests, thus over-burden the framework and prevent it to deliver the normal service.
- iii. Denial of Sleep Attack: The denial of sleep attack interrupts the power supply of the node with a major objective to increase the power consumption for reducing the service time of the node. This attack prevents the node from being inactive after transferring the aptly sensed data [8].
- iv. Distributed Denial of Service (DDoS) Attack: It is a modified variant of a DoS attack. The most concerning thing is the ability to use a large number of IoT nodes to transfer traffic collected on the way to the victim server.
- v. Fake Node/Sybil Attack: In this attack, the attacker makes use of counterfeit nodes to generate fake identities. The presence of a Sybil node can compel the entire network to generate incorrect data or even the neighbouring nodes get spam data and lose their privacy. The data can be transmitted to "legitimate" nodes using fake nodes which compel them to expend their energy, which might cause the shutdown of overall service.

In the light of the above-mentioned issues, node authentication is required for the prevention of fake nodes and illegal access [9]. Data encryption is also required to safeguard the confidentiality of data to be transmitted between nodes (end node, gateway, or server). The different node features such as limited power and storage capacity generate the need for mature lightweight security schemes comprising both lightweight cryptographic algorithms and security protocols.

b) Network Layer: It is known as a transmission layer which is utilized to transfer the information between physical objects or sensors and the processing system over secure lines with the help of a communication system. The recognition of various attacks and risks is done on the network layer, which is defined as [10]:

- i. Man-in-the-Middle (MITM): As indicated by McAfee, DoS (Denial of Service) and MITB (Man in the Browser) attacks occurred frequently. The MITM attack is launched in the presence of an SSL (Secure Socket Layer) attack due to which attackers can listen to traffic that is interpreted and both ends of the data are spoofed.
- ii. Eavesdropping/sniffing: In this passive attack, the intruder has the potential for hearing the private communication over the communication link. The significant information related to usernames and passwords, to recognize or configure the node can be extracted by the intruder that results in other kinds of attacks such as fake node, replay attack, etc.
- iii. Routing attacks: Such attacks have affected the routing of the messages or data. The attacker is capable of spoofing, redirecting, misdirecting, or even dropping the packets at the network layer. The black hole, gray hole, wormhole, and Sybil attacks are known as routing attacks.
  - Black Hole: This attack is called a Denial of Service attack [11]. The attacker makes the deployment of the false node which allows all traffic by representing the shortest path. Consequently, all traffic is redirected to the forged node which leads to redirect them to a proxy server or even drop them.
  - Gray Hole: This attack has similarities with the black hole attack. However, only selected packets are dropped in this attack in place of all the packets.
  - Worm Hole: The attacker is capable of generating a connection amid two points within the network in a wormhole attack. For this purpose, the attacker control at

least 2 nodes and insert new forged nodes in the network. When the link is created, the data is gathered from one end through the intruder and replayed to the other end.

- Sybil: In this kind of attack, multiple identities are created by a forged node for controlling the significant part of the model. Simultaneously, the fake node is available in different places in the network. An enormous volume of information is transmitted in the presence of several Sybil nodes in the same network. The normal nodes are denied to use that information in the network [12].

These potential attacks at the network layer result in describing different security requirements such as hop-to-hop encryption, P2P (point-to-point) authentication, key agreement and management, secure routing, and intrusion detection.

c) Application Layer: This layer has direct interaction with the user. When the traditional application-layer protocols are unable to work in the Internet of Things (IoT), several security issues may launch in the application layer due to the absence of international standards in the IoT.

- i. Cross-Site Scripting: It is considered an injection attack. The attacker gains the potential for inserting a client-side script such as a java script in a trusted site viewed by other users in the Cross-Site Scripting attack. Using this way, the contents of the application are changed following the requirements of the attacker and the original information can be utilized illegally through him.
- ii. Malicious Code Attack: This attack is present in the form of a code in any part of the software that can be utilized to cause undesired effects and damage to the system. The anti-virus tools are unable to block or control such an attack. A malicious code attack is capable of activating itself or pretending like a program that required the attention of the user for acting [13].
- iii. Dealing with the Availability of Big data: A large number of end devices are connected to the Internet of Things (IoT) to manage an enormous volume of data. Consequently, an overhead occurs on the application for analyzing this data that affect the availability of the service(s) which are provided by the application.

To meet the security requirements for the application layer, authentication plays a significant role in the protection of the privacy of users in terms of data. Furthermore, an information



security management system must be utilized in resources and physical security information can be managed.

d) Support Layer: The four-layer architecture of IoT sends information obtained from the perception layer to the support layer. The support layer serves two main purposes. This layer approves that information is transferred by the legal users and safe from threats. The next task of this layer is to transfer information to the network layer. The information from the support layer to the network layer can be transferred over the wireless and wired channels. General threats and issues of the support layer are:

- i. DoS Attack: The DoS attack in a support layer is associated with the network layer. In this attack, the assailant floods the network with a huge amount of data. Therefore, the extreme exploitation of system resources depletes the IoT and the user can't get access to the system [14].
- ii. Malicious Insider Attack: This attack originates with an IoT system to access the private user data. An authorized user generally launches this attack to obtain the information of another user. This attack is quite different and complex and needs various schemes to avoid the risk.

#### **1.4 Location Privacy in IoT**

In recent years, mobile technology has grown rapidly prompting the development of various new mobile devices and social networks besides emerging IoT services. The majority of these advances depend on location-based services (LBS) or the applications of LBS. At present, all IoT gadgets and smartphones have powerful computation capabilities as well as integrated Global Positioning System (GPS) modules. There are multiple websites (e.g., Apple Store or Google Play Store) from where users can download various LBS applications. Users can send their identities, location (for example, obtained by the GPS module via localization methods), interests, and other information (such as time, query range) to the LBS server using these applications. Thus, necessary information regarding nearby shopping malls, stores, cafeterias nearby can be obtained.

However, users while leveraging ease or entertainment from the LBS server might get vulnerable to the outflow of sensitive information from personal or IoT devices, risking the loss of privacy. An assailant can obtain more private user information and their identity with

locations and interests based on the LBS queries of a user. For instance, a user often reveals his location close to a hospital while requesting LBS in an IoT device. An assailant can use this information to infer that the user is possibly suffering from some health issues. The distrusted LBS servers contain all information of users, for example, their location at a specific time, the type of queries they put forward, etc. LBS servers to track all types of users or to reveal their data to other parties may use this information. Therefore, the data-driven IoT service, in particular, should devote greater attention to the location privacy of users, to meet the needs for IoT and big data fusion.

Since a massive volume of data is collected and processed from various sources, IoT functions can significantly impact the privacy of users. Furthermore, in the light of the growing trend of collecting more personal and individual data in IoT, multiple issues concerning the influence on the privacy of individuals from a legal point of view arise [15].

Location information has a significant impact on the data managing or processing of the IoT (Internet of Things) which in turn considerably impacts its location privacy. If sensitive location information without the consent of users gets disclosed, the location information as a key element in efficient inventory and supply chains, effective transport models, context-specific mobile applications, and many other IoT systems may propel privacy attacks and destructive outcomes.

#### **1.4.1 Location Privacy Attacks**

The different attacks on location privacy can be classified as position attacks, context linking attacks, multiple position attacks, attacks combining context linking and multiple position attacks, and attacks based on compromising a TTP (Trusted Third Party) element. Figure 2 describes all these attacks on location privacy.

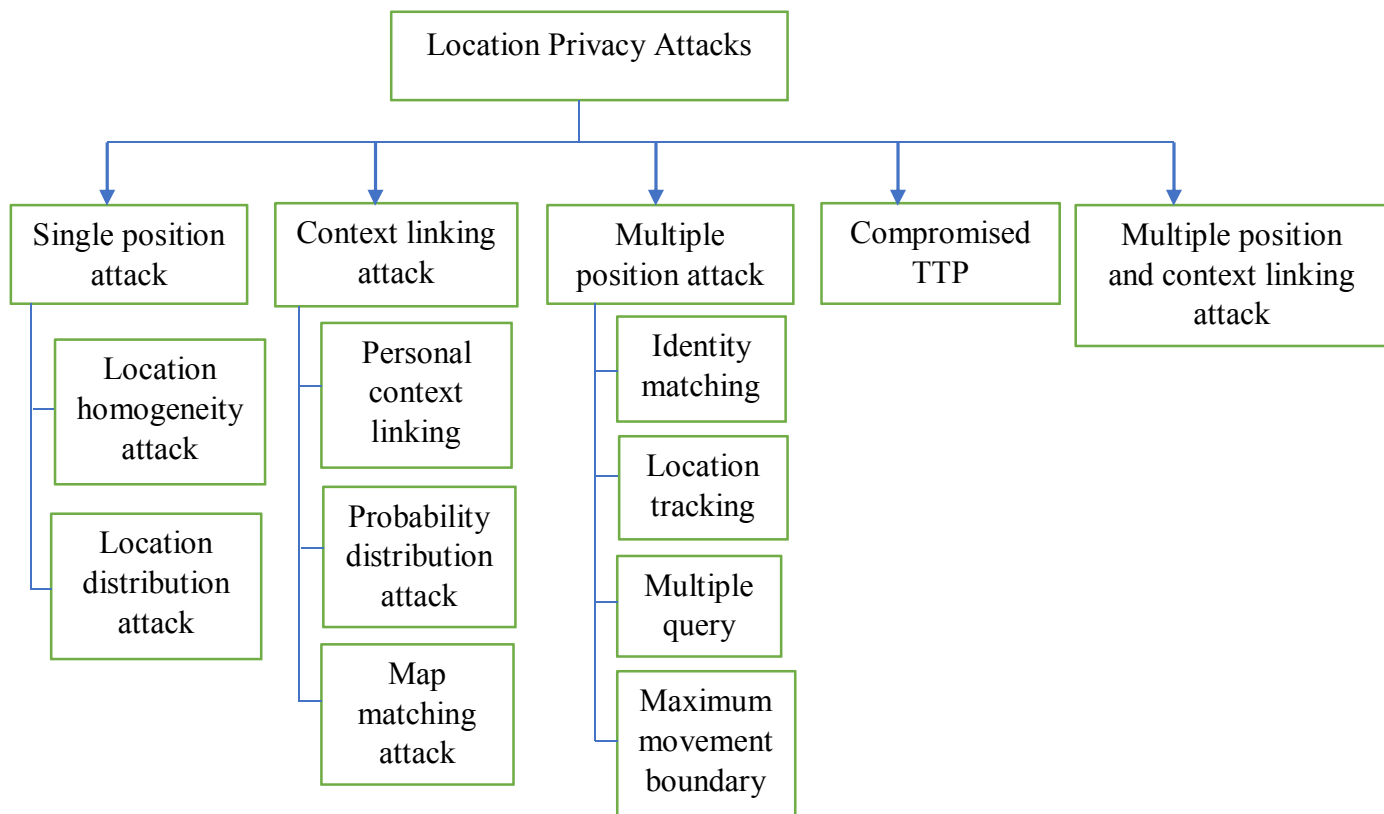


Figure 1.2: Classification of Location Privacy Attacks

Next, we are going to discuss these different attacks in detail.

a. Single position attack: The basic strategy of a single position attack is that the attacker obtains more information about the position or identity of the user by analysing a single query or an update from the user that he does not want to reveal.

- Location homogeneity attack: The attacker can launch a location homogeneity attack against simple  $k$ -anonymity schemes. The attacker examines the location of every  $k$ -cluster member. The location information of all members is disclosed when their positions are nearly the same. The cluster members are distributed over a larger area to protect the position information. An innovative location homogeneity assault reduces the operative area size where users may locate based on the map knowledge [16].
- Location distribution attack: The general idea of a location distribution attack is inspired by the fact that users generally don't disperse homogeneously in space. Some  $k$ -anonymity schemes may get attacked using this idea.

b. Context linking attack: To launch a context linking attack, the attacker uses the context information besides the spatiotemporal information. To reduce user privacy, an attacker may

use the personal context information of the user along with exterior background information, e.g., an office plan, an address book, a map, and more. The context linking attacks can be divided into three types: the personal context linking attack, the probability distribution attack, and map matching:

- **Personal context linking attack:** This attack is launched on the personal context knowledge of every single user, for example, preferences or interests of users. For example, assume a user visiting a pub regularly at a certain point in time makes use of a simple obfuscation approach to secure his location privacy. After this, an attacker can decrease the obfuscation zone to pubs' locations within the obfuscation zone to improve his acknowledged precision of again obfuscated location. An observation attack is a special type of personal context linking attack. The attacker gets access to user information collected by observation in this attack. For example, the attacker after noticing the observed user who is using pseudonyms can retrace all previous locations of the user for a similar pseudonym using a single correlation.
- **Probability distribution attack:** The attacker launches this attack on the collected traffic statistics and environment-aware context information. In this attack, the assailant attempts to determine a probability distribution function of the user location around the obfuscation zone. In the case of non-uniform distribution of probability, an assailant may identify locations where the user is most likely to be.
- **Map matching.** This attack is based on restricting the obfuscation zone to certain locations where users may locate by eliminating all the unrelated areas. For example, a map can be used to remove areas such as lakes from the occlusion zone, effectively shrinking the size of the occlusion region to below the projected size. Attackers can additionally use semantic information delivered by the map for example buildings of interest or type (bars, hospitals, residential buildings, etc.) to further shrink the size of effective obfuscation zone.

c. **Multiple position attack:** In a multiple position attack, an attacker reduces a user's privacy by tracking and correlating many location updates or queries of a user [17].

- **Identity matching:** This attack may be launched on many pseudonyms of a user. The assailant links multiple pseudonyms with the same identity based on identical or similar characteristics to break the provided privacy of the transformed pseudonyms.

- Multiple query attack: Many queries or updates are analysed in this attack. The assailant may launch this attack as a shrink region attack or as a region intersection attack. A shrink region attack may disclose the user's identity and status. Consequently, the assailant constantly monitors updates or queries and related members of the k-anonymity set. An attacker can conclude which user sent the initial update or query when members of the set change. The attackers can use region intersection against location obfuscation approaches for increasing the accuracy of obfuscated locations. As a result, the attacker calculates their intersection using many vague position updates or queries from a user. The attacker can use these interactions to determine the privacy-sensitive areas of the user are or the location of the user.
- Location tracking attack: The general idea of this attack is to use multiple position updates that attackers know. For instance, this attack can be carried out by randomly changing pseudonyms without exploiting the mixed zone. In this attack, the adversary may link spatial and temporal information of subsequent position updates or queries by correlating subsequent pseudonyms, even if an obfuscation mechanism is applied. For example, based on the provided locations of multiple pseudonyms, the assailant may attempt to rebuild a user's movement.
- Maximum movement boundary attack: The assailant triggers this attack by calculating the maximum movement boundary area. This is the area where the user could have moved between two subsequent location updates or queries.

d. Combination of multiple position and context linking attack: An assailant can integrate or use multiple presented attacks or use them sequentially rather than using only a single attack to destabilize the location privacy of the user [18]. For example, an attacker can combine the information of the map restrictions collected by a map matching attack and the limitations of the maximum movement boundary attack to derive the on-going user location.

e. Compromised TTP: A compromised attack from a trusted third party (TTP) is based on the observation that an attacker can gain access to the data stored on the TTP. For example, an assailant may compromise a trusted local server and gain access to the stored data of users. This attack is not considered in TTP-dependent approaches, as it is weak for every approach based on a TTP. To this end, the attack on a TTP is genuine and can't be neglected.

### 1.4.2 Location Privacy Preservation Mechanisms (LPPMS)

Many works are representing state-of-the-art techniques to protect location privacy. Some of these techniques are:

i. Position dummies: The idea of position dummies is concerned with securing the true position of a user by transferring several fake locations (“dummies”) to the local server along with the true position. An important benefit of this scheme is that the user does not need other TTP components and can produce the dummies itself. Nevertheless, creating dummies that cannot be separated from the true user's position is not so easy, especially, when an attacker has more context information, for example, a map, and can track the user for a longer time. A progressive scheme for generating dummies is the Sybil Query approach. This approach is based on assumption that the user has a database of past traffic using which he can create extra dummy positions that can't be differentiated from the true position of the user.

ii. Mix zones: The major concern of the Mix Zone approach is to describe zones termed Mix Zones, where all user locations must be concealed such that the user's position within these zones is not detected. For this purpose, any status updates are not sent within a region. The pseudonyms are changed to match the user identity with other users of the zone to protect user identities when a user enters the Mix Zone. Therefore, an attacker finds itself unable to link various pseudonyms of users even if he successfully traced the entry and exit points of the Mix Zone. The Mobimix scheme implements the idea of the mixed zone to road networks. This scheme considers different reference information that an attacker can use to determine complete trajectories, for example, geometric and temporal restrictions.

iii. K-Anonymity: k-anonymity is a popular and commonly used privacy approach that is not limited to location privacy. This approach guarantees that the target object can be distinguished from the other  $k - 1$  objects in a set comprising  $k$  objects (in our case, mobile users). Therefore, the identifiable probability for the target user is  $1/k$ . The k-anonymity approach to location privacy follows the idea that a user reports a customer [19]an obfuscation area about his status and  $k - 1$  other users' status, rather than his exact status secured by a pseudonym. The local server in this scheme acts as a reliable anonymizer to compute the group of  $K$  users and the obfuscation area according to the positions of recognized users.

iv. Obfuscation and coordinate transformation: Spatial obfuscation schemes attempt to maintain privacy by intentionally decreasing the accuracy of status information delivered from the user end to the location server and then the client. In a standard spatial offset scheme, a user sends a circular region to the LS (location server) rather than the exact user's position. The benefit of this approach is that it provides location privacy without a TTP, as the user can describe the obfuscation area itself. However, this advantage put a bounty that clients don't get precise user position.

v. Cryptography-based approaches: Cryptographic location privacy approaches protect the user positions using encryption. These approaches can inform users when friends are somewhere around without disclosing the status of the current user of the location server. Therefore, it is assumed that every user uses an asymmetric encryption method and shares a secret with each of his friends. Some approaches based on cryptography use the private information retrieval (PIR) method to deliver location privacy. A location server can solve queries without learning or disclosing any information of the query based on PIR. The PCR method is based on the quadratic residual assumption, which suggests that quadratic residuals are difficult to detect in a large overall number of modulo arithmetic for the product of two big primes. Cryptographic schemes generally address the issue of whether it is possible to successfully apply location-based queries e.g., nearest-neighbour queries or range queries over the encrypted data.

vi. Position sharing: This concept is utilized for carrying the queries such as nearest-neighbour or range queries based on the location when the location privacy of the user is protected. This concept is also useful for managing the private position information in non-trusted systems securely [20]. The obfuscated position information is divided into so-called position shares using position sharing at which a position of strictly limited precision is defined with the help of a share. The distribution of these shares is done among a set of non-trusted LSs such that every LS only has a position of limited precision using which calculations can be performed on these shares. The share combination algorithms are implemented to fuse the multiple shares into positions of higher precision for offering the position information related to diverse precision levels to the clients based on the number of accessible shares. Due to the availability of information of limited precision in location sever, a graceful degradation property is comprised in this approach in which an attacker represents

the precision of position that is maximized at a rapid level with the number of compromised location servers.



# Chapter 2

## 2.1 Literature Summary

The Internet of Things(IoT) is defined as the capacity of regular objects to connect with the Internet and exchange data. Different models are suggested in several Internet of Things applications such as smart grids, healthcare systems, and VANET (vehicle ad hoc network). The IoT has become part of daily life and it provides huge market profits. In the healthcare area, associated intelligent sensors or actuators assist the doctors in monitoring their patients and assists the patients who suffered from serious health illnesses in following up and remotely working with their doctors. Recently, healthcare is a rapidly developed domain due to its influences on the total populace. The conventional solutions are unable to satisfy these requirements anymore.

Another IoT application is household automation systems that facilitate consumers for controlling their home system/ appliances for efficacy and savings. A consumer is capable of turning off the water system of the household in the event of hazardous leaks, turning on the AC, or warming up the dinner right before getting home from IoT devices to depend on personal information for accomplishing their tasks. But, various interconnected devices generate this data due to which preservation of full control over this information becomes challenging. The issue has occurred when transparency is absent. The privacy breach of personal data in the Internet of Things environments becomes famous among the research community. The resource-constrained IoT devices are not able for encrypting or decrypting the generated data, due to which it attains vulnerability against an attack by an adversary. Another privacy issue is related to the location of privacy which assists in predicting the location of IoT devices. A major privacy issue is the protection of the usage pattern of users for some generated information through IoT devices.

This paper emphasizes IoT data and location privacy in the healthcare domain. It is essential to protect the data and location privacy in IoT systems by protecting the query privacy while transmitting, processing, and searching the answer. This makes the system robust to deal with inference attacks. A system is required for tackling the heterogeneous platforms and authentication problem. The time response of the system is mitigated for the query answer for acquiring the result from a cloud database. Therefore, the way to warn the privacy of the user is defined based on employed case scenario description initially. Afterward, the potential

privacy threats are analyzed in this framework for recognizing a set of privacy requirements for tackling the privacy risks. These requirements help in guiding the future design of an efficient privacy solution for IoT users.

### IoT Use Case Scenarios

Data and location privacy are useful in protecting the privacy of the Internet of Things. The IoT devices are connected to the Internet for communicating and exchanging information. Therefore, the data or location privacy of these devices may be violated. An individual is careless in the event of the historical backdrop and can record each second with sub-meter accuracy at that point of observing things unexpectedly. Patients at an AIDS testing center probably have not required their developments which are uncovered to the area mindful applications in their working environment or bank.

### Client-Based Scenario

Figure 1 represents that the privacy of users of the Internet of Things could be easily threatened. IoT user is capable of sharing its location and data using IoT devices. An attacker can track the locations of the user, gather sensitive data, employ the identity of the user and build a malicious profile about the user. This malicious profile contains sensitive individual data which is maltreated for burglary, blackmail, or mugging later on. The serial queries regarding the same user/patient are tracked by the attacker for gathering the sensitive data of the users whose extraction is done from the travel histories, relations, and the similarities among the locations and launch the attack.

### Server-Based Scenario

Figure 2 represents the server-based scenario. The server is utilized to implement the protection technique whereas the major task of IoT users is to send a query. Thus, this approach assumed that the server of the Internet of Things is reliable. The server is played the role of a malicious party. The severity of this scenario is that the attacker has the potential to access information about the IoT users, their routes motion, and the details of their preferred locations. Consequently, the users want to know whether an attacker has compromised an IoT device. Generally, users are lack of deep understanding of working IoT devices or interacting with the external entities over their network. To illustrate, an attacker can

compromise the remote server, enable them to steal data that the device has transmitted, or send the device erroneous data or command due to which the device is misbehaved. Moreover, the software is upgraded by the attacker which enables the installation of their software on the device and launching the attack on other devices in LAN or on the Internet. This type of attack is harmful as it is susceptible to detect or notice such passive monitoring of their networks by the users.

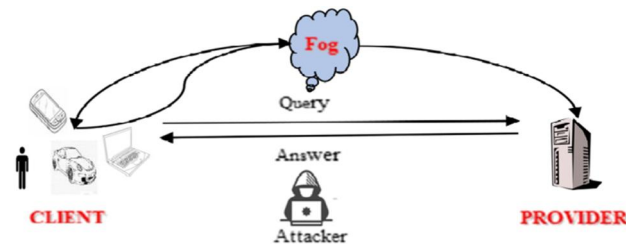


Figure 2.1. Attacker capturing the data traveling from/to the server

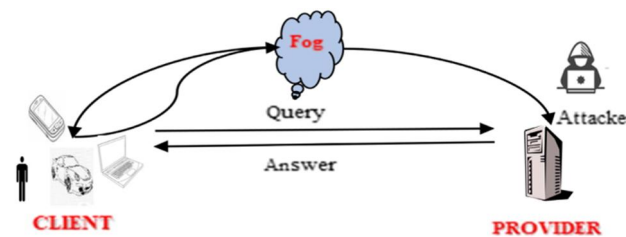


Figure 2.2. A server acting as a malicious party

## MIDDLEWARE CHALLENGES

Middleware is an appropriate solution for IoT corresponding to its distributed components due to their capacity of complying with various requirements in such environments. Various middleware architectures are suggested for dealing with some of the deliberated challenges in an IoT environment. These challenges have resulted from the attributes of IoT infrastructure and application as:

### Infrastructure Challenges:

**Interoperability:** All-inclusive availability and the capacity of exchanging information among inside portions and with the outside world are called interoperability. This test is challenging for IoT middleware as various heterogeneous objects will impart and trade data together.

Maintainability and extensibility: It is the potential of adjusting the framework and helpfully broaden it.

Abstraction provision: A perfect Middleware for the insightful condition has provided the deliberations at numerous levels. To illustrate, heterogeneous gadgets, interfaces, information stream, physicality, and improvement process are comprised in this approach.

## B. Applications Challenges

Availability or Multiplicity: To access the administration's and data constantly, an IoT middleware must ensure various administrations and information sources.

Reliability: An IoT middleware is often operational even in case of failures. The approval of each portion of middleware is essential for accomplishing the elevated level framework unwavering quality such as correspondence, information, advances, and gadgets from all layers.

Real-time: For some IoT applications such as transportation or medicinal services, the data is transmitted. Deferred data in such applications may find inadequate, now and again may risky. For example, a postponed warning of a fall checking application is utilized for promoting the demise of the individual.

Security and Privacy: It is a potential model for adapting to malevolent assaults from outside or inside the framework. The firewalls are introduced; validation and approval procedures are constructed and encryption is employed to enhance security. Various gadgets can communicate with one another and various data is exchanged among them. This data is available at the private and individual level on daily basis life. Therefore, trust, security, and protection are some challenges which are occurred earlier in IoT middleware arrangements.

## OUR PROPOSED PRIVACY PROTECTION APPROACH

The scenario of the suggested approach is explained in this section. This technique is defined and it's a way of utilizing the fog computing model for enhancing the efficacy and effectiveness of location privacy-preserving in IoT environments.

### A. Our Proposed Approach (Fog Computing in IoT)

Different suggested techniques have some limitations such as usage of high bandwidth and timeliness issues which cause serious privacy issues. This approach is focused on preserving the location and privacy in the IoT scenario. Fog computing is presented as a prospective solution as it has distinctive attributes including location-awareness. An effective system is constructed to define fog computing. This system can fulfill the needs of preventing the privacy of IoT devices.

Web services technology is employed for supporting interoperable device-to-device communication over the Internet. This approach emphasizes developing a system for achieving full privacy protection, for LBS users for which location privacy is protected. Fog computing is implemented for alleviating the bandwidth that is useful to communicate and transmit the data amid the smart sensors and the cloud. Initially, no location can be updated in a mixing zone when the objects are moved. Subsequently, another pseudonym is employed by the user while leaving one mix zone to another. Therefore, the perturbation algorithm is deployed with static devices namely home appliances that are responsible for inserting artificial noise to the location of the user. The pseudonym framework is utilized later on for concealing the identities of the users from the applications which not used them and an intruder who has the potential for exploiting vulnerabilities so that the personal data can be accessed. The fog computing prototype aims at lessening the data volume and traffic to cloud servers, diminishing the latency, and enhancing the QoS (quality of service).

### B. Architecture Technique

The strategy introduced in this work includes fog nodes, IoT devices, and the cloud, as illustrated in Figure 3. Let the job of each fog node is to serve a set of IoT devices. It is easily possible to generalize our strategy based on the fact that the fog node is responsible for moving objects with GPS or stationary objects that include responsive data in the form of medical data. In our plan, we create a shortlist using a forwarder and schedule its items based on their priority. It also validates whether an object belongs to the fog group or else send to appropriate fog for arranging order based on their preference and to cope with the challenge of starvation. Afterward, the back-end cloud makes use of the K-anonymity scheme where the LBS server behaves as an anonymizer. concerned with the idea of sharing data with other parties while limiting the ability to link data to identify an individual. Kanonymityis based on

the idea of data tradeoff with other parties and limits the capacity to link data for identifying a particular object.

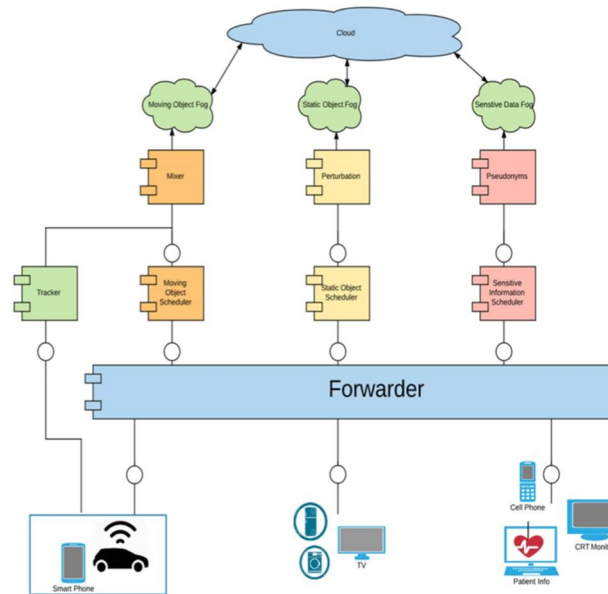


Figure 2.3. Our Proposed Web Services Architecture

## 2.2 Literature Review

Chunyang Yin, et.al (2018) suggested a location privacy protection technique in which differential privacy constraint was satisfied for protecting the location data privacy and increasing the utility of data and algorithm in Industrial Internet of Things [21]. For the higher value and lower density of location data, the utility was integrated with the privacy and a multilevel location information tree technique was constructed. In the end, the Laplace scheme was adopted for the insertion of noises to the accessing frequency of the selected data. The results obtained in the theoretical analysis and the experiments revealed that the suggested approach was capable of obtaining the enhancements concerning security, privacy, and applicability.

Zainab Waleed Hussien, et.al (2020) established an MSCPL (Multi-Sinks Cluster-Based Location Privacy Protection) technique in WSN (Wireless Sensor Network) for the Internet of Things in which the network was partitioned into clusters [22]. One CH managed each cluster. The random fake packets were transmitted in a loop by cluster head (CH). Afterward,

a dynamic routing technique was implemented to send the real packet to the CHs of the neighbor so that the attacker was confused from backtracking the real packet. In this way, the actual location of the source node was not revealed by the attacker. The evaluation was conducted using two metrics like energy consumption and delay.

Amani Abuladel, et.al (2020) developed a generic model for the Internet of Things (IoT) data and location privacy in which the entities and interactions were defined among them [23]. Afterward, a set of general privacy requirements which concerned data and location privacy was recognized by analyzing the potential privacy threats. The fog computing was exploited with the obfuscated method due to which it became difficult for the attacker for detecting the reallocation of the user through which the end-users were facilitated to secure their potentially sensitive data before sending it to the cloud. The developed model was adaptable for enhancing location privacy and performance in comparison with other methods.

Peipei Sui, et.al (2017) emphasized on protecting the privacy for location trajectory data whose gathering was done using intelligent transportation systems in IoT [24]. A novel trajectory anonymity model was put forward to characterize the degree of correlation of parking locations with individuals in inaccurate way. For this, the concept of LF-IUF (Location Frequency-inverse user frequency (LF-IUF)) was utilized. Thereafter, an anonymizing technique was employed for replacing the parking locations with the help of a k-correlation region. At last, a series of experiments were conducted using real-world data sets. The experimental results demonstrated that the presented approach was efficient.

Sami Saad Albouq, et.al (2020) recommended an approach known as DOA (Double Obfuscation Approach) in which integrates Obfuscation technique was integrated with TTP, and their capabilities were improved with the deployment of two technologies namely Caching and Mix-Zone [25]. The fog nodes were executed for enhancing the performance of the system and the privacy of the user. The responses of every query were divided into 5 parts. Consequently, the processing time of the results was diminished and the overall accuracy was boosted at which the user was facilitated to choose the most appropriate parts based on current location. The simulation outcomes depicted that the recommended approach performed well for protecting location privacy and enhanced accuracy.

Weipeng Jing, et.al (2019) presented a differential privacy technique for protecting the location privacy of the user in IoT [26]. Initially, a data query framework was introduced

based on a three-layer communication link structure. Subsequently, the edge node was considered as the central server and the location privacy was protected using the presented technique. Lastly, the data loss that occurred in the process of protecting the location was mitigated with the implementation of linear programming using which the optimal location fuzzy matrix was chosen. The results indicated that the presented approach was useful for protecting location privacy and alleviating the data loss as compared to other techniques.

Donghe Li, et.al (2019) designed a novel reliable online double auction system in which multiunit energy trading was carried out among EVs (electric vehicles), routing optimization was adopted to charge the EV charging and location privacy was protected [27]. Various significant properties and location privacy surety were obtained using the designed system. The results of the experiment validated that the designed system performed better for protecting location privacy.

Mingming Guo, et.al (2018) introduced a novel query-feature-based inference attack with a scenario on a real-world data set [28]. A strong property was obtained along with the differential privacy theory by describing the Indistinguishable Feature-Inferred Location/Grid and Probabilistic k-effectiveness. A new randomized algorithm was developed for dealing with the location privacy attack. Different parameters such as entropy and recourse cost were considered for carrying out the simulations and analysis. The simulation results represented that the introduced system was efficient and effective.

Guangjie Han, et.al (2018) projected a KCLP (k-means cluster-based location privacy) technique to protect the privacy of location for Internet of Things (IoT) [29]. The source location was protected using fake source nodes so that the function of the real sources was simulated. After that, the sink location privacy was protected with the execution of fake sink nodes and a specific transmission pattern. A k-means cluster was deployed for generating the clusters and fake packets which had to be undergone the area for enhancing the safety area. The results revealed that the projected technique was effective for maximizing the safety time and lessening the delay at a lower cost in energy consumption.

Shihong Zou, et.al (2020) investigated an efficient CrowdBLPS (blockchain-based location-privacy-preserving crowdsensing). First of all, the concept of blockchain was put forward [30]. After that, the data sensing quality was enhanced and the worker privacy was protected using a two-fold technique in which the initial phase was pre-registration and the second one



was the final selection phase. At last, the Ethereum public testing network was applied to execute a prototype. The results of the experiment indicated that the investigated system was feasible, applicable, and reliable.

Thu Le, et.al (2018) discussed those novel properties were presented through the Internet of Things [31]. A technique was constructed to protect location privacy. The implementation was done easily in low-capability user devices and run in a distributed IoT system without a trusted server. Every user was capable of storing a portion of the map data and sharing the information with the other user devices so that an obfuscated region having only accessible locations was created. The practicality of the constructed technique to develop a location-protection region was proved in testing. The results exhibited that the constructed technique was efficient and practical.

Mengmeng Yang, et.al (2018) intended a data release system for crowdsensing methods in which differential privacy was utilized to protect the locations of workers [32]. The partitioning technique was planned based on worker's density and non-uniform worker distribution was taken into account in this system. Furthermore, a geocast region selection technique was presented to assign the task to balance the success rate with worker travel distances and system overheads. The experimental results depicted that the intended technique ensured strict location privacy as well as enhanced the performance effectively.

Shengke Zeng, et.al (2021) emphasized location awareness in IoT [33]. The deniability of authentication was adapted for preventing leakage of the location while connecting the IoT devices with the edge nodes. A two-user ring signature-based efficient deniable authentication was developed. The presented technique was robust enough for allowing the fixed edge equipment to accept the legal end devices. Thus, the inherent location risk was handled using this technique. The results demonstrated that the presented technique reduced the computational cost by 14.696%.

Guangjie Han, et.al (2018) devised the CASLP (Confused Arc-Based source location privacy) protection method in Wireless Sensor Networks for Internet of Things (IoT) [34]. The scope of the transmitting path was maximized with the initialization of random walk through the source in a given direction. Thereafter, the convergence of the devised method was maintained when the next relay nodes were chosen by the nodes in a particular range. Finally, the privacy of source location was enhanced for which arcs were focused from numerous

rings around the sink for generating a new closed loop. The results indicated that the devised method assisted in decreasing the delays and energy consumption at a lower cost of safety time in contrast to other techniques.

ShathaAlarabi, et.al (2018) suggested a double level-based scheme for protecting the location privacy of users of the Internet of Things (IoT) [35]. The server-level was adopted which included the installation of an anonymity-based component on the server for protecting the query. At the machine level, the privacy of the location of users of IoT was protected using a transform method. It was analyzed that the suggested technique outperformed the earlier techniques. The future work would aim at simulating the suggested scheme to protect the location of IoT users completely.

Wei Wu, et.al (2020) introduced a zk-PoL (zero-knowledge proof of location) protocol for protecting the location privacy of the user in IoT [36]. This protocol enabled the user to select the significant information so that the server was represented for protecting the hierarchical privacy. The results of the evaluation demonstrated that the introduced protocol contained superior security for providing resistance against attacks. Additionally, the computational efficiency was not dependent on the input metrics and the zk-PoL was also suitable for delay-tolerant location-based services (LBSs).

Hao Wang, et.al (2018) developed an SLPRR (source location privacy protection scheme based on ring-loop routing) to protect location privacy in the Internet of Things [37]. A confounding time-domain transmission was presented for transmitting the real packets so as the backtracking time of the adversary was maximized. Moreover, the location privacy of the source was protected using fake packets, phantom nodes, and a confounding ring. This approach was computed in the experimentation. The simulation outcomes indicated that the developed technique was capable of prolonging the safety time without compromising the duration of the network.

Yan He, et.al (2020) formulated a strong identity verification system for ensuring the authentication security of the system at first [38]. A novel location privacy protection system was planned based on the privacy proximity test problem later on. The ring signatures were utilized to keep the location privacy of the user confidential and for preventing collusion among the positioning nodes after the execution of the positioning detection protocol. At last, the relevant data requirements of service providers were fulfilled and the leakage of the user-

related private data was prevented using homomorphic encryption. The formulated system assisted in keeping the information of the user secret as well as satisfying the needs of a service provider.

Defeng Li, et.al (2020) recommended a location chain storage system for devices of the Internet of Things based on blockchain and simulated the system [39]. The number of transactions in the block had affected the time of the system that offered the location services. The network nodes were computed in the blockchain to set the number of transactions in the block. The outcomes validated that the recommended system had the potential to protect the device location information in IoT and understood the location information that was shared under the premise of ensuring that user privacy was confidential.

Yu He, et.al (2019) established an SRR (sector-based random routing) method for dealing with the issue of source location privacy (SLP) and mitigating the energy consumption [40]. This method was exploited to transmit the data packets to random phantom sources whose location was established in different sectors and distribution was done in all the directions for reaching the sink node. Additionally, the routing strategies were handled and the energy consumption was diminished using a concept of a hop threshold. The results of experiments exhibited that the established method was efficient to protect privacy and mitigating backtracking and direction attacks.

Guangjie Han, et.al (2017) intended an SLP (source location protection) protocol based on dynamic routing for protecting location privacy [41]. A dynamic routing technique was presented to increase the paths to perform data transmission. Initially, an initial node was selected from the boundary of the network at random using the intended protocol. The outcomes acquired in the experimentation depicted that the intended protocol was capable of preserving the SLP and addressing several privacy disclosure attacks without any impact on the duration of the network.

Gang Sun, et.al (2016) suggested an approach named ADLS (Attack algorithm based on dummy-location selection) for protecting privacy to test the security of the Internet of Things (IoT) [42]. The computational costs and diverse privacy needs of various users were taken into account using this approach so that the location privacy of users was protected. The outcomes of the experiments demonstrated that the suggested approach was effective. In

addition, this approach provided a higher probability to recognize the reallocation of users from the selected dummy locations in the DLS algorithm.

Rômulo Meira Góes, et.al (2018) introduced a discrete-event-control-theoretic method for opacity enforcement in which the output events were inserted and deleted to preserve privacy in an indoor environment at which IoT devices were implemented to monitor the users [43]. An obfuscator of user trajectories was planned in a grid model with obstacles. The evaluation revealed that the introduced method was able to protect the location privacy in an indoor environment where an obfuscated position was disclosed in real-time using which the visits of a user to secret locations were concealed. Moreover, this approach was proved practical.

Gang Sun, et.al (2016) presented a location label-based algorithm for preserving location privacy in which three key protocols were comprised known as the user requests aggregation protocol, the pseudo-ID exchange protocol, and the enhanced PLAM protocol [44]. This algorithm was quantified by conducting the experiments. The experimental results exhibited that the presented algorithm had performed better than the traditional techniques. This algorithm was assisted in protecting the privacy of LBS (location-based service) to keep the locations of users of the Internet of Things (IoT) private.

Mengmeng Yang, et.al (2018) developed a blockchain privacy-preservation crowdsensing system for dealing with the issues related to privacy [45]. This system assisted in protecting the privacy of worker locations as well as maximizing the success rate to accomplish the assigned task. A rewards-based task assignment procedure was comprised in this system. The identity information regarding users was concealed using the anonymized attributes of blockchain technology. The experimental outcomes indicated that the developed system provided superior performance to protect the privacy of locations of workers.

Lina Ni, et.al (2018) projected an RPAR (repartition anonymous region) technique to protect location privacy [46]. The central anonymous location was employed to reduce the traffic from the anonymous server to the LBS (located based service) server when the privacy of the user location was protected. This technique assisted in splitting the anonymous region into various sub-regions, replacing the real locations of users with the central location, and performing a repartition for tackling the remaining users after segmenting the anonymous region. The future work would focus on the protection of location privacy in the scenario of the dense region.

Ahmed Mohammed Ibrahim Alkuhlani, et.al (2016) established a secure strategy to protect the privacy of the source node location with the implementation of routing modification of ELB (energy-awareness load balancing) protocol by selecting a random path in multipath routing fashion [47]. Consequently, the path diversity was obtained with the best energy consumption. Every packet was transmitted at random in a diverse direction. Furthermore, the privacy preservation was enhanced using pre-defined tunnels of M intermediate hops to hide the original path of the packet. This technique had the potential to protect the source node location from backtracking through the attackers.

Mohammad Yamin, et.al (2020) investigated a novel method called SPF (Swapping of Peers and Fogs) to protect the location privacy of users from SP (Service Providers) [48]. The attributes of fogs and smart dummies were applied to attain significant enhancements to the level of preserving the identity of users using which personal information of user was easily extracted. The simulations were conducted on comparing the presented technique with the existing approaches. The results depicted that the investigated method was efficient and effective. At last, the association of this method with connected street systems in smart cities was also described.

Mahmoud Elkhodr, et.al (2013) recommended a context-aware adaptive technique for general devices to protect the location privacy throughout an agent in the Internet of Things (IoT) environment at which the users employed general devices to access the LBS (location-based services) [49]. Furthermore, the privacy preferences of users and object operators were also considered in this technique. The major objective of this technique was to generate and deploy an agent for preserving the location privacy concerning the requested network-based services. The experimental results proved that the recommended technique was efficient and effective.

Ruchi Vishwakarma, et.al (2019) intended a honeypot-based method in which ML (machine learning) schemes were utilized to detect the malware attack [50]. The data obtained from the Internet of Things (IoT) was applied as a dataset to train the intended ML model efficiently and dynamically. The Zero-Day DDoS (Distribute Denial of Service attacks) were tackled using this method. This approach was computed by performing its comparison with other models. The future work would emphasize expanding this approach to the next level at which the open challenges or issues would be discovered in real-time scenarios.

VijenderBusi Reddy, et.al (2019) designed a trust model for the Internet of Things (IoT) so that different attacks such as packet dropping, badmouthing and collusion attacks were alleviated [51]. A new similarity framework was put forward for computing the recommendation credibility whose deployment was done as a weight in indirect trust computation for lessening the impact of false recommendations. The malicious nodes were considered to quantify the designed model. It was observed that the designed model was capable of recognizing the malicious recommendations.

Fathima James, et.al (2019) suggested the finite state automata-based attack system for recognizing the smart home-based security attacks [52]. Later on, a risk management model was put forward for computing their effect so as the crucial attacks that occurred on the smart home were lessened. At last, the typical attack behavior and presented model were analyzed and their efficiency and practicability were represented. The suggested system had the potential to improve user privacy and to realize the potential risks in smart homes based on Internet of Things (IoT) environments.

S. Sridhar, et.al (2017) formulated an Intelligent Security model for the devices of IoT (Internet of Things) [53]. The E2E (End-To-End) devices assisted in protecting the IoT service gateway, and sensor nodes having lower power were secured using lightweight asymmetric cryptography. Lattice-based cryptography was adopted to secure the broker devices and the cloud services. The asymmetric key was encrypted for sharing the session key among the nodes. Afterward, the message was transmitted using a session key. Thus, the formulated model protected the system for addressing DDoS attacks and eavesdropping.

Xupeng Luo, et.al (2019) devised a moving target defense (MTD) architecture for defending the scanning-based attacks in the initial stage with the help of SDN (software-defined networking) [54]. For this, the IP addresses of IoT (Internet of Things) devices were mutated due to the maximization of uncertainty and attack surface. Subsequently, a DDoS attack mitigation technique was presented through SDN-based honeypots which were impersonated the IoT devices for increasing their security. The results of experiments validated that the devised architecture was adaptable for detecting and diminishing the attacks of scanning and SYN flood.

Syeda Mariam Muzammal, et.al (2020) introduced a conceptual design known as SMTrust, to protect the routing protocol in the Internet of Things (IoT) based on the mobility-based trust

parameters [55]. This approach emphasized resisting various attacks such as the black hole, grey hole, rank, version number attacks, etc. The introduced approach was more scalable and accurate while detecting the attacks in comparison with the traditional trust systems. This approach was proved as a secure routing algorithm for ensuring confidentiality, integrity, and availability among the sensor nodes under the routing process in IoT communication and networks.

Seungyong Yoon, et.al (2017) constructed the functional model of a remote security management server for enhancing the security and safety of devices in IoT (Internet of Things) [56]. Its server was useful for providing and managing a variety of security functions integrally and systematically. Hence, this model led to prevent several intrusion incidents which were taken place in IoT and lessen the damage. For this, the countermeasures were taken quickly and efficiently in this model during the occurrence of a severe attack. It was analyzed that the constructed model kept the system secure and safe effectively.

S. Kalyani, et.al (2018) projected the IDS (Intrusion detection system) for Internet of Things (IoT) that detected the rank attack and attacker node [57]. These attacks and attacker nodes were recognized based on information about the location node rank, neighboring node rank and its respective rank value using this system. This system had the potential to secure the IoT network and for preventing the network from some attacks. The projected system efficiently detected the attack.

Kashif Naseer Qureshi, et.al (2020) developed a new and secure system to detect the occurrence of security threats in IoT (Internet of Things) networks [58]. Various attacks namely hello-flood attack, VN (version number), sinkhole attack, etc. were detected using this system. Several metrics including accuracy, throughput, and E2E delay were considered to quantify the developed system. The outcomes depicted that the developed system was appropriate for dealing with attacks that occurred in IoT.

David Airehrour, et.al (2018) intended SecTrust-RPL system in which SecTrust (Secure Trust) was embedded into the RPL routing protocol for protecting the system from Rank and Sybil attacks [59]. A trust-based method was employed in this approach for detecting and isolating the attacks during the optimization of network performance. The simulation results revealed that the intended system was efficient and resilient. This system outperformed the others while detecting and isolating the attacks.

Fatima-tuz-Zahra, et.al (2019) established a model to detect the rank and wormhole attack with the implementation of ML (machine learning) methods. The issue of detecting these attacks was resolved after their occurrence in an IoT network [60]. The attacks such as a joint attack having a high probability of occurrence were handled using this model. Different ML methods were put forward to select the suitable technique so as the promising outcomes were generated. Furthermore, the high-performance, efficient and effective solution to tackle the routing attacks was developed further for RPL-based Internet of Things (IoT) networks.

Dong Seong Kim, et.al (2020) emphasized discovering the Mirai malware and its variants and investigated a new graphical security framework for capturing the malware spread [61]. The effect of malware behaviors on the compromise rate was identified concerning the number of infected nodes. Afterward, various scopes of system models and attacker models were utilized and the comparison of their results was done in diverse scenarios. In the meanwhile, novel security parameters were generated for revealing the security level of networks in the presence of botnet attacks and computing their efficacy to mitigate the spread of malware in the Internet of Things (IoT).

Daemin Shin, et.al (2019) presented a secure route optimization protocol for DMM-based smart home systems in IoT [62]. The route optimization was initialized and handover stages were comprised in this protocol. This protocol was planned based on performing mutual authentication, key exchange, and protecting privacy. Two security tools namely BAN-logic and AVISPA (Automated Validation of Internet Security Protocols and Applications) were employed to determine the security of the presented protocol. The results of comparative analysis exhibited the superiority of the presented protocol over the conventional protocols.

Chang Choi, et.al (2019) suggested a suitable power IoT security service model [63]. In addition, a security method whose implementation was possible in such an environment was put forward. For the experimentation, a smart meter, a power system device was applied to generate the attack context scenarios whose occurrence was found extensively. Thereafter, the paths of attacks were determined using the inference rules for every attack phase. Consequently, the suggested model generated promising results for detecting the attack of a higher level based on the inference rules.

Ahmed Yar Khan, et.al (2020) developed a lightweight technique to detect insider attacks. This technique had the potential to detect the anomalies that occurred from the incoming data



sensors in resource-constrained Internet of Things (IoT) environments [64]. The malicious insider attack was detected using the Levenshtein distance method for ensuring that the critical and data of devices were secured in the IoT environment. The outcomes indicated that the accuracy obtained from the developed technique was found higher than the existing methods. In addition, this technique was able to enhance the accuracy while detecting the attack, lessen the FPs (false positives) and computational overhead.

ZieEyaEkolle, et.al (2018) introduced an approach for the security of IoT networks with the implementation of a hybrid security strategy [65]. The grammar-based filtering method was employed for DPI (deep packet inspection) and a clustering algorithm was presented for detecting the attack in an unsupervised manner to establish a security policy against Distributed Denial of Service (DDoS) attacks in the Internet of Things (IoT). This approach was quantified practically in the experimentation and its outcomes were put forward. In the future, the introduced strategy would be optimized to filter and detect DDoS attacks effectively.

Yan Naung Soe, et.al (2019) projected a detection system in which a publically available dataset was utilized for detecting the attacks [66]. To achieve this, ANN (Artificial Neural Network) technique was deployed. However, the Bot-IoT dataset was executed for detecting the DDoS attack and addressing the issue of data imbalance due to the availability of the least amount of benign data and the huge amount of attack data. Thus, SMOTE (Synthetic Minority Over-sampling Technique) was implemented to deal with the issue of imbalanced data so that a DDoS detection system based on ML was deployed.

Jalal Bhayo, et.al (2020) established an SD-IoT-based model using which security services were offered to the IoT network [67]. A C-DAD (Counter-based DDoS Attack Detection) application was designed based on counter values of diverse network metrics for detecting the DDoS attack effectively. The results proved that the designed algorithm performed more effectively using SDN. In addition, the established model was adaptable for detecting the attack efficiently in the least time and lower consumption of CPU and memory resources.

Ridwan Hadiansyah, et.al (2020) designed a technique of trustworthiness management based on the authentication and trust value in IoT [68]. The testing conducted on three scenarios presented the potential of the system to detect the Sybil attack rapidly and accurately. This system took only 9.3287 seconds for detecting the Sybil attacks and an average time of

around 18.1029 seconds was utilized for detecting the intruder object in the system. The results exhibited that the designed technique provided 100% accuracy.

Liu Junjiao, et.al (2020) intended a new method known as SHADOWPLCS to detect industrial process control attacks [69]. Initially, the PLC control code was analyzed in an automatic manner using this method. Subsequently, the attacks were computed by extracting the key metrics of the PLCs. This method assisted in detecting the behavior of attack in real-time active communication. Two Siemens S7-300 PLCs available on a gas pipeline network platform were applied to evaluate the performance of this method. The results of experiments validated that the intended method was efficient for detecting the process control attacks in real-time without any impact on the normal operations of PLCs. The accuracy attained from the intended method was calculated at 97.3% that was superior to other schemes.

Nagarathna Ravi, et.al (2020) devised a new system recognized as LEDEM (learning-driven detection mitigation) for detecting DDoS (Distributed Denial-of-Service) attack for which the semi-supervised ML algorithm was utilized [70]. A testbed was utilized for testing this system and its results were compared with existing solutions. The devised system was capable of resisting the DDoS attack. The results showed that the system attained 96.28% while detecting the attack. The future work would emphasize implementing the ML Techniques for enhancing the precision to detect the attack.

James Jin Kang, et.al (2019) recommended a new approach in which a hybrid routing system, having appointing dedicated nodes to enforce the routing amid IoT devices and users with minimal intervention and workload to the network, was deployed [71]. The suspicious nodes and networks were avoided for determining the secured paths in the network. The stability was offered for travel times for a TTS (trusted time server) so that the accuracy of estimated travel times was enhanced. The packet was inspected for the security checks in this approach. It was analyzed that the recommended approach was applicable to maximize the security of IoT networks for which it detected intruders in real-time.

Mohammad M. Shurman, et.al (2019) suggested a hybrid design of signature-based IDS and anomaly-based IDS [72]. This design focused on improving the IDPS (intrusion detection and prevention systems) so as any DoS attack was detected at the initial phases. For this, the network packets were classified based on user behavior. The simulation results demonstrated the efficiency of the suggested design for detecting the attack in primary phases. This system

was enhanced further for which the FPs (false positives) were mitigated at an earlier stage for a suspected DoS attack in the Internet of Things (IoT).

Giuseppe Potrino, et.al (2019) investigated a novel IoT security system in which a secured MQTT (Message Queue Telemetry Transport) protocol was implemented to exchange the data amid sensor and actuator nodes [73]. This system was designed based on HIDS to lessen the DoS attacks on fog nodes. To achieve this, some packets were accepted with limited frequency and buffer fullness was monitored to grant topics priorities. An event-driven simulator was applied to authenticate the investigated system. The results of the simulation revealed that the investigated system was performed better for dealing with DoS (Denial-of-Service) attacks.

Yusuf Muhammad Tukur, et.al (2019) formulated a new security algorithm for protecting the IoT system against DoS (Denial-of-Service) attacks at the application layer in the Internet of Things. It had multi-layer security architecture for protecting the whole IoT system [74]. This quantification of this algorithm was done against IoT security and privacy requirements. The formulated algorithm provided a superior level of security and assisted in checking the malicious access and DoS attacks.

AKM Jahangir Majumder, et.al (2020) focused on planning and developing a CPS (Cyber-Physical System) for detecting IoT security threats through a smartphone [75]. The deployment of device power consumption rate was suggested in the presence and absence of attack for predicting and detecting a security threat. Thus, the LR (logistic regression) method was implemented. A sample of smart IoT devices was applied with diverse test scenarios to carry out the experiments on the device in an idle state, DDoS attack, and Active with a MitM (man-in-the-middle) attack. The results exhibited that the developed system was efficient for detecting a potential security threat with an average accuracy of around 74% and a device high of 85%.

Ramesh Paudel, et.al (2019) introduced a new GODIT (Graph-based Outlier Detection in Internet of Things) technique in which smart home IoT traffic was demonstrated as a real-time graph stream [76]. The graph data was processed effectively and the DoS (Denial-of-Service) attack was detected in real-time. A real-world data collected from IoT-equipped smart home was exploited to conduct the experiments. The experimental results validated that

the introduced technique provided more effectiveness in contrast to the conventional ML techniques.

Mujahid Mohsin, et.al (2016) designed the IoT SAT methodology which was a formal model to analyze the security of IoT (Internet of Things) [77]. This approach was utilized to model the generic behavior of IoT systems based on device configurations, network topologies, user policies, and IoT-specific attack surfaces. Thereafter, the resilience of the system was evaluated against the potential attacks and threat vectors and the specific attack methods were recognized that assisted in obtaining higher-level objectives. The results indicated that the

the designed methodology provided scalability to reveal the complex attack vectors of Internet of Things systems.

Christiana Ioannou, et.al (2019) focused on implementing an SVM (Support Vector Machine) anomaly detection system for detecting the abnormalities in IoT (Internet of Things) [78]. A normal profile hyperplane was generated based on benign and malicious local sensor activity using SVM. The accuracy obtained from the presented system was counted 100% on unknown data gathered from the similar network topology and it was found 81% on an unknown topology.

# Chapter 3

## Problem Formulation

### 3.1. Problem Formulation

The internet of things is a technology that is decentralized in nature. Due to the decentralized nature of the network security and routing are the major issues of this network. This research work is both to increase the security of the IoT. Due to the decentralized nature of the network malicious enter the network which triggers various types of active and passive attacks. Location protection is the active type of attack which increases the delay in the network. In the location protection attack, the malicious node sends data through the longest route which affects network performance. The technique which is proposed in the previous research work is based on the threshold delay. Due to defining threshold delay, the accuracy of malicious node detection is very less. In this research work, a novel approach will be proposed for the detection of the malicious node in the least amount of time.

### 3.2. Objectives

Following are the various objectives of this research work:-

1. To study and analyze various malicious node detection techniques of IoT
2. To implement a threshold-based mechanism for the malicious node detection in IoT
3. To propose a novel approach for the detection of the malicious node in the internet of things
4. Implement proposed approach and compare with existing in terms of certain parameters

### **3.3. Research Methodology**

This research work is based on the detection of location protection attacks from the IoT. The internet of things is a decentralized network in which sensor nodes ping their neighbors after a certain amount of time. In the attack, a malicious node floods the unlimited number of packets in the network for the denial of service. When the malicious node floods the unlimited number of packets in the network, normal sensors are busy receiving packets from the malicious node. When the normal sensor nodes are busy, it is unable to reply to their neighbors which leads to packet loss and also delay in localization of sensor nodes. To detect malicious nodes from the network following two steps will be followed:-

Step 1: In the first step, we will detect that some malicious node in the network which can trigger an attack to do so, we will check packet loss and delay in the node localization process. The beacon signals are used to localize their neighbors. When the sensor nodes don't respond for a certain amount of time then it is considered that an attack is triggered in the network

Step 2: In the second step proposed technique will detect which sensor node triggers attack in the network. To detect a malicious node, the node which is unable to localize its neighbor that node will monitor the traffic of the network. It will maintain a list of the traffic which is processed in the network. When a node with particular identification transmit the maximum number of control in the network that node will be marked as the malicious node.

#### **Benefits of proposed Work**

Following are the various benefits of the proposed work:-

1. The proposed methodology works in two phases which is to ensure that an attack is triggered in the network and the second is to find malicious node from the network. This process will use the least number of network resources for malicious node detection.
2. The second major benefit is accuracy as when it ensured that an attack is triggered then we will find which node is malicious it can improve the accuracy of malicious node detection

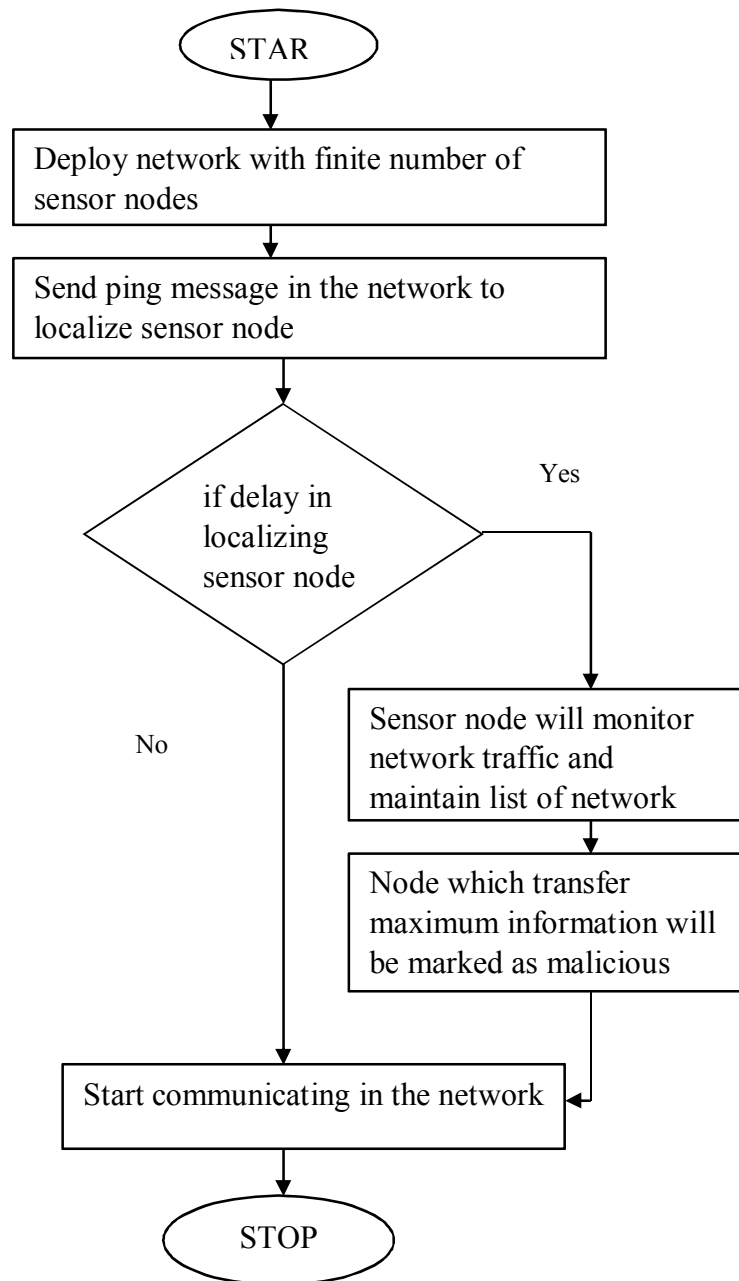


Figure 3.1: Proposed Flowchart

# Chapter 4

## Result and Discussion

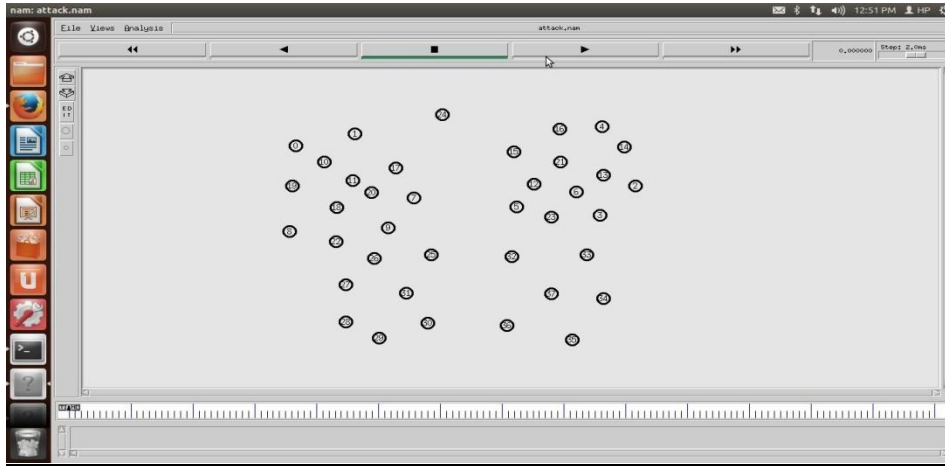
### 4.1. Tool and Technologies

Network Simulator (version 2), popular as NS2, is an event-driven simulation tool. This tool is successfully used to analyze the dynamic behavior of communication networks. Wired as well as wireless network functions and protocols (eg, algorithms, routing algorithms, TCP, UDP) can be simulated using NS2. In general, NS2 tool bestows users a method to specify such network protocols and simulate their corresponding behavior. NS2 has steadily gained popularity in the networking research community since its birth in 1989, due to its flexible and integrated nature. Apart from this, this package can easily generate many sorts of network traffic types, for example, CBR (Constant Bit Rate), ABR (Available Bit Rate), and VBR (Variable Bit Rate). It is a prominent simulation package in the education sector. NS2 includes two main languages: C++ and OTcl (Object-Oriented Tool Command Language). Tcl is a comparatively new language that makes use of object-oriented features. It was devised as an extended version of object-oriented Tcl (Tool Command Language) in MIT. On one hand, if C++ defines the internal scheme (ie, backend) of the simulation, OTcl on the other, assembles and configures objects along with scheduling discrete events (ie, frontends) to initiate simulation. TclCL is utilized to link C++ with the Tcl. Mapped to a C++ object, variables available in the Tcl domains are sometimes considered as the handles. NS2 runs on different platforms such as UNIX (or Linux), Windows, and Mac systems. This tool is developed in the Unix environment; thus, the smoothest ride is included in it and it can be installed easily.



### **4.1.1 Deployment of Network**

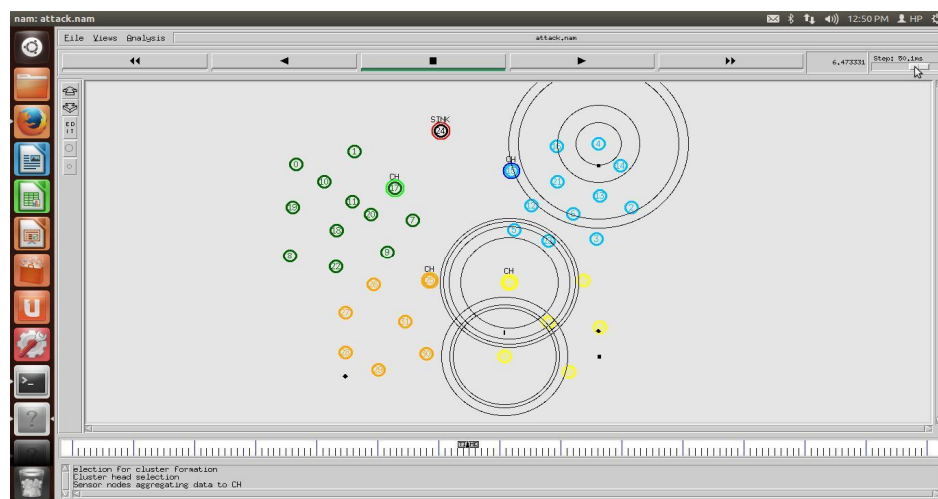
The IoT network deployment is done in this step. As shown in figure 4.1, the IoT network is deployed with a finite number of sensor nodes.



**Figure 4.1: Deployment of Network.**

### **4.1.2 Division of Network in Clusters**

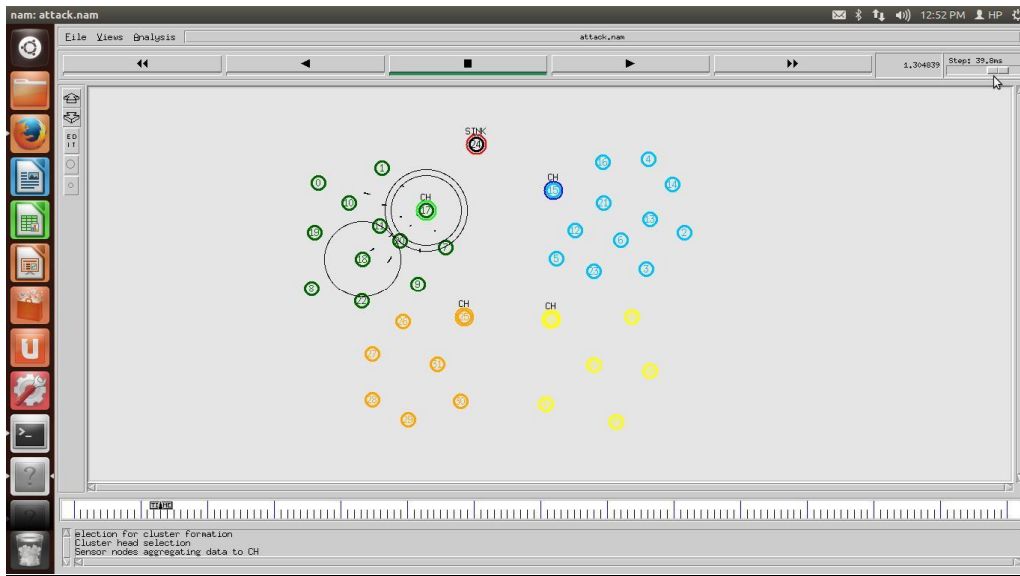
The network which is divided randomly is divided into finite clusters. The cluster heads are selected in each cluster based on the energy and distance. The sensor node which has maximum energy and the least distance to the base station is selected as cluster head. The complete scenario is illustrated in figure 4.2.



**Figure4.2: Division of the network in clusters**

### 4.1.3 Aggregation of sensed information

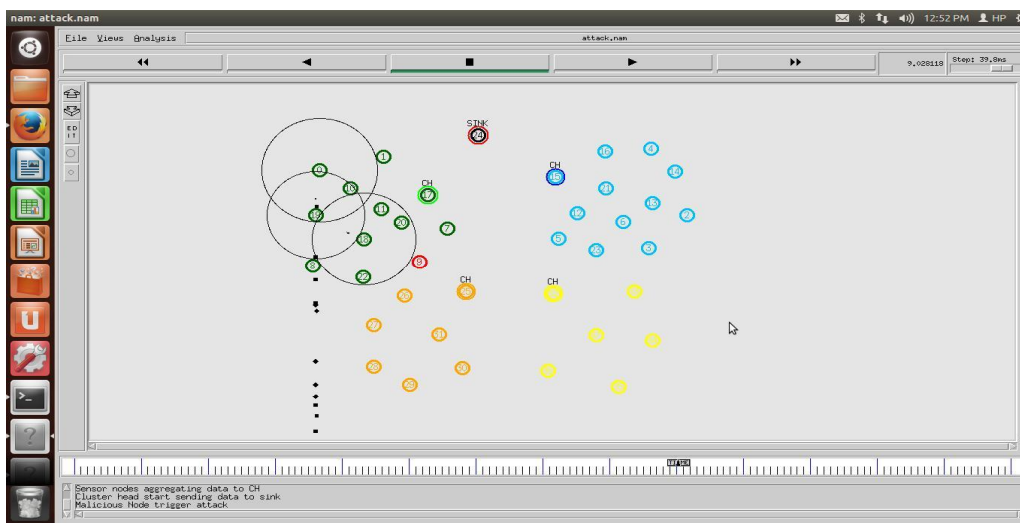
The information which is sensed by the sensor nodes is transmitted to a base station. The data which is sensed by the sensor nodes are transmitted to the cluster head. The cluster head will transmit information to the base station and it is shown in figure 4.3.



**Figure 4.3: Aggregation of sensed information**

### 4.1.4 Location Protection Number Attack

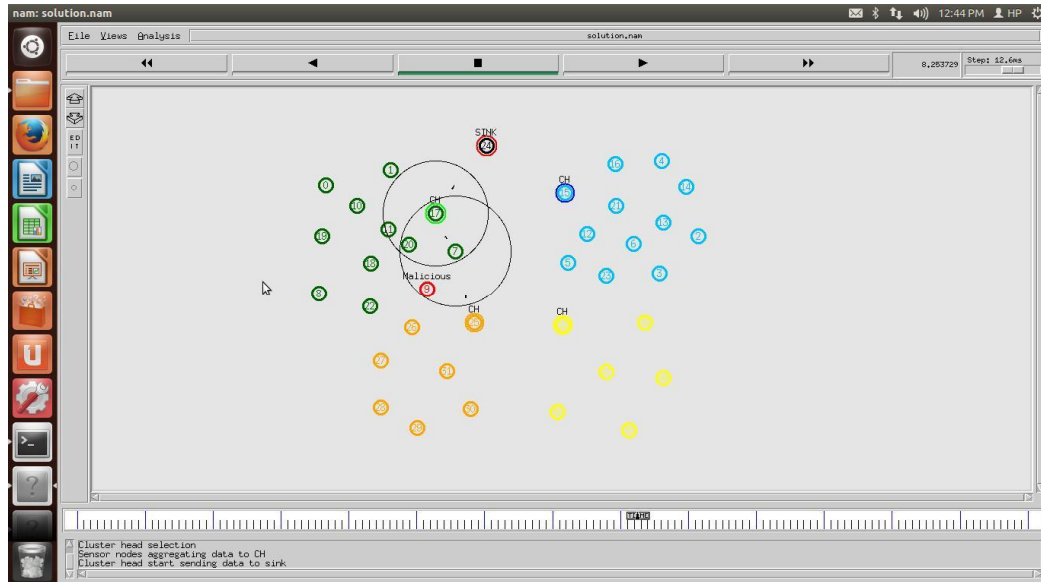
The version number attack is triggered in the DODAG protocol is shown in figure 4.4, As a result, malicious nodes will create the loop and data will be transmitted in that loop, Thus it leads to the loss of packet in the network.



**Figure4.4: Location Protection Number Attack**

### **4.1.5 Proposed Methodology**

The proposed methodology is implemented in this figure. The technique of trust-based mechanism is implemented and sensor nodes that have the least trust are detected as malicious nodes from the network.



**Figure4.5: Proposed Methodology**

This research work is based on the detection and isolation of malicious nodes from IoT. The malicious node is detected with threshold-based and monitor mode techniques. The performance of the proposed model is tested in terms of energy consumption, throughput, and delay

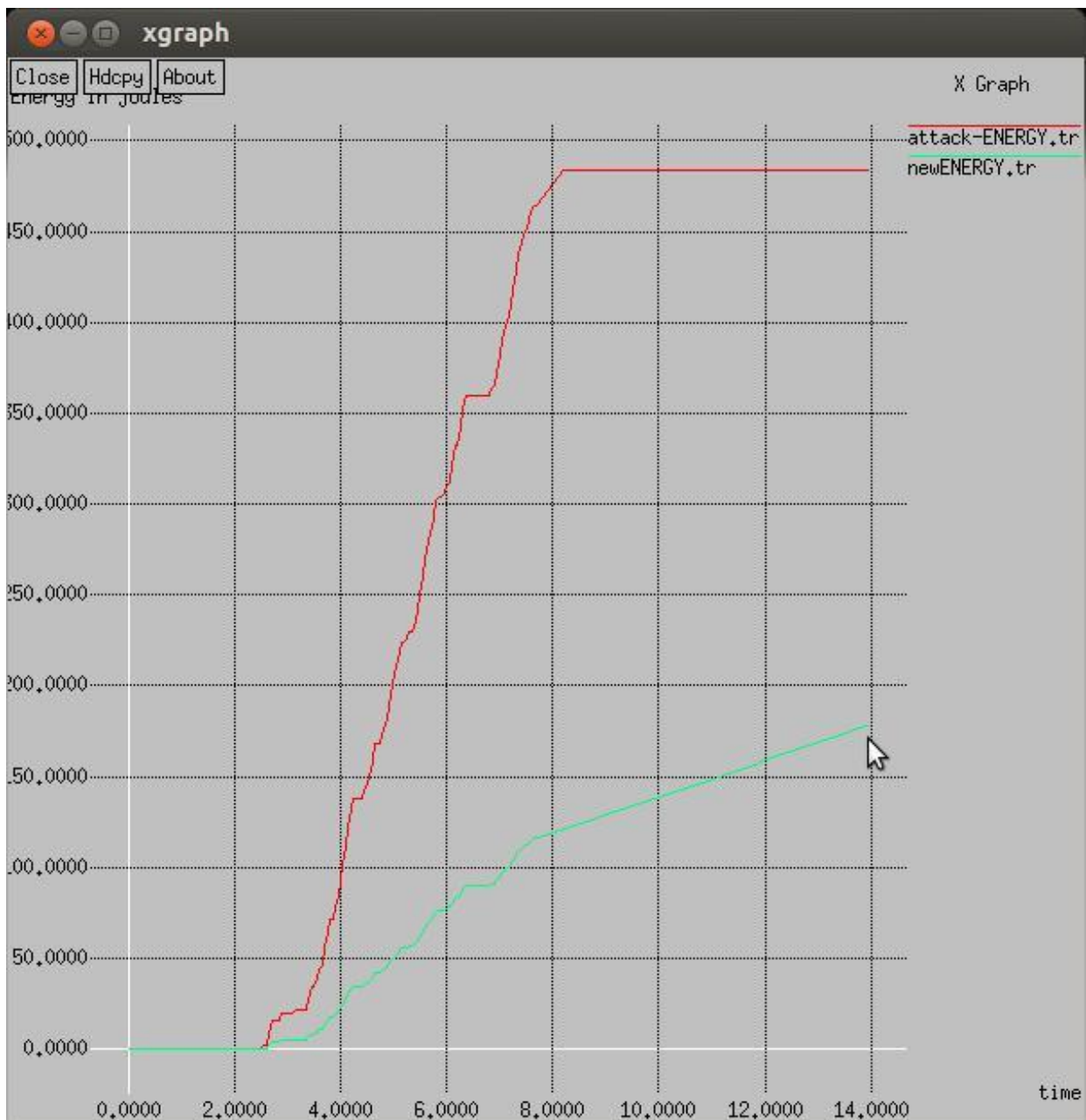


Figure 4.6: Energy Consumption

As shown in figure 4.6, the energy consumption of the proposed method is compared with the attack scenario. The proposed methodology gives low energy consumption as compared to the existing methodology which improves the performance of the model.

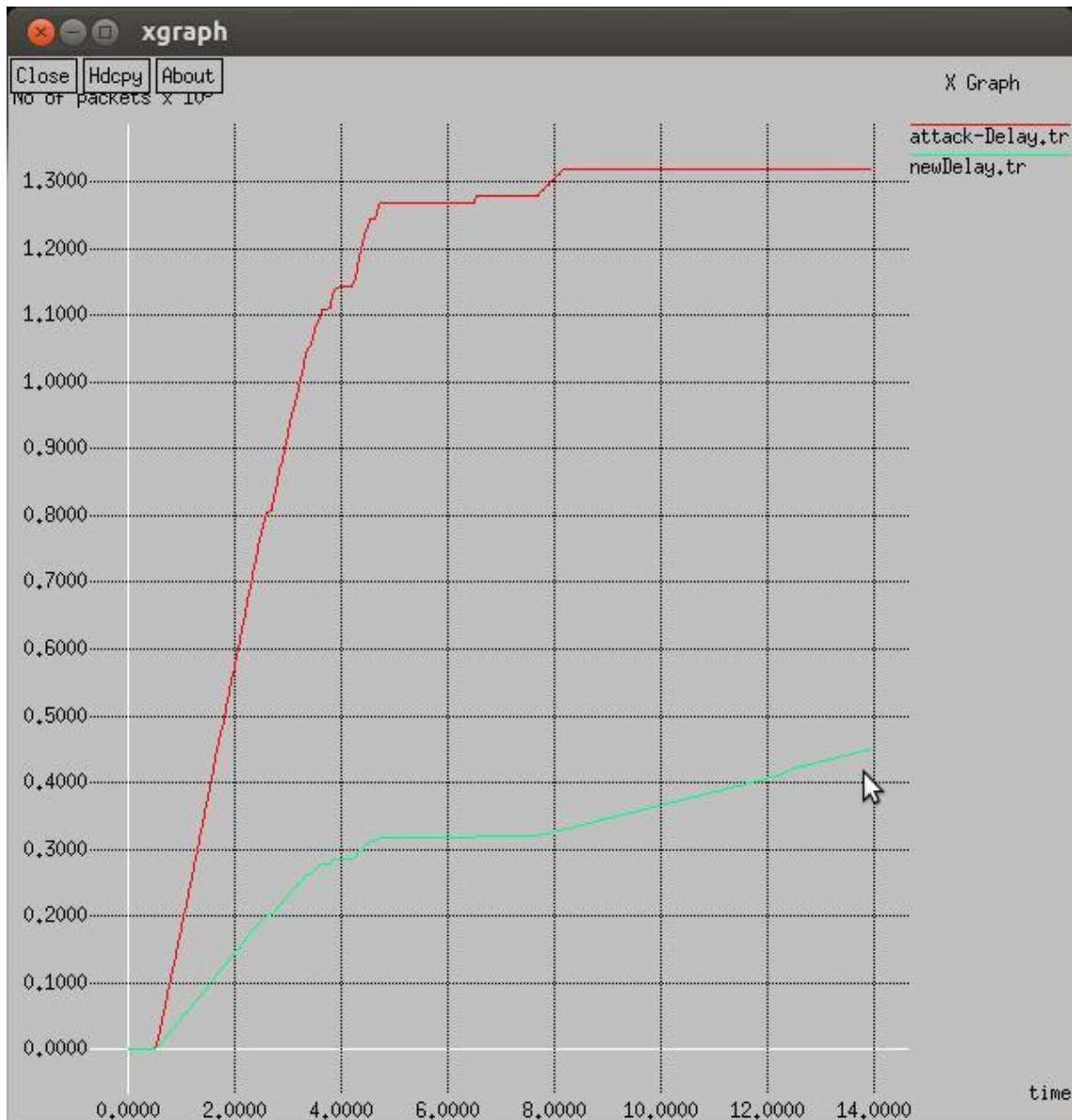


Figure 4.7: Delay Analysis

As shown in figure 4.7, the delay of the proposed methodology is low as compared to the existing technique. The proposed methodology detect malicious node in the least amount of time due to which delay is reduced in the network.

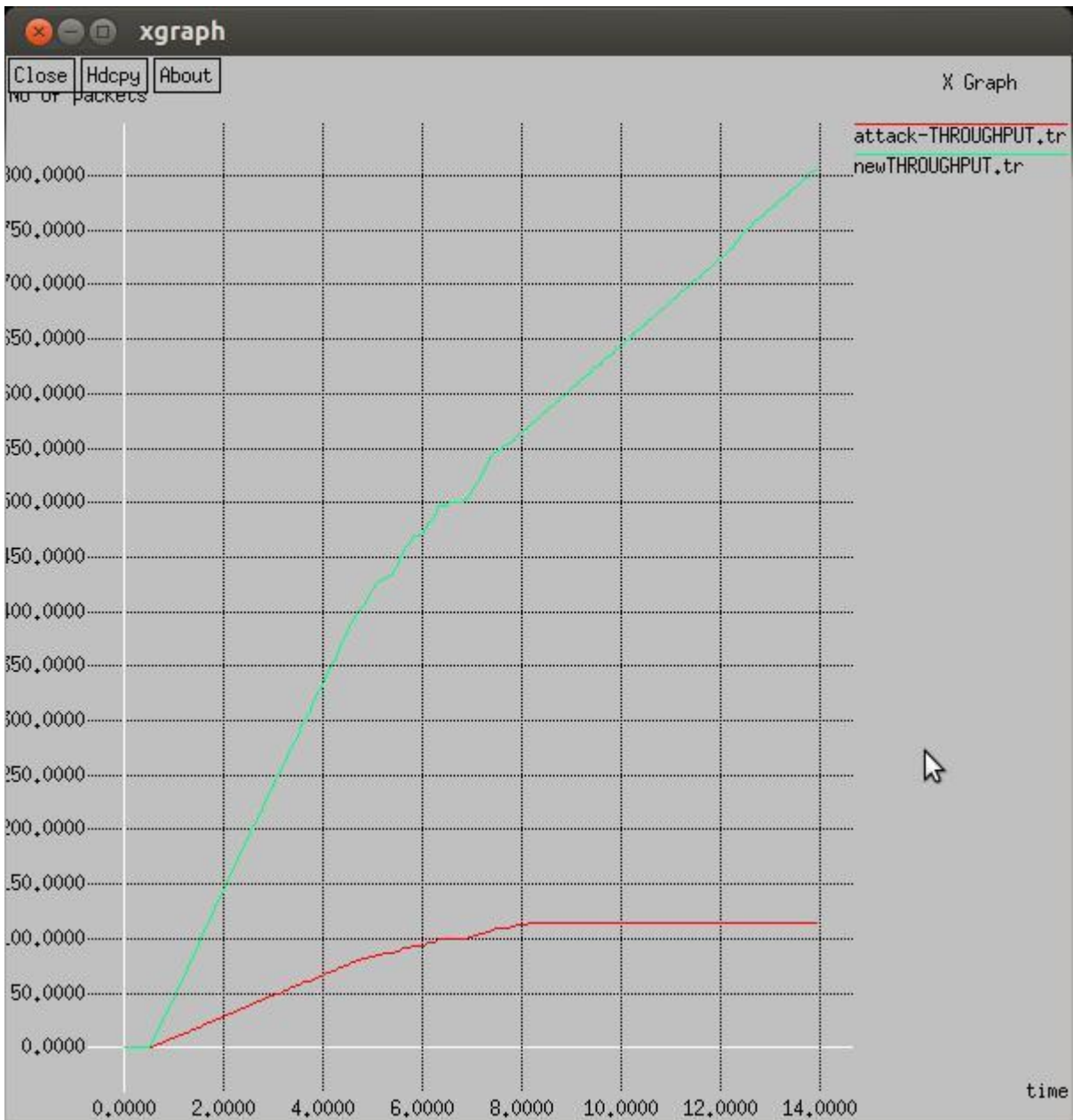


Figure 4.8:Throughput Analysis

As shown in figure 4.8, the throughput of the proposed technique is high as compared to the existing technique. The throughput of the network is increased due to the detection of malicious nodes.

# Chapter 5

## Conclusion and Future Work

### 5.1. Conclusion

In this paper, it is concluded that the internet of things is the decentralized type of network in which sensor nodes sense information and pass it to the base station. Due to such dynamic nature of the network, malicious nodes enter the network which triggers various types of security attacks. The location protection attack is the denial of service-based attack of IoT. One more challenging aspect is that location privacy may have many meanings and present various requirements, based on the scenario wherein the clients are moving and on the services the clients are communicating with. Location privacy can be divided into three categories, i.e., identity privacy, position privacy, path privacy. Identity privacy is intended to protect the identity of customers connected to or identifiable by location information. For this purpose, privacy schemes aim to minimize the disclosure of data using which attackers can get access to user identities. Identity privacy is appropriate in those applications that do not need users' IDs to provide the service. Privacy of the position secures the status of individual clients by reducing related information and reducing the accuracy of location information [6]. Position privacy is appropriate for situations that require the identities of users' successfully deliver services. An approach that uses the maximum solutions, either explicitly or implicitly, reduces accuracy by measuring a location with scalar granularity (from meters to hundreds of meters, from a city block to an entire city, etc). The objective of path privacy is to protect the privacy of information corresponding to user movements, for example, paths followed during traveling or walking in a city. Many privacy-based services (personal navigation systems) can be used to disrupt path privacy or track users illegally. Since location privacy definitions and requirements vary according to the situation, this is not possible for a single technology to meet the needs of all location privacy classes. Consequently, in past years, the researchers aiming at providing schemes to protect users' location privacy, has presented several methodologies that can be categorized into three main categories: anonymity-based, obfuscation- Based and policy-based methods In this research work technique of threshold and monitor mode is proposed for the detection of malicious nodes from the network. The proposed technique is implemented in NS2 and results are analyzed in terms of energy,

throughput, and delay. It is analyzed from the results that the proposed methodology improved results up to 10 percent as compared to the existing technique.

## **5.2. Future Work**

Following are the various future possibilities of this work:-

1. The proposed model can be further extended to improve security using the authentication techniques
2. The proposed model can be compared with other security models to test reliability



## References

- [1] Inayat Ali, Sonia Sabir, Zahid Ullah, “Internet of Things Security, Device Authentication and Access Control: A Review”, 2016, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8
- [2] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah, “Security Issues in the Internet of Things (IoT): A Comprehensive Study”, 2017, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6
- [3] R.Vignesh and A.Samydurai, “Security on the Internet of Things (IoT) with Challenges and Countermeasures”, 2017, IJEDR, Volume 5, Issue 1
- [4] Ş. Okul, M. Ali Aydın, “Security Attacks on IoT”, 2017, International Conference on Computer Science and Engineering (UBMK)
- [5] MeriemBettayeb, Omnia Abu Waraga, Manar Abu Talib, Qassim Nasir, Omar Einea, “IoT Testbed Security: Smart Socket and Smart Thermostat”, 2019 IEEE Conference on Application, Information and Network Security (AINS)
- [6] Jalindar B. Karande, Sarang A. Joshi, “Comprehensive Assessment of Security Attack Detection Algorithms in the Internet of Things”, 2018, Fourth International Conference on Computing Communication Control and Automation (IC3CAA)
- [7] Lulu Liang, Kai Zheng, Qiankun Sheng, Xin Huang, “A Denial-of-Service Attack Method for an IoT System”, 2016, 8th International Conference on Information Technology in Medicine and Education (ITME)
- [8] Tu-Liang Lin, Hong-Yi Chang and Sheng-Lin Li, “A Location Privacy Attack Based on the Location Sharing Mechanism with Erroneous Distance in Geosocial Networks”, 2020, sensors
- [9] Konstantinos Dimitriou and IoannaRoussaki, “Location Privacy Protection in Distributed IoT Environments Based on Dynamic Sensor Node Clustering”, 2019, Sensors
- [10] Tao Peng, Qin Liu, Guojun Wang, “Collaborative trajectory privacy preserving scheme in location-based services”, 2016, Information Sciences

- [11] Dan Liao, Hui Li, Victor Chang, "Location and trajectory privacy preservation in 5G-Enabled vehicle social network services", 2018, Journal of Network and Computer Applications
- [12] Tinghuai Ma, Jing Jia, Mznah Al-Rodhaan, "Protection of location privacy for moving kNN queries in social networks", 2017, Applied Soft Computing
- [13] Mahdi DaghmehchiFiroozjaei, Jaegwan Yu, Hyoungshick Kim, "Privacy-preserving nearest neighbor queries using geographical features of cellular networks", 2017, Computer Communications
- [14] Gang Sun, Dan Liao, Victor Chang, "L2P2: A location-label based approach for privacy-preserving in LBS", 2016, Future Generation Computer Systems
- [15] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home", 2017, IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)
- [16] Sachi Nandan Mohanty, K. C. Ramya, Ashish Khanna, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy", 2019, Future Generation Computer Systems
- [17] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, Michael H. Breitner, "Privacy concerns in the smart home context", 2020, Springer
- [18] Martin J Kraemer, Ivan Flechais, "Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods", 2018, IET Living in the Internet of Things: Cybersecurity of the IoT Conference
- [19] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, Hui Li, "Achieving k-anonymity in privacy-aware location-based services", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications
- [20] SamehZakhary, Milena Radenkovic, Abderrahim Benslimane, "Efficient Location Privacy-Aware Forwarding in Opportunistic Mobile Networks", 2014, IEEE Transactions on Vehicular Technology, Volume: 63, Issue: 2

- [21] Chunyong Yin, Jinwen Xi, Ruxia Sun, Jin Wang, "Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things", 2018, IEEE Transactions on Industrial Informatics
- [22] Zainab Waleed Hussien, Doaa Sami Qawasmeh, Mohammad Shurman, "MSCLP: Multi-Sinks Cluster-Based Location Privacy Protection scheme in WSNs for IoT", 2020, 32nd International Conference on Microelectronics (ICM)
- [23] Amani Abuladel, Omaimah Bamasag, "Data and Location Privacy Issues in IoT Applications", 2020, 3rd International Conference on Computer Applications & Information Security (ICCAIS)
- [24] Peipei Sui, Xianxian Li, Yan Bai, "A Study of Enhancing Privacy for Intelligent Transportation Systems:  $k$ -Correlation Privacy Model Against Moving Preference Attacks for Location Trajectory Data", 2017, IEEE Access
- [25] Sami Saad Albouq, Adnan Ahmed Abi Sen, Abdallah Namoun, Nour Mahmoud Bahbouh, Ahmad B. Alkhodre, Abdullah Alshamqiti, "A Double Obfuscation Approach for Protecting the Privacy of IoT Location Based Applications", 2020, IEEE Access
- [26] Weipeng Jing, Qiucheng Miao, Houbing Song, Xuebin Chen, "Data Loss and Reconstruction of Location Differential Privacy Protection Based on Edge Computing", 2019, IEEE Access
- [27] Donghe Li, Qingyu Yang, Dou An, Wei Yu, Xinyu Yang, Xinwen Fu, "On Location Privacy-Preserving Online Double Auction for Electric Vehicles in Microgrids", 2019, IEEE Internet of Things Journal
- [28] Mingming Guo, Kianoosh G. Boroojeni, Niki Pissinou, Kia Makki, Jerry Miller, Sitharama Iyengar, "Query-Aware User Privacy Protection for LBS over Query-Feature-based Attacks", 2018, IEEE Symposium on Computers and Communications (ISCC)
- [29] Guangjie Han, Hao Wang, Mohsen Guizani, Sammy Chan, Wenbo Zhang, "KCLP: A  $k$ -Means Cluster-Based Location Privacy Protection Scheme in WSNs for IoT", 2018, IEEE Wireless Communications

- [30] Shihong Zou, Jinwen Xi, Honggang Wang, Guoai Xu, "CrowdBLPS: A Blockchain-Based Location-Privacy-Preserving Mobile Crowdsensing System", 2020, IEEE Transactions on Industrial Informatics
- [31] Thu Le, Isao Echizen, "Lightweight Collaborative Semantic Scheme for Generating an Obfuscated Region to Ensure Location Privacy", 2018, IEEE International Conference on Systems, Man, and Cybernetics (SMC)
- [32] Mengmeng Yang, Tianqing Zhu, Yang Xiang, Wanlei Zhou, "Density-Based Location Preservation for Mobile Crowdsensing With Differential Privacy", 2018, IEEE Access
- [33] Shengke Zeng, Hongjie Zhang, Fei Hao, Hongwei Li, "Deniable-Based Privacy-Preserving Authentication Against Location Leakage in Edge Computing", 2021, IEEE Systems Journal
- [34] Guangjie Han, Hao Wang, Jinfang Jiang, Wenbo Zhang, Sammy Chan, "CASLP: A Confused Arc-Based Source Location Privacy Protection Scheme in WSNs for IoT", 2018, IEEE Communications Magazine
- [35] ShathaAlarabi, Shahad Almuzeri, Sara Alaradi, NisreenInnab, "Two Level Based Privacy Protection Approach for Internet of Things Users in Cloud Computing", 2018, 21st Saudi Computer Society National Computer Conference (NCC)
- [36] Wei Wu, Erwu Liu, Xinglin Gong, Rui Wang, "Blockchain Based Zero-Knowledge Proof of Location in IoT", 2020, IEEE International Conference on Communications (ICC)
- [37] Hao Wang, Guangjie Han, Wenbo Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT", 2018, Computer Networks
- [38] Yan He, Jiageng Chen, "User location privacy protection mechanism for location-based services", 2020, Digital Communications and Networks
- [39] Defeng Li, Yuan Hu, Mingming Lan, "IoT device location information storage system based on blockchain", 2020, Future Generation Computer Systems

- [40] Yu He, Guangjie Han, Whenbo Zhang, “A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things”, 2019, Future Generation Computer Systems
- [41] Guangjie Han, Lina Zhou, Sammy Chan, “A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things”, 2017, Future Generation Computer Systems
- [42] Gang Sun, Victor Chang, Dan Liao, “Efficient location privacy algorithm for Internet of Things (IoT) services and applications”, 2016, Journal of Network and Computer Applications
- [43] Rômulo Meira Góes, Blake C. Rawlings, Stéphane Lafortune, “Demonstration of Indoor Location Privacy Enforcement using Obfuscation”, 2018, IFAC-Papers
- [44] Gang Sun, Dan Liao, Victor Chang, “L2P2: A location-label based approach for privacy preserving in LBS”, 2016, Future Generation Computer Systems
- [45] Mengmeng Yang, Tianqing Zhu, Robert H. Deng, “A blockchain-based location privacy-preserving crowdsensing system”, 2018, Future Generation Computer Systems
- [46] Lina Ni, Yanfeng Yuan, Jinqun Zhang, “A Location Privacy Preserving Scheme Based on Repartitioning Anonymous Region in Mobile Social Network”, 2018, Procedia Computer Science
- [47] Ahmed Mohammed Ibrahim Alkuhlani, S. B. Thorat, “Enhanced location privacy and energy saving technique for sensors in Internet of Things domain”, 2016, International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICCC)
- [48] Mohammad Yamin, Adnan Ahmed Abi Sen, “A New Method With Swapping of Peers and Fogs to Protect User Privacy in IoT Applications”, 2020, IEEE Access
- [49] Mahmoud Elkhodr, SeyedShahrestani, Hon Cheung, “A contextual-adaptive Location Disclosure Agent for general devices in the Internet of Things”, 2013, 38th Annual IEEE Conference on Local Computer Networks – Workshops

- [50] Ruchi Vishwakarma, Ankit Kumar Jain, “A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks”, 2019, 3rd International Conference on Trends in Electronics and Informatics (ICOEI)
- [51] VijenderBusi Reddy, Atul Negi, S Venkataraman, V Raghu Venkataraman, “A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT)”, 2019, IEEE 5th World Forum on Internet of Things (WF-IoT)
- [52] Fathima James, “A Risk Management Framework and A Generalized Attack Automata for IoT based Smart Home Environment”, 2019, 3rd Cyber Security in Networking Conference (CSNet)
- [53] S. Sridhar, S. Smys, “Intelligent security framework for iot devices cryptography based end-to-end security architecture”, 2017, International Conference on Inventive Systems and Control (ICISC)
- [54] Xupeng Luo, Qiao Yan, Mingde Wang, Wenyao Huang, “Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT”, 2019, Computing, Communications and IoT Applications (ComComAp)
- [55] Syeda Mariam Muzammal, Raja Kumar Murugesan, Noor Zaman Jhanjhi, Low Tang Jung, “SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications”, 2020, International Conference on Computational Intelligence (ICCI)
- [56] Seungyong Yoon, Jeongnyeo Kim, “Remote security management server for IoT devices”, 2017, International Conference on Information and Communication Technology Convergence (ICTC)
- [57] S. Kalyani, D. Vydeki, “Survey of Rank Attack Detection Algorithms in Internet of Things”, 2018, International Conference on Advances in Computing, Communications and Informatics (ICACCI)
- [58] Kashif Naseer Qureshi, Shahid Saeed Rana, Gwanggil Jeon, “A novel and secure attacks detection framework for smart cities industrial internet of things”, 2020, Sustainable Cities and Society

- [59] David Airehrour, Jairo A. Gutierrez, Sayan Kumar Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things”, 2018, Future Generation Computer Systems
- [60] Fatima-tuz-Zahra, NZ Jhanjhi, Sarfraz Nawaz Brohi, Nazir A. Malik, “Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning”, 2019, 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)
- [61] Dong Seong Kim, Kok Onn Chee, Mengmeng Ge, “A Novel Graphical Security Model for Evolving Cyber Attacks in Internet of Things”, 2020, 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)
- [62] Daemin Shin, Keon Yun, Jiyeon Kim, Philip Virgil Astillo, Jeong-Nyeo Kim, Ilsun You, “A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks”, 2019, IEEE Access
- [63] Chang Choi, Junho Choi, Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service”, 2019, IEEE Access
- [64] Ahmed Yar Khan, Rabia Latif, Seemab Latif, Shahzaib Tahir, Gohar Batool, Tanzila Saba, “Malicious Insider Attack Detection in IoTs Using Data Analytics”, 2020, IEEE Access
- [65] ZieEyaEkolle, KuramitsuKimio, Kohno Ryuji, “Intelligent Security Monitoring in Time Series of DDoS attack on IoT Networks using Grammar base Filtering and Clustering”, 2018, International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)
- [66] Yan Naung Soe, Paulus InsapSantosa, Rudy Hartanto, “DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment”, 2019, Fourth International Conference on Informatics and Computing (ICIC)

- [67] Jalal Bhayo, Sufian Hameed, Syed Attique Shah, “An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)”, 2020, IEEE Access
- [68] Ridwan Hadiansyah, Vera Suryani, AuliaArifWardana, “IoT Object Security towards the Sybil Attack Using the Trustworthiness Management”, 2020, 8th International Conference on Information and Communication Technology (ICoICT)
- [69] Liu Junjiao, Xiaodong Lin, Chen Xin, Wen Hui, Hong Li, Hu Yan, Sun Jiawei, Shi Zhiqiang, Limin Sun, “ShadowPLCs: A Novel Scheme for Remote Detection of Industrial Process Control Attacks”, 2020, IEEE Transactions on Dependable and Secure Computing
- [70] Nagarathna Ravi, S. Mercy Shalinie, “Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture”, 2020, IEEE Internet of Things Journal
- [71] James Jin Kang, Kiran Fahd, Sitalakshmi Venkatraman, Rolando Trujillo-Rasua, Paul Haskell-Dowland, “Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks”, 2019, 29th International Telecommunication Networks and Applications Conference (ITNAC)
- [72] Mohammad M. Shurman, Rami M. Khrais, Abdulrahman A. Yateem, “IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS”, 2019, International Arab Conference on Information Technology (ACIT)
- [73] Giuseppe Potrino, Floriano de Rango, Amilcare Francesco Santamaria, “Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker”, 2019, IEEE Wireless Communications and Networking Conference (WCNC)
- [74] Yusuf Muhammad Tukur, DhavalkumarThakker, Irfan-Ullah Awan, “Multi-layer Approach to Internet of Things (IoT) Security”, 2019, 7th International Conference on Future Internet of Things and Cloud (FiCloud)
- [75] AKM Jahangir Majumder, Jared D. Miller, Charles B. Veilleux, Amir A. Asif, “Smart-Power: A Smart Cyber-Physical System to Detect IoT Security Threat through Behavioral Power Profiling”, 2020, IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)



[76] Ramesh Paudel, Timothy Muncy, William Eberle, “Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach”, 2019, IEEE International Conference on Big Data (Big Data)

[77] Mujahid Mohsin, Zahid Anwar, GhaithHusari, Ehab Al-Shaer, Mohammad Ashiqur Rahman, “IoTSAT: A formal framework for security analysis of the internet of things (IoT)”, 2016, IEEE Conference on Communications and Network Security (CNS)

[78] Christiana Ioannou, VasosVassiliou, “Classifying Security Attacks in IoT Networks Using Supervised Learning”, 2019, 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)