HALMSTAD
UNIVERSITY

Master's Programme in Computer Network Engineering, 60 ECTS

MASTERTHESIS

Detection of and Prevention from Sybil Attacks in Internet of Things - a literature review

Filimon Barbu

Master Thesis, 15 ECTS

Halmstad

6 April 2016

Detection of and Prevention from Sybil Attacks in Internet of Things - a literature review

Master's Thesis in Network Engineering

6 April 2016

Author: Filimon Barbu

Supervisor: Professor Tony Larsson; Mahboobeh Parsapoor

Examiner: Professor Tony Larsson

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD, Sweden

Detection of and Prevention from Sybil Attacks in Internet of Things - a literature review

Abstract

Vast scale networks confront every day immense number of network attacks, including additionally Sybil attacks. Regardless of the quality of the current security defending schemes, these systems stay defenseless, as new tools and methods are by and large continually created by hackers. The rising Internet of Things (IoT) are defenseless against Sybil attacks where attackers can control fake characters or misuse pseudo-identities to compromise the viability of the frameworks. For instance, Sybil attacks is most critical in distributed systems, since a lot of individual and sensitive data is posted transparently in diverse networks, the dangers postured by Sybil attacks are intense particularly in light of the fact that they are hard to detect and has been no universally accepted technique to counter them up until now. In the presence of Sybil attacks, the IoT frameworks may produce wrong reports, and users may get spam and lose their privacy.

This thesis presents a literature review on IoT including security requirements for IoT. Furthermore it investigates and analyzes diverse types of defense mechanisms that have been proposed after some time to diminish the Sybil attacks.

List of abbreviations

2FA	Two-factor authentication
6LoWPAN	IPv6 over Low power Wireless Personal Area Network
ATM	Automated teller machine
Botnet	a large number of compromised computers that are used to generate spam, relay viruses or flood a network with excessive requests to cause it to fail
Bluetooth	technology standard for exchanging data over short distances in ISM band from 2.4 to 2.485 GHz
CA	Certificate Authority
CCA	Centralized Certification Authority
CoAP	Constrained Application Protocol
CFD	Customer Facing Devices
DC	Decentralized cryptographic
DTH	Distributed hash table
e.g.	means "for example" (from the Latin *exempli gratia*)
ETSI	European Telecommunications Standards Institute
FI	Future internet
GPRS	General packet radio service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
i.e.	means "that is" (from the Latin *id est*)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF ROLL	Routing Over Low power and Lossy networks
IoT	Internet of Things
IoT-i	Internet of Things initiative project
IPT	IP testing
ISM	Industrial, Scientific and Medical
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information technology

LLN	Low-Power and Lossy Network
M2M	machine-to-machine
MAC	media access control protocol
NFC	Near Field Communication
P2P	Peer-to-peer
PKI	Public Key Infrastructure
RC	Recurring cost
RFID	Radio frequency identification
SG	Social graph
SIM	Subscriber identity module
SMS	Short message service
SyMon	Sybil Monitor
TCP/IP	Transmission Control Protocol/Internet Protocol
TD	Trusted device
TOR	The Onion Router - is a distributed proxy network designed to provide anonymity on the internet
UMTS	Universal Mobile Telecommunications System
UWB	Ultra-Wide Band
WSN	Wireless Sensor Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WPAN	Wireless Personal Area Network
ZigBee	global wireless standard to provide the foundation for the IoT

Table of contents

List of figures

Chapter 1: Introduction

The Internet of Things (IoT) is the system of physical articles, such as gadgets, vehicles, buildings and different things, inserted with hardware, programming, sensors, and system connectivity that empowers these items to gather and exchange information. The IoT permits items to be detected and controlled remotely crosswise over existing system infrastructure, making opportunities for more straightforward integration of the physical world into computer based frameworks. Each thing is individually identifiable through its implanted processing framework and can interoperate within the current Internet infrastructure [1].

The IoT incorporates Customer Facing Devices (CFD) (e.g. to create digital interactions inside physical locations), and also products and services that are not customer facing, for example, gadgets intended for organizations to empower computerized communications between machines. For instance, the term IoT can incorporate the type of Radio Frequency Identification ("RFID") tags that organizations place on items in stores to screen stock; sensor systems to monitor electricity utilized as a part of houses; and Internet connected drills on oil rigs. Besides, the "things" in the IoT for the most part do exclude desktop or laptop computers and their nearby analogs, for example, smartphones and tablets, in spite of the fact that these gadgets are regularly utilized to control or communicate with other "things" [2].

1.1 Security risks in IoT

It ought to be noticed that expanded network between enormous amount of very common "things" and the Internet might increase various security and privacy risks.

About the risks, it ought to be said that IoT gadgets display an assortment of potential security risks that could be abused to harm the clients by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety.

1. On IoT gadgets, as with desktop or laptop computers, a lack of security could empower intruders to get to and abuse individual data gathered and transmitted to or from the gadget. For instance, new smart televisions empower customers to surf the Internet, make acquisitions, and share photographs, like a laptop or desktop computer. Like a computer, any security vulnerabilities in these televisions could put the data stored on or transmitted through the television at risk. In the event that smart television or different gadgets store sensitive financial account data, passwords, and different sorts of data, unauthorized persons could abuse vulnerabilities to facilitate identity theft or fraud. In this way, as customers introduce more

smart gadgets in their homes, they might increase the quantity of vulnerabilities an intruder could use to compromise individual information.

2. Security vulnerabilities in a specific gadget might facilitate attack on the purchaser system to which it is connected, or empower attacks on different frameworks. For instance, a compromised IoT gadget could be utilized to launch a Sybil attack. These attacks are more compelling the more gadgets the attacker has under its control; as IoT gadgets multiply, vulnerabilities could empower these aggressors to collect vast quantities of gadgets to use in such attacks. Another probability is that a connected gadget could be utilized to send malicious emails.

3. Unauthorized persons may misuse security vulnerabilities to make risks to physical safety now and again. For instance somebody portrayed how he could hack remotely into two distinctive connected insulin pumps and change their settings so that they no more delivered medicine.

These potential risks are deteriorated since securing connected IoT gadgets might be more challenging than securing a home computer [2], for two fundamental reasons.

1. It ought to be said that a few organizations entering the IoT business sector might not have experience in dealing with security issues.

2. Although some IoT gadgets are exceedingly complex, numerous others might be inexpensive and basically expendable. In those cases, if a vulnerability was found after manufacture, it might be troublesome or impossible to update the software or apply a patch. And if an upgrade is accessible, numerous clients might never find out about it.

Relatedly, numerous organizations, especially those developing low-end gadgets, might need financial motivating reasons to give continuous support or software security updates at all, leaving users with unsupported or vulnerable gadgets soon after purchase [2].

1.2 Privacy risks in IoT

Notwithstanding risks to security, were also acknowledged privacy risks spilling out of the Internet of Things. Some of these risks include the direct collection of sensitive individual data, for example, exact geographic location, financial related record numbers, or health data, risks as of now exhibited by conventional Internet and mobile commerce. Others emerge from the accumulation of individual data, habits, locations, and physical conditions after some time, which might permit an entity that has not straightforwardly collected sensitive data to infer it. Other issue is that apparent risks to privacy and security, regardless of the possibility that not understood, could weaken the clients certainty important for the technologies to meet their maximum capacity, and might bring about less far reaching acceptance [2].

1.3 Sybil attack synopsis

In a Sybil attack, a solitary node displays different characters to different nodes in the system. Any framework whose proper conduct depends on the supposition that most nodes will behave legitimately might be at risk for Sybil attacks.

Sybil attacks performed against wireless networks and be particularly harmful against many IoT applications. The Sybil attack is particularly threatening to fault tolerant plans, for example, distributed storage, routing algorithms, data aggregation, voting, fair resource allocation, misbehavior detection and topology maintenance [3].

Replicas, storage partitions, or routes accepted to be utilizing disjoint nodes could include a solitary foe showing numerous personalities. Sybil attacks additionally represent a critical risk to geographic routing protocols. Location aware routing frequently obliges nodes to exchange coordinate data with their neighbors to proficiently route geographically addressed packets. It is just sensible to anticipate that a node will acknowledge yet a solitary arrangement of set of coordinates from each of its neighbors, however by utilizing the Sybil attack a foe can be in more than one spot at once [4]. It can strike the routing algorithms by defining many routes through one and only one node [3].

Resources of a node can be emptied by requests from multiple entities which are indeed displayed by a solitary malicious node [3]. Sybil attack tries to corrupt the integrity of information security and resource use that the distributed algorithm endeavors to accomplish [5].

Encryption and authentication schemes can keep an outsider to launch a Sybil attack on the sensor system. Assuming that a compromised node puts on a show to be two of the three nodes the algorithms utilized might attain that redundancy has been accomplished while in all actuality it has not [5].

Sybil attacks can in the worst scenario, empower malicious nodes to assume control over the entire system and defeat the replication mechanisms in distributed systems.

1.4 Problem statement

Sybil attack has turned into a disturbing danger for open access distributed frameworks and online social networks in the IoT, that permits an attacker to exploit framework assets and control the system performance.

The aggressor's purpose is to maximize the quantity of Sybil personalities [6] in the overlay network (e.g. a computer network that is built on top of another network), despite the fact that in a few frameworks, a small number of Sybil characters is able to prevent the attacker from exploiting the system.

The aim of Sybil defense is to precisely distinguish Sybil characters and preclude them to misuse the system assets.

1.5 Thesis objective

The objective is to protect from the Sybil attack by recognizing Sybil personalities, or associates that produce such characters, and confine them from the overlay network.

The thesis objective is a research study which endeavors to investigate and assess the performance of the security mechanisms which are proposed to detect and defend Sybil attacks.

The questions to be addressed are the following:

- How to create a Sybil node?
- What could be the characteristics of a Sybil node?

Chapter 2: Background

At the point when individuals discuss about the Internet, they are typically alluding to the electronic network that allows computers around the globe to communicate with one another [7].

2.1 What is the Internet of Things (IoT) ?

There is no all around settled upon definition, however by and large, the term is utilized to depict systems of articles that are not themselves computers but rather that have embedded parts that connect with the Internet [7].

Internet of Things (IoT) alludes to systems of articles that communicate with different items and with computers through the Internet. "Things" might incorporate basically any item for which remote communication, information gathering, or control may be helpful, for example, vehicles, medicinal gadgets, electric grids, fabricating hardware, or building frameworks. As such, the IoT possibly incorporates colossal numbers and sorts of interconnected articles. It is frequently viewed as the following significant stage in the advancement of the internet [7].

Two components makes articles part of the IoT such as a unique identifier and Internet connectivity. Such "smart" articles each have a unique Internet Protocol (IP) address to recognize the item sending and getting data.

2.2 What is machine-to-machine?

Machine-to-machine (M2M) is characterized as the innovations that permit machines, normally (little) computing sensors that perform particular errands to convey or transfer data as required ordinarily over basic protocols yet all the more as of late over Internet protocols (IP) over remote or wired or even short message service (SMS) [8].

2.3 What is the difference between IoT and M2M ?

Industry discussions on the IoT and its potential advantages have brought up various issues with respect to refinements between IoT and its precursor, M2M communications. Remote gadget access is a core normal deliverable for both arrangements (IoT and M2M), so inquiries concerning how to recognize M2M and IoT are reasonable [9].

In any case, shared characteristic between the two arrangement sorts to a great extent closes there, and they differ by the way they accomplish remote gadget access. For instance, conventional M2M arrangements commonly depend on point-to-point communication utilizing embedded equipment modules and either cellular or wired systems. Conversely, IoT arrangements depend on IP-based systems to interface gadget information to a middleware stage [9].

The M2M arrangements offer remote access to machine information, these information are customarily focused at point arrangements in service applications. Mix of gadget and sensor information with huge data, investigation and other endeavor applications is a core idea driving the developing IoT. This combination is critical to accomplishing various advantages all through the assembling endeavor and, eventually, development in the marketplace [9].

2.4 Remote gadget access

Access to remote gadgets, machines, resources and different elements gives an essential worth suggestion to both M2M and IoT solutions. M2M applications are regularly made out of equipment modules embedded in a machine at a client site that convey by means of restrictive cellular or wired systems to a devoted programming application, frequently at the supplier's service operation. This capacity permits the gadget (resource, machine) supplier to diminish its administration costs through remote diagnostics, remote investigating, remote upgrades and other remote abilities that decrease the need to send field service staff [9].

In the IoT arrangements, the 'what, how and why' of remote gadget access includes much more extensive accomplishment. IoT obliges the same gadgets (resources, machines) as M2M applications, additionally low-power and passive sensors and cheap gadgets that will not have the capacity to legitimize a devoted M2M equipment module. IoT gadgets communicate by means of standards based IP systems, and their information are joined into big business applications to empower enhanced service, as well as operational improvement and new plans of action, for example, item as product-as-a-service [9].

The capacity for applications all through the undertaking to get to gadget information to empower execution upgrades, business advancement or different conceivable outcomes obviously recognizes the capability [9] of IoT versus M2M. Conversely, M2M ordinarily utilizes on point-to-point communication.

The structural planning likewise makes IoT more versatile, disposing of the requirement for incremental hard-wired connections and subscriber identity module (SIM) card establishments [9]. This is one motivation behind why M2M is frequently alluded to as M2M is about short message service (SMS) and general packet radio service (GPRS), while IoT is about the IP stack [10].

It is certain that these two ideas (M2M and IoT) do indeed have distinctive meanings. Most reason that IoT is a more extensive idea, which will advance from M2M and different technologies [11].

2.5 Evolution of the Internet

Before the analysis of the IoT in detail, it is important to take a glance at the development of the Internet. In the late 1960s, communication between two computers was made possible through a computer network [12]. In the early 1980s, the Transmission Control Protocol/Internet Protocol (TCP/IP) stack was brought in. Then, commercial use of the Internet started in the late 1980s. Later, the World Wide Web (WWW) became available in 1991 which made the Internet more well-known and awaken the very quick advancement. The WWW is using the Hypertext Transfer Protocol (HTTP). Then, mobile devices linked to the Internet and formed the mobile Internet. With the rise of social networking, users started to become linked together over the Internet. The next step in the IoT is the time when 'things' around us will be able to link to each other (e.g. machine to machine) and interact via the Internet [12].

The IoT affirmation to create a world where all the 'things' (also called smart objects) around us are connected to the Internet and connect with each other with minimum human intervention. The ultimate goal is to create 'a better world for human beings', where objects around us know what we like, what we want, and what we need and act accordingly without specific instructions [12].

In [13], [14], the IoT pioneers Adam Dunkels and Zach Shelby freely demonstrated that native IP support is possible for the resource constrained gadgets utilized as a part of remote sensor systems and smart objects.

With the expanding enthusiasm for low-power networks, the Internet Engineering Task Force (IETF) chartered a working group 4 in 2006 to standardize an adaptation layer for transmitting IP packets over IEEE 802.15.4, the most well-known low-power radio standard at the time [15]. The subsequent Internet Protocol version 6 (IPv6) over Low power Wireless Personal Area Network (6LoWPAN) specifications [16], [17] depend on the Internet Protocol version 6 (IPv6), which has a modular configuration, and consequently is more suited for adaptation than its predecessor Internet Protocol version 4 (IPv4).

Moreover, IPv6 provides a 128-bit address space permitting 2^{128}, or just about 3.4×10^{38} addresses. That is around 340 trillion addresses. The real number is littler because of the intelligent organizing of IPv6 addresses and because of the way that some IP addresses have been held for different uses, for example, for use in private frameworks. Still, the number is sufficiently vast to all around address each and every gadget connected to the Internet within a reasonable time-frame. The proposed IP-based IoT idea now empowers the seamless integration of the physical world into the virtual world represented by the computer frameworks that are globally connected through the Internet [9].

Studies by research firms [18] anticipate more than 50 billion connected gadgets and an aggregate monetary quality include of 1.9 trillion dollars before the end of 2020.

2.6 Connections in Internet of Things

As depicted in figure 1, the IoT allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [12], [19]. They are ''Material objects connected to material objects in the Internet''.

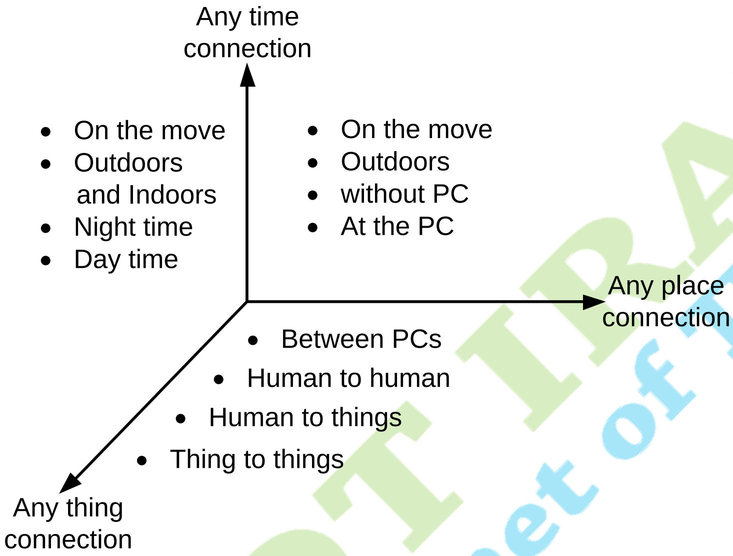

Figure 1: Connections in IoT [20]

For instance, through RFID, laser scanners, infrared sensors and other data detecting gadgets are connected with any article for communication services and information exchange. Finally, to achieve the smart gadgets to be tracked, located, and monitored and to handle the system functions, to make the Information Technology (IT) framework and physical infrastructure strengthening IoT is the most required one [12].

2.7 Architecture of IoT

The driven vision of the IoT is to expand the Internet from the digital world to the physical world by interfacing each object to the Internet [21], [22]. The things in this idea differ from physical items to cyber entities, for example, television sets, computing gadgets, programming elements, and so forth [22]. The IoT idea empowers these things to join and communicate with one another or to be controlled remotely. This makes a situation for sharing data between the things in real-time [23]. Nature merges the physical world and the virtual world together [24], and makes a connection to exchange information between genuine gadgets and digital applications in a secured connection [25].

The IoT idea is recognized by its dynamic structural planning, because of a few qualities that empower it to share data, wise taking care of and vast scale cooperation. Sharing data represents the functions of getting and exchanging data with things in one hand and with different gadgets over the Internet in another, while smart handling represents the capacity of processing and controlling data brilliantly. The last notable characteristic of IoT is the huge scale characteristic for connected things. The straightforwardness of the IoT architecture is another viewpoint that makes the IoT architecture dynamic [23]. The three-hierarchical layer architecture is shaped by the perception layer, network layer and application layer [26], as appeared in figure 2.

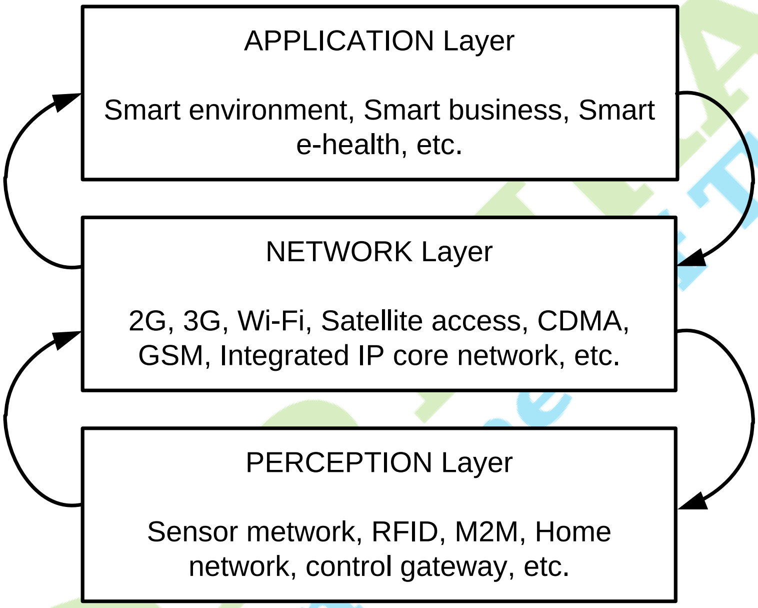
APPLICATION Layer
Smart environment, Smart business, Smart e-health, etc.
NETWORK Layer
2G, 3G, Wi-Fi, Satellite access, CDMA, GSM, Integrated IP core network, etc.
PERCEPTION Layer
Sensor metwork, RFID, M2M, Home network, control gateway, etc.

Figure 2: The three layer architecture of IoT [12]

The working standard of the hierarchical architecture begins when the perception layer gathers information of connected things through its detecting technology, for example, RFID and sensors. At that point, it exchanges the gathered information to the following layer which is the network layer. This layer uses the communication methods of the Internet or local network to convey the gathered information to the applications in the application layer for processing [32]. At long last, in this layer the information is processed and examined to be put in databases or to be shared with other application frameworks [27].

2.8 IoT Protocol Stack

With respect to IoT Protocol Stack, delineated in the figure 3, from a physical (PHY) layer viewpoint, the current IEEE 802.15.4-2006 PHY layer suffice as far as energy effectiveness [12], [28].

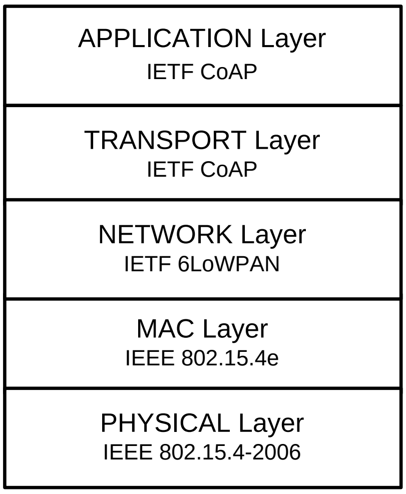

Figure 3: IoT Protocol Stack [12]

Given that a lot of IoT applications however will require just a couple of bits to be sent, it might be appropriate to start investigating a standardized PHY layer which permits ultra low rate transmissions over very narrow frequency bands, with the undeniable favorable position of tremendous link budgets and subsequently altogether upgraded ranges. IEEE 802.15.4e standard is extremely suitable for a protocol stack for IoT on the grounds that it is most recent era of highly reliable and low-power Media Access Control (MAC) protocol [12].

From a networking viewpoint, the presentation of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of IETF Routing Over Low power and Lossy networks (ROLL) permitted suitable routing protocols to accomplish universal connectivity. From the transport layer and an application point of view, the presentation of the IETF Constrained Application Protocol (CoAP) protocol family has been instrumental in guaranteeing that application layers and applications themselves do not need to be re-designed to keep running over low-power embedded networks [12], [28].
A draft architecture for a middleware which gives interoperability between 6LoWPAN and outer IPv6 systems has been defined [29].

The fundamental physical and MAC layer for the 6LoWPAN protocol is the IEEE 802.15.4 standard. The 802.15.4-2006 (successor of the 2003 version) is the physical or layer 1 protocol for low-power and low rate (information exchange at 250 kbps) LLNs (Low-Power and Lossy Network). The MAC layer change to the current 802.15.4-2006 has been made called IEEE 802.15.4e to better backing the industrial markets. The key technical component of the new proposed 802.15.4e is channel hopping, which essentially increases strength against noisy and lossy systems and steady multi-path fading [30]. The application layer protocol for presenting the Web-service worldview in the Web of Things is being worked upon by the IETF Constrained RESTful Environments (CoRE) work group [31]. The

CoRE work group has characterized a REST based web exchange protocol called Constrained Application Protocol (CoAP).This protocol incorporates a few HTTP functionalities however has been re-design to consider the low processing power and energy consumption constraints of IoT gadgets [30].

2.9 Applications of IoT

A study done by the Internet of Things Initiative (IoT-i) project in 2010 identified IoT application scenarios which are gathered in 14 domains like: Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User association, Culture and tourism, Environment and Energy [32]. This study depended on 270 responses from 31 nations and the situations drawing in the most interest were: smart home, smart city, transportation and health care services [32].

2.9.1 IoT in smart home

Presently a days, smart homes are turning out to be more practical and intellectualized with proceeded progress and expense lessening in communication innovation, data innovation, and electronics, which connects the Internet with regular gadgets and sensors for interfacing virtual and physical items through the information capture and communication capacities improvement [12].

Reading of remote smart meter devices can be accomplished through the smart home frameworks. That infers, the information related with home power, data transfers, gas and water can be sent consequently to their corresponding service organization to upgrade the effectiveness of the work. Moreover, by virtue of smart home frameworks, windows, home ventilation, doors, lighting, air conditioning, etc., can be controlled by remotely. Each electronic gadget, for example, fridge, clothes washer, oven, etc., can be controlled by remote stages or programs [12]. Entertainment hardware like radios and television sets can be connected to common channels which are in remote. Furthermore, home security and health care are additionally essential parts of smart homes. For example, health help gadgets can assist a senior individual with sending demand or alert to a relative or an expert medical center. In the smart home plan, the house and its diverse electrical apparatuses have been furnished with actuators, and sensors [12].

The home gadgets functions in a nearby system however on specific events joined with a remote administration stage keeping in mind the end goal to do processing and information collection [12].

2.9.2 Privacy and security in smart grid

Any framework that assembles data and take action on it should address honest worries over privacy and security. Of these, security can comprehensively be expected to utilizing proper encryption and verification inside of the different layers of the framework. It is aided by keeping communication between a machine and its customer computer, in this way anticipating others 'hacking in' to machines. Privacy is much more complicated. At times there may be few issues, for instance few will be worried about whether their neighborhood street light is reporting an out of order bulb or not. Other application, for example, healthcare may raise profound concerns. Privacy should be tended to on an application-by-application basis and in light of showing that the application conveys advantages to the end user that unequivocally exceed any potential confidentiality security issues [33].

2.10 Technical challenges in IoT

The accompanying is a rundown of significant specialized challenges that should be tended to by middleware solutions for the IoT [34].

2.10.1 Interoperability

Interoperability can be characterized as the capacity of distinctive sorts of computers, systems, operating frameworks, and applications to cooperate successfully, so as to exchange data in a helpful and important way. The IoT represents an enormous interoperability challenge for middleware approaches following heterogeneous gadgets are relied upon to team up together in communication and data exchange. This challenge expands the exploration push to outline a middleware that can cover an extensive number of diverse sorts of gadgets, and even new sorts of gadgets that may be found later on [34].

2.10.2 Scalability

Since the IoT is required to bolster a substantial number of gadgets, scalability is by all accounts one of the significant challenges confronted by the middleware approaches. This is the consequence of having many gadgets that will communicate, yet luckily, just about in one spot [34]. A steady IoT middleware is needed to successfully oversee scalability issues so that the fundamental capacities will work effectively in both small scale and substantial scale situations [69].

2.10.3 Data volumes

While some application situations will include brief, rare communication, others, for example, sensor systems, logistics and huge scale ‘real world awareness’ situations, will involve immense volumes of information on central system nodes or servers [69].

2.10.4 ’’Arrive and operate’’

Smart regular articles ought not be seen as computers that require their clients to configure and adjust them to specific circumstances. Versatile things, which are regularly just occasionally utilized, need to build up connection quickly, and configure themselves to adapt their specific surroundings [69].

2.10.5 Spontaneous interaction

In the IoT, occasional events occur because of the unexpected quick cooperation that are brought about by the movement of things, where new objects are arriving into the remote range of different articles [34]. In this situation, middleware is required to deal with events in an ’’arrive and operate’’ mode [35].

2.10.6 Unfixed infrastructure

Not at all like the customary conveyed environment, where assets are supervised by a certain server, every gadget in the IoT ought to be equipped for declaring its presence and the assets it gives without requiring a fixed infrastructure [69]. Utilizing a dedicated server for asset administration does not work in the IoT, as a result of the high distribution and portability of gadgets. In this situation, a middleware for the IoT ought to give automated discovery of gadgets in addition to administration of assets over diverse sorts of services [34].

2.10.7 Multiplicity

Two noteworthy assortment challenges ought to be taken into the thought of the IoT middleware outline. In the first place, gadgets in the IoT are frequently required to communicate with different gadgets at the same time [69]. Second, a gadget that is taking an interest in an IoT domain is required to choose the most suitable administrations from a huge arrangement of services, in light of the fact that such gadgets will frequently depend on services that are accessible at other adjacent gadgets. Furthermore, they ought to manage the effects came back from distinctive services [34], which may negate with one another.

2.11 Technical developments for IoT

From a specialized perspective, the IoT is not the result of a solitary novel innovation. Rather, a few reciprocal specialized improvements give capacities that taken together cross over any barrier between the virtual and physical world. These capacities incorporate [69] the following:

2.11.1 Communication and collaboration

Items can coordinate with Internet assets or even with one another, to make utilization of information and services and upgrade their state. Remote advancements, for example, GSM (Global System for Mobile Communications) and UMTS (Universal Mobile Telecommunications System), Wi-Fi (Wireless Fidelity), Bluetooth (innovation standard for trading information over short separations in Industrial, Scientific and Medical (ISM) band from 2.4 to 2.485 GHz), ZigBee (worldwide remote standard to give the establishment to the IoT) and different remote networking standards right now being worked on, especially those identifying with Wireless Personal Area Networks (WPANs), are of essential pertinence here [69].

2.11.2 Addressability

Inside of an IoT, articles can be located and tended to by means of discovery, look-up or name services, and thus remotely examined or configured [69].

2.11.3 Identification

Items are individually identifiable. RFID, Near Field Communication (NFC) and optically readable bar codes are samples of advancements with which even passive objects which do not have constructed in energy resources can be recognized (with the guide of an ‘mediator’, for example, an RFID reader or cellular telephone [69]). Distinguishing proof empowers articles to be connected to data associated with the specific item and that can be recovered from a server, provided the mediator is connected with the system (figure 4).

2.11.4 Sensing

Objects gather data about their surroundings with sensors, record it, forward it or respond specifically to it [69].

2.11.5 Actuation

Items contain actuators to control their surroundings (for instance by changing over electrical signals into mechanical movement). Such actuators can be utilized to remotely control real world processes through the Internet [69].

2.11.6 Embedded information processing

Smart items highlight a processor or microcontroller, in addition to capacity limit. These assets can be utilized, for instance, to prepare and decipher sensor data, or to give items a ‘memory’ of how they have been utilized [69].

2.11.7 Localization

Smart things know about their physical area, or can be located. Global Positioning System (GPS) or the cellphone system are suitable advancements to accomplish this, and ultrasound time estimations, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known directions) and optical advances [69].

2.11.8 User interfaces

Smart items can communicate with individuals in an appropriate way (either straightforward or indirect way, for instance by means of a smartphone). Innovative communication ideal models are important here, for example, specific client interfaces, adaptable display and voice, picture or signal acknowledgment techniques [69].

Nearly all particular applications just need a subset of these capacities, especially since actualizing every one of them is frequently costly and requires important technical effort (e.g. all the activities required to implement and execute the systems engineering process). Logistics applications, for instance, are as of now focusing on the estimated localization (e.g. the position of the last read point) and generally low cost identification of items utilizing RFID.

Although, nowadays remote interchanges modules are getting to be littler and less expensive, IPv6 is progressively being utilized, the limit of flash memory chips is developing, the per guideline energy prerequisites of processors keeps on falling and cellphones have built-in bar code recognition, NFC and touch screens, and can take the part of mediator [69] between individuals, ordinary things and the Internet (figure 4).

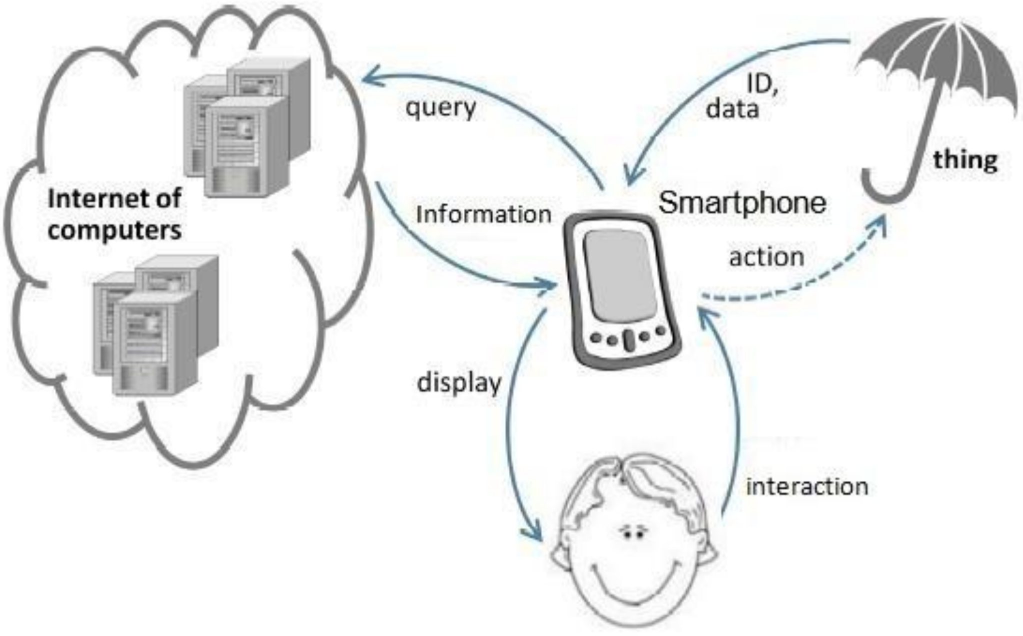

Figure 4: Smartphone as a mediator among people, things and the Internet [69]
It has been extracted from a paper that has been published in 2010

2.12 Security requirements in IoT

This section outlines the security requirements for an IoT domain and how security operation can be incorporated [36].

2.12.1 Conventional security requirements for IoT

It is expected that security of IoT will soon turn into a testing errand as IoT worldview will connect the physical world with future internet (FI). The expanding multifaceted nature of the framework will increase the quantity of security difficulties. Entire IoT services need to fulfill some essential security properties. Notwithstanding, extra security necessities for a particular IoT service may rely on upon particular applications and frameworks [36].

2.12.1.1 Data Confidentiality

IoT services may contain delicate information; in this manner, IoT associated objects information ought to be kept confidential. Secrecy can be accomplished through encryption. Diverse existing symmetric and asymmetric encryption methods can be utilized to guarantee confidentiality. In any case, determination of a specific kind of encryption is exceptionally application and gadget ability subordinate. For instance, consider a smart home environment that keeps up the data about the proprietor movement at the home. The proprietor will never welcome the way that anyone who goes to his home could read the information just by review the action observing gadget [36].

2.12.1.2 Data Integrity

IoT services deal with basic information with different administrations furthermore with the outsiders (e.g. authorities, service suppliers, control centers and so forth.), which set forward stringent request that sensed, stored and transmitted information must not be altered either malevolently or coincidentally. Honesty security of sensor information is pivotal for planning solid and reliable IoT applications. This is guaranteed with message validation codes utilizing one way hash capacities. The determination of these codes relies on upon application and gadget capacities. Consider the case of smart home that is connected with the smart grid. The smart grid supplier conveyed a power utilization checking service with a specific end goal to deliver electric bill. The supplier never needs that the utilization information can be altered amid transmission [36].

2.12.1.3 Availability

Our imagined IoT environment may involve sensor node facilitated administrations. In this way, it is critical that these IoT administrations be accessible from anyplace whenever with a specific end goal to give data (i.e., measured information, sensor alarm, and so forth.) regularly. There is no solitary security protocol that can fulfill this property. Nonetheless, distinctive down to business measures can be taken to guarantee the accessibility. Notwithstanding these conventional security properties there are additionally recognized the accompanying properties that should be tended to by any IoT environment [36].

2.12.1.4 Data Authenticity

It alludes to the methods utilized for the confirmation of one's identity. In IoT circumstance, shared verification is required on the grounds that IoT information is utilized as a part of diverse choice making and impelling procedures. Consequently, both the service supplier and administration buyer should be guaranteed that the service is access by legitimate client and service is offered by an authentic source. Moreover, solid validation method should be deployed to avoid mimic. Implementing any validation system requires to enlist client identity and resource impediment of IoT articles postures stringent limitations to empower any authentication procedure [36].

2.12.1.5 Authorization

It alludes to the method for communicating the entrance polices that expressly dole out specific consents to subjects. The IoT environment needs to give re-useable, progressive, simple to utilize polices characterizing and overhauling method. Subsequently, it is basic to externalize the approach definition and authorization component of IoT services. Besides, the asset impediment of IoT sensor node obstruct to utilize such method [36].

2.12.1.6 Access Control

This is an implementation component that permits just approved clients' access to the resources. The implementation is normally in light of access control decisions. Since, IoT is getting to be ubiquitous, protection issue has turned into a genuine concern [36]. For example, consider a smart home that has smart power metering as IoT services (smart meter is a device that use two-way communication to collect electricity usage and related information in real-time)
and without an appropriate access control instrument it could not just prompt divulgence of power use design however it could likewise offer enemy to reason client some assistance with relating data, for example, when the client is at home, at office or voyaging. Indeed, even it is conceivable to induce about the client action (i.e., staring at the TV, resting, and so forth) and home appliance present in the home. Along these lines, it is critical to reveal clients information just to authorized parties [69].

2.12.1.7 Trustworthiness

Numerous applications which are emotional in nature, for example, security basic services, social insurance administrations need to survey reliability of a few entities included. From IoT application point of view, evaluating reliability of sensors and sensor information is critical. Malicious sensor nodes and incorrect or non reliable sensor information can prompt a debacle in a security basic circumstance. Untrusted sensor information may originate from a trusted sensor node. Non-reliable conduct may have two reasons: purposeful misconduct and accidental mistakes. It may be less including so as to demand to guarantee reliability of IoT dependability appraisal highlight than by hardening the security of nodes and information through physical measures [36].

2.12.1.8 Auditing

The auditing stays informed regarding the client's collaboration with the framework. The IoT situations need to know when their administrations are accessed, who is making the service demand, when the solicitation is going on. This data will not just help in dealing with the security but additionally in assessing security hazard. If there should be an occurrence of security rupture, such data may help in distinguishing the security opening exist in the framework. Keeping up an audit record in IoT services is a challenging assignment [36].

Chapter 3: Sybil attack in Internet of Things

Sybil attack is an attack on computer framework or network in which a foe makes as various fake characters, assume as distinctive entities, and after that launch attacks through these fake personalities. Such personalities itself regularly gets to be untraceable [37].

The idea of Sybil attack was initially proposed by John Douceur in peer-to-peer (P2P) networks [38]. Sybil attack is named after the subject of the 1973 book (and later film) "Sybil", a contextual investigation of a lady determined to have numerous identity issue. The name was proposed by Brian Zill at Microsoft research lab. This attack danger is especially intense in decentralized frameworks, where it might be illogical or difficult to depend on a solitary authority to guarantee which clients are honest [37].

Sybil attacks in which an enemy forges a conceivably unrestricted number of personalities are a peril to distributed frameworks and online social networks. With Sybil nodes consisting of a substantial part of remaining nodes in the framework, the foe can take control of the framework [37].

The principle thought of the Sybil attack is to present malevolent peers, the sybils, which are all controlled by one element. Situated strategically, the sybils permit to pick up control over a small amount of the distributed system or even over the entire system. The sybils can screen the traffic (conduct of alternate peers) or misuse of the protocol in different ways. Routing requests may be sent to the wrong end-hosts or re-routed to other Sybil elements [39].

3.1 Attack and attacker

An attack can be characterized as an endeavor to extend unauthorized access to investigate, a source or data, or the try to help availability, integrity, or confidentiality of a system.

Attackers, the enemies or the intruders are the originator of an attack. The shortcoming in a framework security outline, implementation, configuration or constraints that could be abused by attackers is known as vulnerability or flaw. Any condition or occasion, (for example, the presence of an attacker and vulnerabilities) with the possibility to adversely affect a framework through a security rupture is called threat and the likelihood that an attacker will misuse a specific weakness, making harm to a framework resource is known as risk [40].

3.2 Sybil attacker

Figure 5 shows general depiction of Sybil attacker [41]. In a Sybil attack, a foe node expect numerous personalities, in this manner introducing itself to the system as various nodes. At the end of the day, a straightforward presentation of numerous personalities for a solitary physical node can be thought to be a

Sybil attack [41]. The Sybil attack can happen in a distributed system that works without a central authority to verity the personalities of every communicating entity [41].

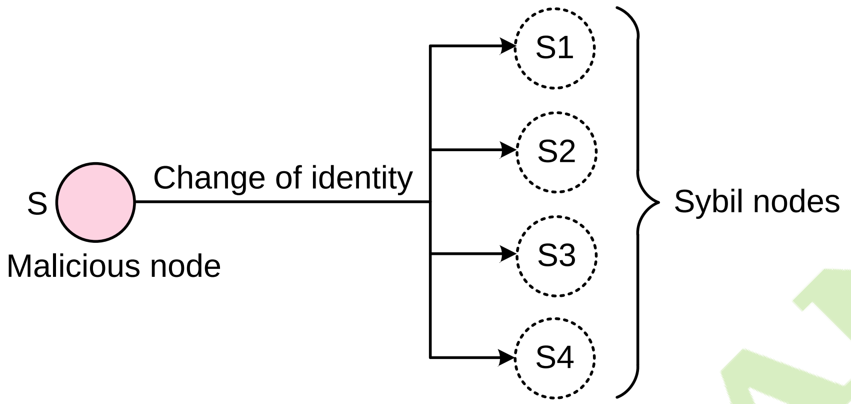

Figure 5: A Sybil attacker with multiple identities [41]

At the point when a node illegitimately asserts various characters or claims fake IDs, the system experiences an attack called Sybil attack. An attacker may produce a subjective number of extra node personalities, utilizing only one physical gadget. The node duplicates itself to make numerous copies to confuse and breakdown the system [41].

3.3 Characteristics of Sybil attacker

To better comprehend the Sybil attack, for that reason are introduced distinctive sorts of Sybil attack. The capacity of the attacker (also known as adversary) is dictated by a few characteristics: (1) direct and indirect communications, (2) stolen and fabricated identities, (3) simultaneously and non-simultaneously, (4) insider and outsider, (5) selfish and malicious, (6) busy and idle [42].

3.3.1 Direct and indirect communication

In direct communication, Sybil node which has been made by attacker and it has communicated to normal node, directly. In indirect communication, Sybil node could not straightforwardly communicate with normal node yet by support of malicious node [43].

3.3.2 Stolen and fabricated identities

Fabricated characters make new complete personalities with the help of attacker. Stolen personalities bargains from stolen the characters from honest node with help of pernicious node. It would make a new identities as same as stolen characters [43].

3.3.3 Simultaneous and non-simultaneous

Simultaneous means attacker makes various characters; those are participating in network at same time. Non-simultaneous means attacker introduces vast number of personalities over a timeframe, after fixed or variable interval of time [43].

3.3.4 Insider and outsider

Whether an attack is an insider or outsider straightforwardly concludes the ability of the attacker, and the severity of initiating a Sybil attack. Attacker holds no less than one genuine personality for an insider and claims that as though it gets certain information from alternate nodes, and that is by utilizing the fake characters. Distributed framework consider that every node is honest and along these lines expect that the false information can be efficiently sent to the entire framework. Notwithstanding, for an outsider, it is any illegal or dishonest entity; before launching or inducing a Sybil attack, it needs to first get to the framework. In any case, distributed frameworks utilize some sort of authentication to anticipate illegal access, for instance, entering a password, information encryption. The outsider requires comprehension of all mechanisms of the framework preceding to launching Sybil attacks. That is the reason distributed frameworks are more defenseless to inside attackers [42].

3.3.5 Selfish and malicious

For security similar issues, there are two sorts of attackers: either selfish or malicious. Selfish attackers control the false information only for their own advantage, while malicious attackers endeavor to threaten or weaken a system. In case an attacker is selfish or malicious is normally controlled by the distinctive sorts of targeted distributed system and also by final attacking consequences. For example, if the attacker has asset accessing rights all to itself, then certainly it is a malicious attacker, on the grounds that others cannot utilize the asset. Be that as it may, if different clients can likewise get to the asset with a littler measure of likelihood, then it is selfish attacker. Since malicious attacks for the most part have considerably more genuine impacts, it is of more noteworthy significance to secure against conceivably malicious attacks than that of possibly selfish attacks [42].

3.3.6 Busy and idle

All Sybil personalities can take part in a distributed framework at the same time, or just some of them can work, while others are in an idle state [42]. Basically, the determination of these two plans is controlled by how inexpensive it is to acquire a personality. On the off chance that the attacker can undoubtedly get adequate of fake personalities, some Sybil nodes that are idle could make them all the more genuine, as a legitimate node may leave or re-enter the framework several times. In any case, the effort of Sybil attacks results from the quantity of the characters.

Getting a substantial number of personalities is extremely troublesome, then the attacker must utilize every one of them with a specific end goal to launch or induce an effective attack [37].

3.4 Creation of Sybil nodes in sensor network

There are a few approaches to make Sybil nodes in sensor systems based upon the characteristics of the attacker, for example, communication, simultaneity and fabricated identities. It demonstrates that when one of the nodes communicate with other node (i.e. one hop communication) all things considered any compromised node get the access from normal node and it would be effectively to get the data's from normal node, for example, position, ID, and so forth, by utilizing this parameters attacker would be make a same kind of characters and set up the attacks to normal node, finally it will confuse and corrupt the networks [43].

3.5 Normal node makes redundant backup

The term redundant portray computer or network system segments, such as hard disk drives, servers, operating systems, switches and telecommunication links that are installed to backup primary resources in case they collapse.

As shown in figure 6, when an ordinary node makes system redundant backup, it chooses a gathering of elements, for example, node S1, S2, S3 and S4 that have distinctive identities. However, indeed, node S1, S2, S3 and S4 really do not exist, in light of the fact that they are the malicious nodes made by the attacker AD, so the backup cannot complete [44].

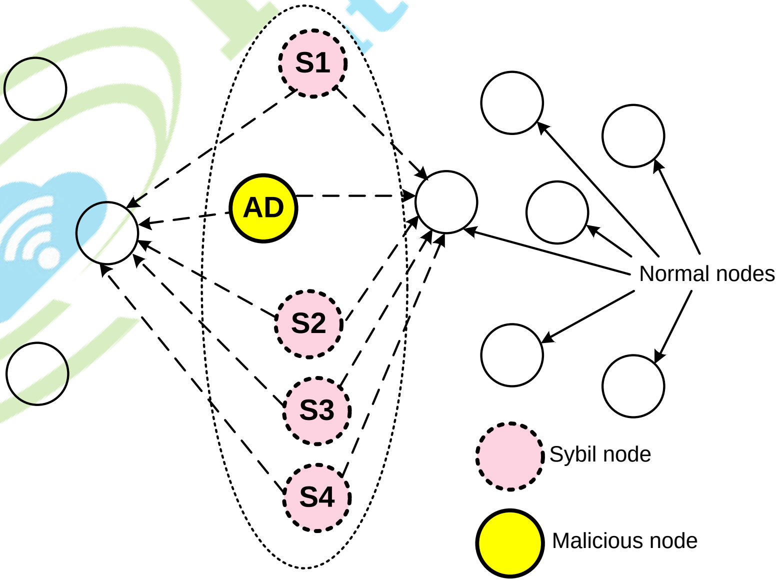

Figure 6: Normal node makes redundant backup [44]

A pernicious node or a foe node (AD) may show different fake personalities to a distributed system so as to show up and work as various unmistakable nodes.

In the wake of turning out to be a piece of the P2P system, the foe may act malevolently. By disguising and introducing various personalities, the foe can control over the entire system [44].

Redundancy lets distributed frameworks compensate for faulty nodes like for instance store information on different nodes. The Sybil attack undermines redundancy [45].

3.6 Sybil attack

Most protocols expect that nodes have a solitary one of a kind character in the system. In a Sybil attack, a solitary node exhibits different characters to different nodes in the system. This can be creating so as to persuade fake personalities of nodes situated at the edge of communication extent. Various characters can be involved inside of the sensor network either by creating or taking the personalities of real nodes [40].

Figure 7 demonstrates Sybil attack where an adversary node ‘AD’ is present with multiple identities. The adversary ‘AD’ shows up as node ‘F’ for 'A', ‘C’ for ‘B’ and ‘A’ as to ‘D’ so when ‘A’ needs to communicate with ‘F’ it sends the message to ‘AD’ [40].

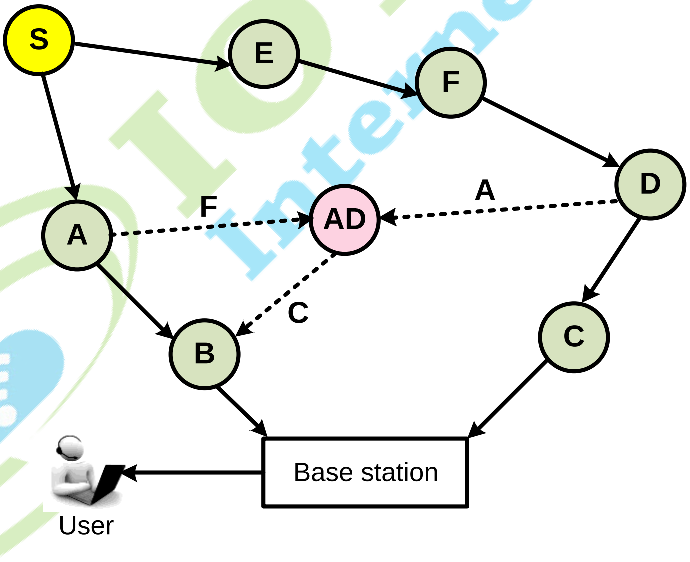

Figure 7: Sybil attack with an adversary node ‘AD’ presents with multiple identities [40]

The Sybil attack can disturb ordinary working of the sensor system, for example, multipath routing, used to investigate the numerous disjoint paths between source to destination sets. It can essentially decrease the viability of fault tolerant plans, for example, distributed storage, multipath routing and topology maintenance [46].

Sybil attack additionally represents a critical risk to geographic routing protocols. Location aware routing frequently obliges nodes to interchange coordinate data with their neighbors to efficiently route geographically addressed packets. It is just sensible to anticipate that a node will acknowledge a solitary set of coordinates from each of its neighbors, but by utilizing the Sybil attack an adversary can ‘’be in more than one spot at once’’ [46].

3.7 Defenses against the Sybil attack

In figure 8 are delineated the distinctive sorts of defenses against Sybil attacks [47].

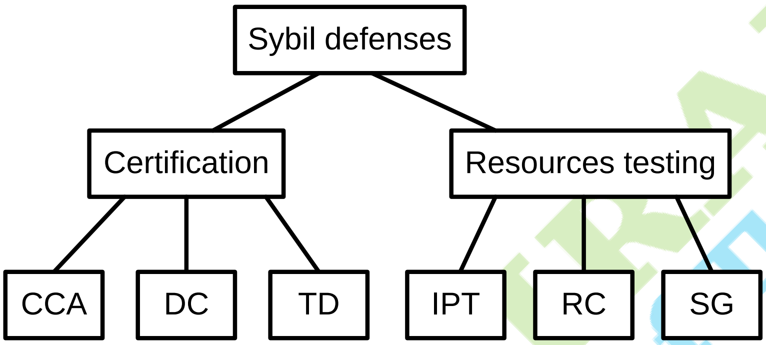

Figure 8: An illustration of different types of defenses against Sybil attacks [47]

The acronym terms used in figure 8 are as the following:

CCA – centralized certification authority

DC – decentralized cryptographic

TD – trusted devices

IPT – IP testing

RC – recurring cost

SG – social graph-based approach

3.7.1 Defenses using Trusted Certification

The trusted certification methodology is apparently the most famous system in the setting of this study, subsequent to Douceur [38] demonstrated its capability to eliminate the Sybil attack. In the ordinary type of this methodology, a centralized authority guarantees that the personalities assigned to every peer are exclusive and legitimate by matching these characters to pre-allocated certifications. These accreditations may incorporate cryptographic keys, synchronized random strings that are typically produced by one-time password generators, or digital authentications issued by the centralized authority [47].

3.7.1.1 Centralized certification authority

Central trust authority is one of the efficient Sybil defense methods in which an outsider is utilized to authenticate the nodes. In central trust authority, a node is said to be honest if get a certificate from the central server [48]. In true, such certification can be an uncommon equipment gadget or a digital number. Prior to a member joins a peer-to-peer framework, its character must first checked by the central server [49]. For instance, when somebody is applying for a bank automated teller machine (ATM) card, it is asked for to provide personal social security number for authentication [49].

Brought together trusted certification schemes are regularly actualized by asymmetric cryptography, (for example, public/private keys). They expected that every node imparts an one of a kind symmetric key to a trusted centralized base station. In the wake of checking the legitimacy of one another, a couple of nodes can build up a shared key. Amid information transmission between adjacent nodes, they can utilize the key for common verification and approval, and can likewise encrypt the information [49].

However the central trust technique appeared to be encouraging, it represents a considerable measure of issues. Firstly, it is troublesome for every one of the nodes in huge distributed systems to trust the central party. Secondly, as the central server is included in every last step, it could be overloaded with an excess of service solicitations. Thirdly, the central server turns into the solitary purpose of attack and if by any methods in the event that it is put in peril, the entire framework would collapse and it may get to be very difficult to identify Sybils in the system [48].

3.7.1.2 Decentralized cryptographic primitives

Cryptographic primitives are entrenched, low-level cryptographic algorithms that are oftentimes used to assemble cryptographic protocols for computer security frameworks [47]. These schedules incorporate, however are not restricted to, one-way hash functions and encryption functions. (one-way hash function is a numerical function which takes a variable length input string and changes over it into a fixed-length binary sequence; a hash function which is considered basically impossible to invert, that is, to reproduce the information from its hash value alone); (e.g. encryption function is a kind of public key encryption in which having a secret key permits one to learn a function of what the ciphertext is encrypting).

Some work with cryptographic primitives has been done [50], [51]. These primitives go for giving a foundation to verifying peers with a specific end goal to make the Sybil attack harder to apply by having just honest peers participate in the overlay. For the most part, this work tries to misuse a public key base in a distributed way utilizing threshold cryptographic components (e.g. secret sharing and threshold signatures) keeping in mind the end goal to guarantee coordinated effort among evidently genuine clients to authenticate peers that join the overlay over its operation time [47]. Interestingly, the unequivocally expressed inspiration past some of these primitives [50], [52] is that a large portion of the non-cryptographic protocols in the literature expect the presence of a confirmation framework for authentic clients in the overlay (e.g. SybilGuard and SybilLimit). Therefore, the cryptographic methodologies are intended to guarantee effective operation of such protocols [47].

3.7.1.3 Trusted devices

Like the thought of trusted accreditation, some examination proposed the utilization of trusted gadgets or trusted modules that store certificates, keys, or authentication strings beforehand allocated to clients by a centralized authority. Such gadgets are difficult to acquire due to their conceivably high cost, and thus can be utilized to cutoff open doors for Sybil attacks. Cases of such instruments are proposed by Rodrigues et al. [53] and Newsome et al. [54], in spite of the fact that the last work is on remote sensor systems. In principle, when the plan of the attacker is known ahead of time, these defenses may be persuasive [47].

3.7.2 Defenses using resource testing

Resource testing is the most generally actualized answer for turning away Sybil attacks. The fundamental standard is that the quantum of figuring assets of every entity on the system is constrained. Typically, every client can have one and only personality, and every character should work on a solitary machine [49].

On the other hand, when Sybil attacks are begun, the Sybil characters work on a solitary framework. When are given a few limitations like time or asset expending assignments to a gathering of characters, on the off chance that they can finish the work inside of an edge, then it is most conceivable that they are honest nodes, else it can contain some Sybil nodes. All in all, the objective of resource testing is to figure out if the chosen characters have a reasonable measure of resource [49].

3.7.2.1 IP testing

Generic testing schemes incorporate testing the IP address of peers, attempting to decide their locations and coordinating them to their exercises. Specifically, if a sure measure of action is produced from the same geographic zone, it is likely that some of this activity is because of Sybil characters [47]. In addition, the fundamental supposition in such work is that it is not cheap to acquire IP addresses in distinctive geographic wide ranges.

In any case, with pointers for the presence of huge botnets [55], and also compromised hosts under control of a solitary entity and residing in distinctive autonomous frameworks, it is very sure that such protection methods are useless [55]; (e.g. botnet is a group of computers connected in a planned manner used to transmit malware or spam, or to launch attacks).

3.7.2.2 Recurring cost

Some work has suggested recurring cost as a method of defending against the Sybil attack. Specifically, computational puzzles [56], [57], and Turing tests are proposed as quick fix [48]; (e.g. in artificial intelligence, the Turing test is a technique for figuring out if or not a computer is equipped for taking on a similar mindset as a human).

Other comparative handy arrangements that are broadly utilized are telephone numbers (like Google email checking) or email addresses (as in social network site enrollments). On the other hand, for the same reason that IP testing would not conflict with an attacker that controls a botnet, these expense based methods will not fill in too [47].

3.7.2.3 Social network-based Sybil defense

While the greater part of the already proposed answers for a Sybil attack in distributed systems have constraints and deficiencies in somehow, social network–based Sybil defenses attempt to overcome such weaknesses in a few subtle ways [6].

In the first place, social network–based Sybil defenses are generally decentralized answers for a Sybil attack, which implies these plans work with no centralized authority, a component that is exceedingly attractive and vital in most distributed frameworks. This decentralized model is further made simpler on account of the random walk theory, a fixing method for the most part used in these defenses [6].

Second, these defenses use trust of the social connections among social nodes, making cooperation among fair nodes conceivable and simple [6]. Third, these protections were appeared in a few studies [58], [59], to be pragmatic and successful in defending against Sybil attacks with ease and are further created as parts in numerous administrations, including distributed hash tables (DHT) and Sybil voting, and are used in mobile system routing [6]; (e.g. DHT - is a class of a decentralized distributed framework that gives a lookup service like a hash table: (key, value) pairs are stored in a DHT).

In spite of the fact that they contrast incredibly in their configuration points of interest and operation, all social network–based Sybil defenses have two basic presumptions: an algorithmic property (called the fast mixing property) and trust.
To start with, these protections depend on the fast mixing property of social graphs. Casually, the fast mixing property of the social graph suggests that the honest nodes in such a graph are all affected, and the honest region does not

contain a sparse cut (a cut that link two vast subsets of legitimate nodes with a couple of social connections) [6].

The second assumption normal to this kind of defense is trust. Specifically, these defenses accept a high trust value in the fundamental social graphs, as demonstrated, for instance, by up close and personal collaborations among the nodes. This specific presumption is important with a specific end goal to decide the trouble of invading the inducing the social network by self-assertively setting up numerous attacker social connections [6]. While the operation of a Sybil defense to accurately distinguish honest nodes in the social graph is ensured by the fast mixing assumption, and the development of the relating plan that uses such an algorithmic property, the ability to recognize Sybil nodes is just ensured accepting that the attacker control a couple joins amongst themselves and other legitimate nodes in the social graph. Such connections are called attack edges [6].

3.8 Social networks as one aspect in IoT

Distributed systems are defenseless against malevolent attacks where an adversary professes to have different personalities. This kind of attack is known as Sybil attack and such personalities are known as Sybil characters [60]. Sybil attack can exceedingly impact the working of open enrollment frameworks, for example, Facebook, Twitter, Google+, and so on.

Customary methodology for counteracting Sybil attacks relay on trusted authorities, when certify personalities. Be that as it may, requesting that clients present credentials, for example, social security numbers or other trusted personalities will influences the achievement of open enrollment frameworks. In any case, these prerequisites includes additional burdens on clients, it seriously influences clients aim to join these frameworks [60].

There are two sorts of Sybil defense systems, centralized and decentralized. Defending against Sybil attacks utilizing a centralized approach is much harder. One least complex methodology is to bind nodes to IP addresses. Be that as it may, it can just give restricted security against attacks. Using social network topologies is an approach to defend Sybil attacks [60].

3.8.1 Social graph

Mathematicians have created graph theory keeping in mind the end goal to concentrate a wide range of systems [61]. A set is a collection of objects. These articles are called elements of the set. A graph is a set of objects joined by lines. Items can be anything: numbers, individuals, different sets, and so on. The items in a diagram are typically called nodes or vertices. The lines joining the items are generally called connections or edges [61].

All the more formally, a chart G is characterized as a requested pair *G* = (*V*, *E*) where

- *V* is a set of vertices (nodes)
- *E* is a set of edges (links)
- Each edge is a pair of vertices. At the end of the day, every element of *E* is a pair of elements of *V*

In a direct graph, the two directions are counted as being distinct directed edges. In a direct graph, edges are composed utilizing parenthesis to mean ordered pairs. For instance, edge (2, 3) is guided from 2 to 3, which is not quite the same as the coordinated edge (3, 2) from 3 to 2. Directed graphs are drawn with arrowhead on the connections, as appeared in figure 9(a).

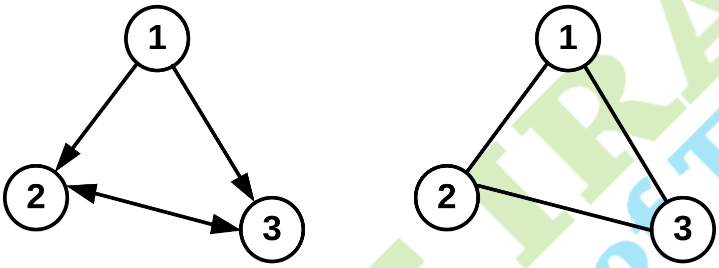

Figure 9: (a) Directed graph [61] (b) Undirected graph with three vertices and three edges [61]

Undirected graph (figure 9(b)) is a graph where the edges of a graph are assumed to be unordered pairs of vertices, which are usually called edges, arcs, or lines [61].

3.8.2 Sybil Defense in Online Social networks

Consider a system topology G = (V, E), involving an arrangement of vertices (or nodes) V with an arrangement of edges E. In social network topologies, a node *v* ∊ *V* signifies a client on the system, and an edge (*u*, *v*) ∊ *E* means a friendship relationship between two clients *u* and *v*. Here are just considered common connections, subsequently (*u*, *v*) ∊ *E* is proportional to (*v*, *u*) ∊ *E* and G is an undirected graph [62]. The edges associating the honest region (i.e., the area containing all the legitimate nodes) and the Sybil region (i.e., the area containing all the Sybil characters made by malicious clients) are called attack edges [62].

Figure 10 delineates the social network with honest nodes, Sybil nodes and attack edges [63].

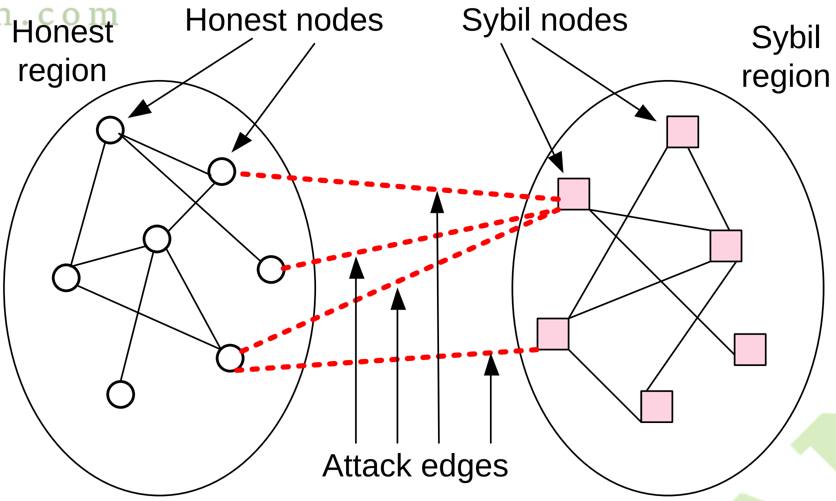

Figure 10: Social network with honest nodes, Sybil nodes and attack edges [63]

3.8.3 Defense mechanisms against Sybil attacks

To secure against Sybil attacks, it is important to accept that every node character is the main personality displayed by the relating physical node. There are two sorts of approaches to validate node personality. The main sort is called direct validation, in which a node straightforwardly tests if another node character is legitimate. The second sort is called indirect validation, where nodes that have as of now been confirmed or checked are permitted to guarantee for or demonstrate false different nodes [37].

3.8.3.1 SybilGuard

Haifeng Yu et al. (2008), in their analysis paper have presented SybilGuard [64]. SybilGuard is a novel decentralized protocol for diminishing the terrible impacts of Sybil attacks, by bouncing both the number and size of Sybil groups. This protocol depends on the social network between client characters, where an edge between two personalities determines a human built up trust relationship.
Despite the fact that malevolent clients can make numerous characters however they can have few trust connections [64]. In this way, there is a disproportionality small cut in the diagram between the fast mixing honest region and the Sybil area (figure 11). SybilGuard makes utilization of this property to bind the quantity of characters a pernicious user can make. SybilGuard depends on these properties of the clients fundamental social network, specifically that (1) the honest region of the network is fast mixing, and (2) malevolent users may make numerous nodes however generally few attack edges [64].

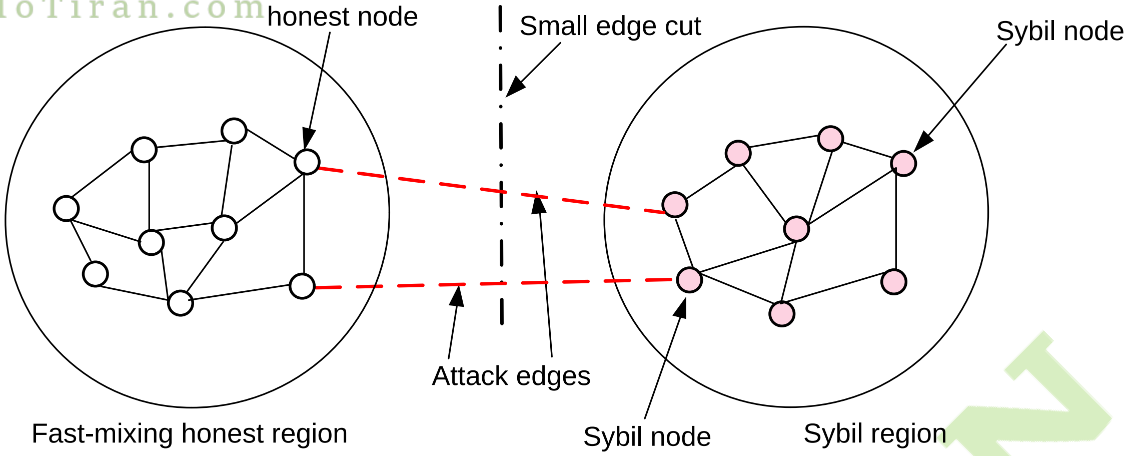

Figure 11: Sybil detection relies on the small edge cut between the fast mixing honest region and the Sybil region [67]

The current SybilGuard outline depends on the fast mixing property of social networks. In the event that the social networks is not fast mixing, SybilGuard will at present appropriately bound the quantity of acknowledged Sybil nodes inside with high probability [37]. The main drawback of a slower mixing social network is that more honest nodes will be mistakenly repudiated [64].

SybilGuard ensures that a genuine node acknowledges, furthermore is acknowledged by, most other legitimate nodes with high probability. In this way, a genuine node can effectively get service from, and give service to, most other honest nodes [37].

3.8.3.2 SybilShield

SybilShield is a novel decentralized defense protocol against Sybil attacks in social networks which constrains the negative impacts of tolerating Sybils erroneously and mislabeling honest nodes [37]. SybilShield depends on basic properties of real world social networks that the non-Sybil regions are fast mixing and the quantity of attack edges made by a foe is generally not exactly that of foreign edges among honest groups, which are approved on the given MySpace (a social networking website) topology information pattern. Motivated by these social networks properties, with help of agent nodes SybilShield considerably decreases false positive rate of non-Sybils among different groups, while viably recognizing Sybil nodes [37]. Through the hypothetical probability examination and investigations on the MySpace information set, SybilShield is appeared to significantly outperform SybilGuard, decreasing the false positive rate while keeping the viability of distinguishing Sybil nodes with an adequate acknowledgment [37], [65].

An edge between two distinct groups is known as a foreign edge. It additionally accept that social networks are fast mixing, i.e. despite the fact that if an enemy makes huge number of Sybil characters, the quantity of trust connections built up between a honest node and a Sybil node is constrained. In this way, foreign edges shaped between honest communities are more when compared to honest and Sybil communities [37].

Figure 12 portray the different communities in real world social networks with foreign edges.

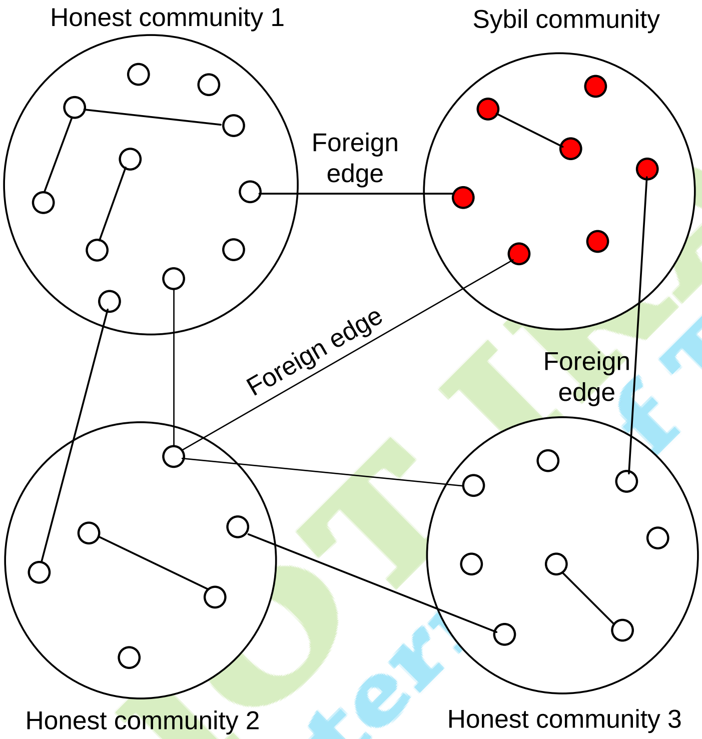

Figure 12: Different communities in real world social networks with foreign edges [48]

3.8.3.3 Sybil Defender

Sybil Defender is a Sybil defense method that influences the system topologies to defend against Sybil attacks in social networks [49]. Taking into account performing a minimum number of random walks within the social graphs, Sybil Defender is most proficient and it is adaptable to vast social networks. Sybil Defender can viably recognize the Sybil nodes and identify the Sybil community around a Sybil personality, notwithstanding when the quantity of Sybil nodes presented by every attack edge is near the hypothetically perceptible lower bound. Sybil Defender [49] comprises of two segments:

- Sybil node recognizable identification algorithm.
- Sybil bunch around that Sybil node detection algorithm.

3.8.3.4 SybilLimit

SybilLimit is an ideal defense against Sybil attacks with the utilization of social networks [37].

SybilLimit's advancement gets from the combination of various novel procedures: (1) utilizing numerous free cases of the random route protocol to accomplish numerous short random routes; (2) misusing crossing points on edges rather than nodes; (3) utilizing the novel equalization condition to manage getting away tails of the verifier [37], and (4) utilizing the novel standard strategy to securely evaluate [58].
At last, comes about on real world social networks affirmed their fast mixing property and along these lines it has likewise approved the central assumption behind SybilLimit's and SybilGuard's methodology.

SybilLimit [59] exhibited another protocol that influences the same knowledge as SybilGuard yet offers drastically enhanced and near optimal insurances. The protocol name is SybilLimit on the grounds that: (1) it confines the quantity of Sybil nodes acknowledged, and (2) it is near ideal and hence pushes the approach to the limit [37].

3.8.3.5 SyMon

SyMon is a novel method to defend against Sybil attacks in distributed decentralized systems [49]. It guarantees honest nodes are shielded from Sybils with high probability. In SyMon, every solitary node in the system is connected with a non-Sybil called as SyMon (Sybil Monitor). The non-Sybil or SyMon is picked progressively, such that the possibility of both nodes being Sybils is incomprehensible. Each SyMon is given the obligation of checking the activities of the given node making it unimaginable for the other node to put in risk the framework. A SyMon ought to ensure that a malevolent node needs to contribute a considerable measure of expense to make a fake personality. What is more, in SyMon approach any node in the system can confirm with high probability whether a pair nodes are Sybils or not [48].

3.8.3.6 Summary for proposed Sybil defense methods

Many researchers have proposed defense strategies like SybilGuard, SybilLimit, SybilShield, SybilDefender, SyMon [37]. These types of defense systems against Sybil attacks have been compared against each other, and a summary follows. SybilGuard is a protocol for restricting the harmful impacts of Sybil attacks and limits the quantity of personalities a malicious user can make. SybilLimit protocol enhances SybilGuard's constrain by utilizing limited numbers of random walks, tolerating less Sybil personalities per attack edge. SybilShield is the first protocol that defend against Sybil attack utilizing multi-community social network structure in real world. SybilDefender is a defense method that influences the system topologies to secure against Sybil attacks in social networks and is productive, adaptable to vast social networks, taking into account performing a set number of random walks inside of the social graphs. SyMon superior defense method in huge structure peer-to-peer frameworks where it relate each peer with another non-Sybil peer known as SyMon, arbitrate the exchanges including the given peer and henceforth makes it practically unimaginable for sybils to compromise the framework [37].

3.9 Sybil attacks in online social networks

Sybil attacks happen in the IoT to maliciously control the frameworks. In the social graph, makes utilization of node to represent user, identity, or account in the real network. The edge between each pair of two nodes is weighted by their social connections. An attack edge is the edge associating an honest node and a Sybil node [66], as appeared in figure 13.

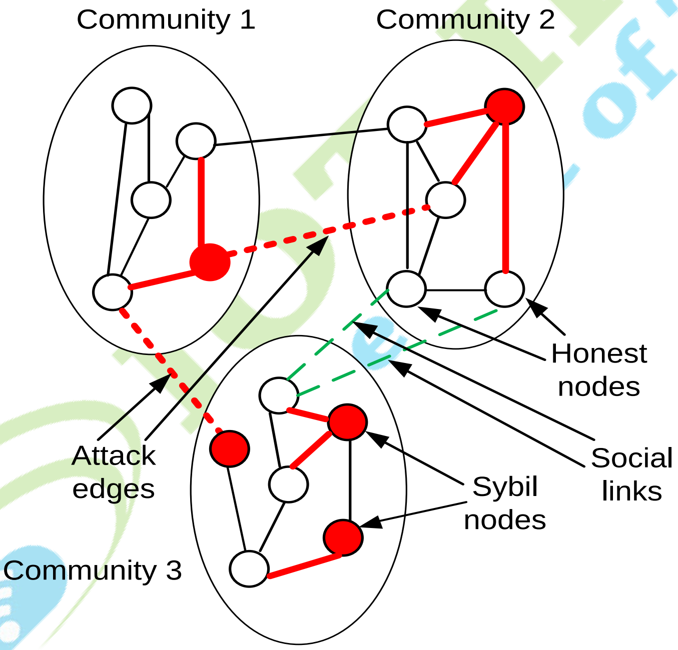

Figure 13: Sybil attack in online social networks [66]

Sybil attackers are commonly present in social networks. Sybil attacker can manufacture the social associations among Sybil ways of life as well as with the typical clients. At the end of the day, the ability of Sybil attacker is solid to mirror the typical client's social structures from the point of view of social graph. Hence, the quantity of attacks edges is vast [66].

The objective of Sybil attacker is to spread spam, advertisements, and malware, take and disregard client's security, and perniciously control the reputation framework. For instance, in online social systems, Sybil attacker can produce the profiles and companion list as ordinary clients, however deliberately spread spam, commercials, and malware. Moreover, Sybil attacker could create a lot of positive audit remarks in a service assessment framework to misrepresent the benefits of service, or produce numerous negative remarks to criticize services [66]. Clearly, Sybil attacker would concentrate on some particular practices and repeat them several times.

Unique in relation to sensing area going for natural checking, social domain gives the IoT applications to encourage the social connection among clients.

Driven by the comparative concerns, clients could form virtual online group to interchange data and offer share multimedia assets. For the most part, clients in social domain have the Internet access and can cooperate with both the online servers and different clients. Clients in social domain can look at the attractive content, discover the breaking news, and offer data or content with their social companions [66].

3.10 Different defense solutions proposed against Sybil attacks

A few methodologies have been proposed in different research papers against Sybil attacks. The diagram in figure 14 demonstrates the synopsis [68].

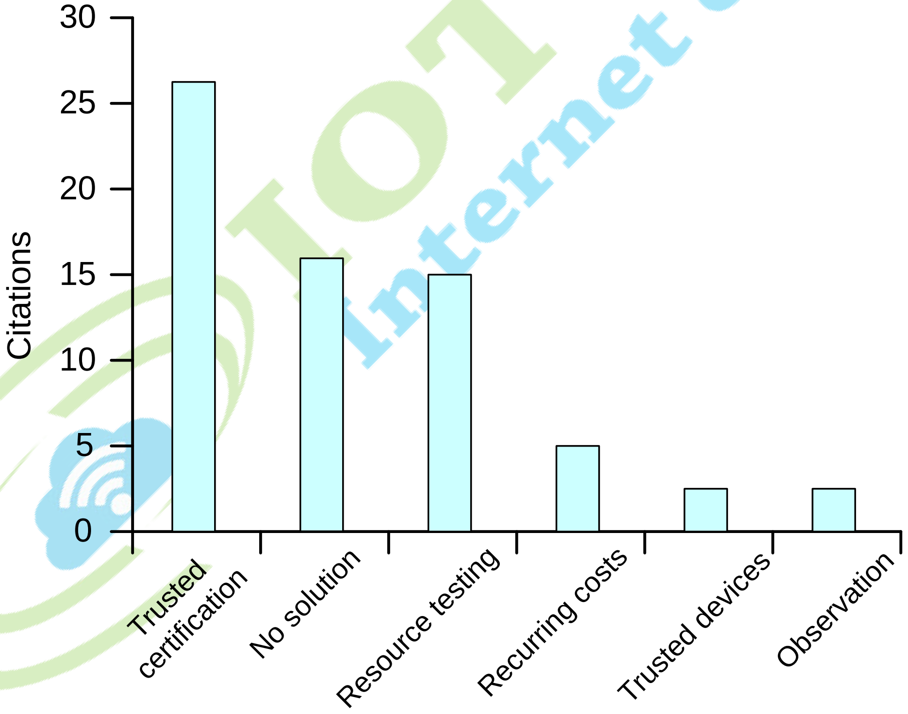

Figure 14: Sybil attack approaches in the literature, summarized [68]
It has been extracted from a paper that has been published in 2006

Since the first investigation of the Sybil attack, somewhere in the range of eleven diverse methodologies have been proposed to avoid or relieve the attack. In [68] Levine et al., refers to the 90 articles which specify either the

Sybil attack or pseudo-spoofing (a prior term for the utilization of numerous false personalities) and depict every methodology. Around half of the distributed papers either propose certification as an answer for the Sybil attack, taking after Douceur's methodology, or basically express the issue without giving an answer [68]. The remaining papers utilize one of nine particular techniques. In figure 14 is shown the quantity of references for distinctive ways to deal with the Sybil issue [68].

Douceur [38] has demonstrated that trusted certification is the only approach that can possibly totally kill Sybil attacks. Appropriately, it is referred to as the most well-known solution. In any case, trusted certification depends on a centralized authority that must guarantee every entity is assign precisely one personality, as demonstrated by ownership of a certificate. Truth be told, Douceur offers no method for guaranteeing such singularity, and realistic it must be performed by a manual or an individual procedure. This may be exorbitant or make an execution bottleneck in expansive scale frameworks. In addition, to be viable, the certifying authority must guarantee that lost or stolen characters are found and revoked. In the event that the execution and security suggestions can be solved, then this methodology can eliminate the Sybil attack [68].

Conclusions and future work

Sybil attacks, in which an adversary produces a conceivably unbounded number of personalities, are a peril to distributed systems and online social networks in the IoT. Douceur [38] showed that without the usage of a brought together centralized authority that certifies all nodes, it is hard to counteract Sybil attack. Sybil attack is a key issue in various frameworks, and it has so far prevented an all around pertinent agreement. In this thesis, I have presented a comprehensive literature review on the IoT and security challenges and issues of the IoT system. I have also listed important techniques that have been proposed to defend against the Sybil attacks. Diverse proposed defense procedures have been scrutinized, explored and thought about against one another. In this thesis I have attempted to answer how Sybil node is created. I also explained about characteristics of Sybil node.

For the purpose of future work, I propose to develop a method in order to strengthen user authentication and authorization process, using the two-factor authentication (2FA) technology, applicable to smart meter devices in IoT.

References

[1] Internet of Things (IoT), https://en.wikipedia.org/wiki/Internet_of_Things

[2] FTC report on Internet of things, Privacy and security in a connected world, 2015

[3] M. Malik, An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations, Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management DOI: 10.4018/978-1-4666-0101-7.ch024

[4] Pooja, Manisha, Dr. Yudhvir Singh, Security Issues and Sybil Attack in Wireless Sensor Networks

[5] Sahabul Alam, Debashis De, Analysis of security threats in wireless sensor network, International journal of wireless & mobile networks, vol. 6, no. 2, April 2014

[6] Aziz Mohaisen, Joongheon Kim, "The Sybil attacks and defenses: A survey", Smart Computing Review, vol. 3, no. 6, December 2013

[7] Eric Fisher, Internet of Things: Frequently asked questions, 2015

[8] Enrique Ortiz, M2M vs. Internet of Things, 2010

[9] Chantal Polsonetti, Know the difference between IoT and M2M, 2014

[10] Jim Stogdill, M2M, IoT, and the invisibility of ubiquity, 2014

[11] What is the difference between M2M and IoT?, 14 May 2013, https://m2m.telefonica.com/blog/what-is-the-difference-between-m2m-and-iot

[12] J. Sathish Kumar, Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887), Volume 90 – No 11, March 2014

[13] A. Dunkels. Full TCP/IP for 8-bit Architectures. In Proceedings of the 1st International Conference on Mobile Systems, Applications, and Services, MobiSys, pages 85–98, San Francisco, CA, USA, 2003

[14] Z. Shelby, P. Mahonen, J. Riihijarvi, O. Raivio, and P. Huuskonen. NanoIP: The Zen of Embedded Networking. In Proceedings of the 2003 IEEE International Conference on Communications, ICC, pages 1218–1222, Anchorage, AK, USA, 2003

[15] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs), IEEE Std 802.15.4-2003, 2003

[16] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), Sept. 2007, Updated by RFCs 6282, 6775

[17] Z. Shelby, S. Chakrabarti, E. Nordmark, C. Bormann. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 6775 (Proposed Standard), Nov. 2012

[18] D. Lund, C. MacGillivray, V. Turner, Worldwide Internet of Things (IoT) 2014–2020 Forecast: Billions of Things, Trillions of Dollars. Market Analysis 243661, IDC, 2013

[19] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context Aware Computing for the Internet of Things: A Survey” IEEE Communications Surveys & Tutorials, 2013

[20] ITU internet report 2005: The Internet of things, executive summary

[21] N. Bari, G. Mani, S. Berkovich, "Internet of things as a methodological concept," in Computing for Geospatial Research and Application (COM. Geo), 2013 Fourth International Conference on, 2013, pp. 48-55

[22] Y. Kang, Z. Zhongyi, Summarize on Internet of Things and exploration into technical system framework, in Robotics and Applications (ISRA), 2012 IEEE Symposium on, 2012, pp. 653-656

[23] Anas M Mzahm, Mohd S Ahmad, Alicia Y.C. Tang, Enhancing the Internet of Things via Concept of Agent of Things, Journal of Network and Innovative Computing, ISSN 2160-2174 Volume 2 (2014) PP.101-110

[24] Y. Huang, G. Li, "A semantic analysis for internet of things," in Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on, 2010, pp. 336-339

[25] T. Fan and Y. Chen, "A scheme of data management in the Internet of Things," in Network Infrastructure and Digital Content, 2010 2nd IEEE International Conference on, 2010, pp. 110-114

[26] G. Gang, L. Zeyong, and J. Jun, “Internet of Things Security Analysis,” 2011 International Conference on Internet Technology and Applications (iTAP), 2011, pp. 1-4

[27] C. Xiang, X. Li, "General analysis on architecture and key technologies about Internet of Things," in Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on, 2012, pp. 325-328

[28] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, "Standardized protocol stack for the internet of (important) things," Proceedings of IEEE, 2012, pp. 1-18

[29] K. Kim, S. Yoo, H. Kim, S. D. Park and J. Lee, "Interoperability of 6LoWPAN," draft-daniel-6lowpan-interoperability-01, IETF, vol. 7, 2005

[30] Ronak Sutaria, Raghunath Govindachar, "Making sense of interoperability: Protocols and Standardization initiatives in IoT", 2013

[31] Z. Shelby, K. Hartke, C. Bormann and B. Frank, "Constrained application protocol (coap)," draft-ietf-corecoap-07, 2011

[32] O. Vermesan, P. Friess, A. Furness, The Internet of Things 2012, By New Horizons, 2012

[33] W. Webb, Understanding the world of connected machines: Making sense of Internet of Things

[34] Moumena A. Chaqfeh, Nader Mohamed, "Challenges in Middleware Solutions for the Internet of Things", 2012

[35] K. Paridel, E. Bainomugisha, Y. Vanrompay, Y. Berbers, W.D. Meuter, "Middleware for the Internet of Things, design goals and challenges", ECEASST Journal, ISSN 1863-2122, 2010

[36] Sarfraz Alam, M.R. Chowdhury, Josef Noll, "Interoperability of Security-Enabled Internet of Things", Wireless Pers Commun (2011) 61:567–586, DOI 10.1007/s11277-011-0384-6

[37] Snehal Pise, Ratnaraj Kumar, Recent Trends in Sybil Attacks and Defense Techniques in Social Networks, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 1, January - 2014

[38] J.R. Douceur, The Sybil attack. In First International Workshop on Peer-to-Peer Systems (IPTPS '02), Mar. 2002

[39] Moritz Steiner, Taoufik En-Najjary, Ernst W. Biersack, Exploiting KAD: Possible Uses and Misuses

[40] R.S. Jigalur, Dr. Suresha, "Reviewing Security Issues, Attacks, and Countermeasures in WSN" https://www.academia.edu/6721469/Reviewing_Security_Issues_Attacks_and_Countermeasures_in_WSN

[41] A. Vasudeva, M. Sood, "Sybil attack on lowest ID clustering algorithm in the mobile ad hoc network", International Journal of Network Security & its Applications (IJNSA), Vol.4, No.5, September 2012

[42] Wei Chang, Jie Wu, A Survey of Sybil Attacks in Networks

[43] Abirami K, Santhi B, Sybil attack in Wireless Sensor Network, International Journal of Engineering and Technology, ISSN: 0975-4024, Vol 5, No 2, Apr-May 2013

[44] Chirag Parmar, Chaita Jani, A Survey On Peer-to-Peer Network Attacks and Defenses, International Journal for Innovative Research in Science & Technology, Volume 1, Issue 7, December 2014, ISSN (online): 2349-6010

[45] Orhan Umut Eryılmaz, SybilGuard: defending against Sybil attacks via social networks

[46] C. Karlof, D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003

[47] Neha Gahlot, Survey on Sybil Attacks and its Defensive Measures, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 6, June 2015

[48] Rupesh Gunturu, "Survey of Sybil Attacks in Social Networks"

[49] Rakesh G.V, Shanta Rangaswamy, Vinay Hegde, Shoba G, "A Survey of Techniques to Defend Against Sybil Attacks in Social Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014

[50] F. Lesueur, L. Me, V. V. T. Tong, –An efficient distributed PKI for structured P2P network, **‖** in Proc. of IEEE P2P, pp. 1-10, 2009

[51] A. Avramidis, P. Kotzanikolaou, C. Douligeris, –Chord-PKI: Embedding a public key infrastructure into the chord overlay network,**‖** in Proc. of EuroPKI, pp. 354-361, 2007

[52] F. Lesueur, L. Me, V. V. T. Tong, —A Sybilproof distributed identity management for P2P networks,‖ in Proc. of IEEE ISCC, pp. 246-253, 2008

[53] R. Rodrigues, B. Liskov, L. Shrira, —The design of a robust peer-to-peer system,‖ in *Proc. of the10th ACM SIGOPS European Workshop*, pp. 1-10, 2002

[54] J. Newsome, E. Shi, D. Song, A. Perrig, —The Sybil attack in sensor networks: analysis & defenses,‖ in *Proc. of ACM IPSN*, pp. 259-268, 2004

[55] B. B. Kang, E. Chan-Tin, C. P. Lee, J. Tyra, H. J. Kang, C. Nunnery, Z. Wadler, G. Sinclair, N. Hopper, D. Dagon, Y. Kim, —Towards complete node enumeration in a peer-to-peer botnet, ‖ in Proc. of ACM ASIACCS, pp. 23-34, 2009

[56] N. Borisov, – Computational puzzles as sybil defenses,**‖** in Proc. of the 6th IEEE Conference on Peer-to-Peer Computing, pp. 171-176, 2006

[57] F. Li, P. Mittal, M. Caesar, N. Borisov, SybilControl: practical Sybil defense with computational puzzles,**‖** in Proc. of the 7th ACM workshop on Scalable trusted computing, pp. 67-78, 2012

[58] Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, Feng Xiao, "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks" IEEE/ACM Transactions on networking, vol. 18, no. 3, June 2010

[59] C. Lesniewski-Laas, — A Sybil-proof one-hop DHT,‖ in Proc. of the 1st Workshop on Social Network Systems, pp. 19-24, 2008

[60] Julia George, Intent Search and Centralized Sybil Defense Mechanism for Social Network, 2014

[61] Bruce Hoppe, Introduction to Network Mathematics, http://webmathematics.net/

[62] Peng Gao, Neil Zhenqiang Gong, Sanjeev Kulkarni, Kurt Thomas, Prateek Mittal, SybilFrame: A Defense-in-Depth Framework for Structure-Based Sybil Detection

[63] Nguyen Tran, Combating Sybil attacks in cooperative systems, 2012

[64] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks", IEEE/ACM transactions on networking, vol. 16, no. 3, June 2008

[65] Lu Shi, Shucheng Yu, Wenjing Louy, Y. Thomas Hou "SybilShield: An Agent-Aided Social Network-Based Sybil Defense among Multiple Communities", IEEE Infocom 2013

[66] Kuan Zhang, Xiaohui Liang, Sybil Attacks and Their Defenses in the Internet of Things, IEEE Internet of Things Journal, Vol. 1, No. 5, 2014

[67] Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove, Ansley Post, Exploring the design space of social network-based Sybil defenses, 2012

[68] B. Levine, C. Shields, N.B. Margolin, "A Survey of Solutions to the Sybil Attack", http://forensics.umass.edu/pubs/levine.sybil.tr.2006.pdf

[69] F. Mattern and C. Floerkemeier. From the Internet of Computers to the Internet of Things, volume 6462 of LNCS, pages 242–259. Springer, 2010