Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

A Study on Device Oriented Security Challenges in Internet of Things (IoT)

R.Vijaithaa
Department of Computer Science, Avinashilingam University, Coimbatore-43
Email: vinuravi20@gmail.com
G.Padmavathi
Department of Computer Science, Avinashilingam University, Coimbatore-43
Email: padmavathi.avinashilingam@gmail.com

ABSTRACT

Internet of Things (IoT) basically discusses about the connection of various physical devices through a network and let them take an active part by exchanging information through Internet. This paper presents important applications of IoT and the different challenges of IoT. Out of the various challenges, attacks on the devices used in IoT are of serious concern. Device oriented attacks and the defensive mechanisms are studied in this paper. A comparison is done for the specific malicious attacks on the M2M communicating devices.

Keywords - **Applications, Challenges, Device oriented security challenges, M2M Communicating devices, Security solutions.**

Date of Submission: April 05, 2017 Date of Acceptance: April 24, 2017

1. Introduction

The Internet of Things is a network of objects, devices or any item in general with sensors embedded in it. These devices are capable of communication with each other and exchange data. The Internet of Things allow objects to be sensed and controlled remotely across existing network infrastructures creating various opportunities for direct integration between physical world and computer-based systems. This results in improved efficiency, accuracy and also economic benefits. When IoT is augmented with sensors and actuators, the technology becomes an instance of the general class of Cyber-Physical Systems (CPS), which also encompasses technologies such as smart grids, smart home, intelligent transportation and even smart cities. Every object connected to the network is uniquely identifiable. Experts estimate that IoT would consist of almost 50 billion objects by 2020.

The scope and applications of IoT are enormous. But still, there are many challenges in IoT. Among the challenges discussed, security and privacy are the major challenges in IoT. Moreover, IoT mainly deals with communication between devices and thereforeensuring security of IoT devices is very critical. Hence, the objective of the paper is to explore the threats in IoT devices. Particularly Machine to Machine (M2M) communication devices. Security threats in M2M communications and the defense mechanisms are discussed.

The rest of the paper is organized as below:

Chapter 2 discusses about Applications of IoT.

Chapter 3 deals with the Challenges in IoT.

Chapter 4 discusses about the Devices in IoT.

Chapter 5 discusses about the Machine to Machine (M2M) communication devices.

Chapter 6 discusses about the Security Threats in M2M devices.

Chapter 7 discusses about the Defense mechanisms for malicious attacks.

Finally Chapter 8 concludes the paper.

2. Applications of IoT

The scope and application of Internet of Things is enormous. Some important applications relevant to today's needs are listed below: [1].

- Smart Cities
- Smart Environment
- Smart Water
- Security &Emergency
- Retails
- Logistic
- Industrial Control
- Smart Agriculture
- Smart Animal Farming
- Domestic and Home Automation
- E-Health

Other than the above important applications, there are certain other applications that may also emerge in future. Though IoT is a not new concept, there are many unsolved challenges in IoT. The next section discusses about the challenges inIoT.

3. Challenges in IoT

Though the concept of IoT seems to be interesting and useful it would be impossible to cover the broad scope of issues surrounding the Internet of Things in a single section. Therefore, an overview of five topics frequently discussed in relation to IoT isdiscussed below [2]. These include: security, privacy,

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

interoperability,regulatory, legal, and rights issues and other general issues. Fig 1shows the classification of general challenges in IoT.

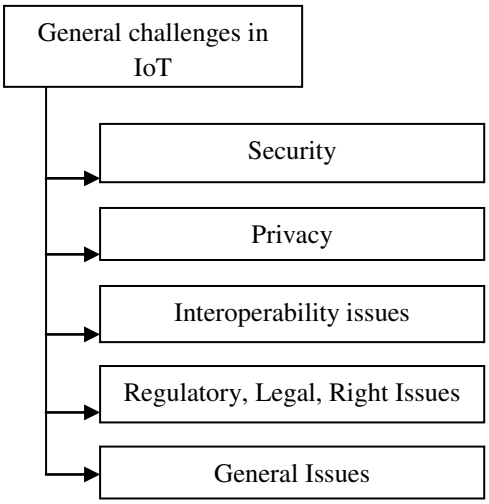

Figure 1: General challenges in IoT

Of the five important challenges, security and privacy challenges are considered for study in this paper as they are the most important ones. Today, devices handle many personal data and they are also connected to the Internet. These days, Internet isexposed to various attacks and the devices connected to Internet become the victim as they operate mostly in unsafe environments.

3.1. Security Challenges due to IoT Devices

IoT devices tend to differ from traditional computers and computing devices in important ways that challenge security.

• Many IoT deployments consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics.

• Many IoT devices will be deployed with an anticipated service life, many years longer than is typically associated with high-tech equipment. Further, these devices might be deployed in circumstances that make it difficult to upgrade them; or these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. The long-term support and management of IoT devices is a significant security challenge.

• Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical.

• Many IoT devices operate in a manner where the user has little or no real visibility into the internal workings of the device or the precise data streams they produce. This creates security vulnerability when a user believes that an IoT device is performing certain important functions, where as in reality it might be performing unwanted functions or collecting more data than the user intends.

• Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Attackers may have direct physical access to IoT devices.

3.2. Privacy Aspects of Internet of Things

Generally, privacy concerns are amplified by the way in which the Internet of Things expands the feasibility and reach of surveillance and tracking.

3.3. Challenges in IoT Interoperability / Standards

Interoperability, standards, protocols, and conventions arethe primary issues in the early development and adoption of IoT devices. While not exhaustive, a number of key considerations and challenges include:

- Proprietary Ecosystems and Consumer Choice
- Technical and Cost Constraints
- Schedule Risk
- Technical Risk
- Devices Behaving Badly

3.4. Regulatory, Legal, and Rights Issues

The applications of IoT devices pose a wide range of challenges and questions from a regulatory and legal perspective, which needs thoughtful considerations. In some cases, IoT devices create many legal and regulatory situations and concerns over civil rights that do not exist prior to these devices. In other cases, these devices amplify legal issues that already exist. Several regulatory and legal issues that affect the IoT applications are discussed below:

- Data Protection and Cross border Data Flows
- IoT Data Discrimination
- IoT Devices as aids to Law Enforcement and Public Safety
- IoT Device Liability
- Proliferation of IoT Devices used in Legal Actions

Apart from regular challenges there are certain general challenges available.

3.5. General Challenges of IoT Connectivity

Some general challenges of IoT connectivity are listed below.

- Signaling
- Presence detection
- Power consumption
- Bandwidth

This section briefly discussed the important challenges in IoT. As mentioned above security is a very challenging task in IoT devices. As mostly, the devices

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

are connected through sensor networks, the types of devices connected and the communication between devices are very important to be explored. The next section deals with that.

4. Devices in IoT

The devices in IoT are broadly classified into two namely, based on objects connected and based on the data exchanged between them. Fig 2 explains the concept.

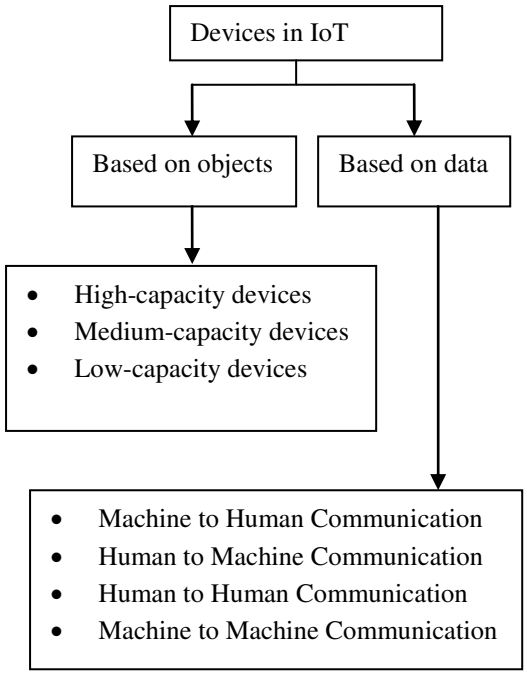

Figure 2: Devices in IoT

Based on objects, the devices are further classified into three types as high-capacitated, medium-capacitated and low-capacitated devices[3]. Based on the data exchanged, four types of communication are identified:between Machine to Human, Human to Machine, Human to Human and Machine to Machine. The next section discusses particularly about Machine to Machine communication devices.

5. Introduction to Machine To Machine Communication Devices

In Machine-to-Machine (M2M) communication of data one or more entities are involved. M2M is also called as Machine Type Communication (MTC). It is different from the current communication models due to:

- Recent or diverse market scenarios
- Lesser cost and effort
- A large number of terminals that communicate potentially
- Less traffic for each terminal.

GSM-GPRS, CDMA EVDO are some of the significant standards for machine to machine communication. Machine to Machine communication confines to the underlying network, the role of mobile network is significant which serves as a transport network.

5.1. Applications of M2M

M2M communication applications are listed below [4]:

- Security
- Tracking and Tracing
- Payment
- Health care
- Remote Maintenance/Control
- Metering
- Manufacturing
- Facility Mana
- gement

5.2. M2M Communication Challenges

There are several key areas that pose challenges to M2M adoption. The challenges of machine to machine communicating devices are given below in Fig 3.

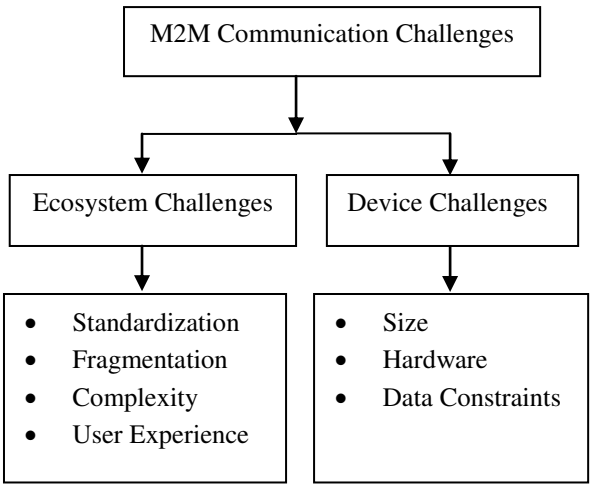

Figure 3: Challenges of M2M Communicating Devices

Apart from the above two fundamental challenges, security is one of the vital challenges in M2M communication. M2M communicating devices face lot of threats and vulnerabilities. The next section deals that.

6. Security Threats in M2M Communicating Devices

There are two fundamental threat classes that are related to system failures and malicious attacks. Fig 4 refers to the classification of security threats in M2M devices [4].

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

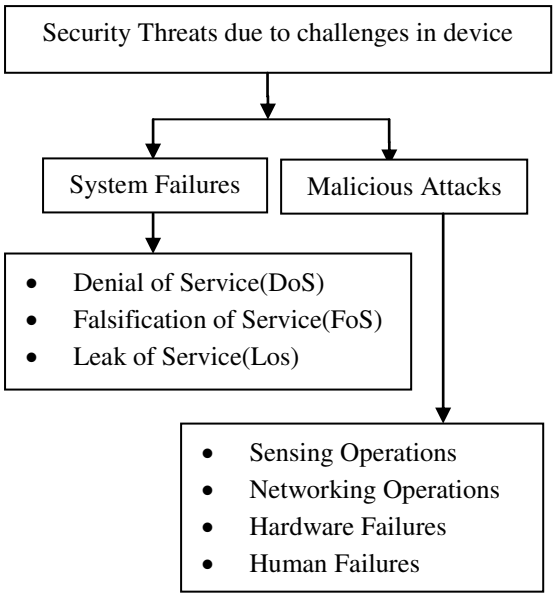

Figure 4: Classification of Security Threats in M2M Communicating Devices

System failures are due to failure in sensing operations, networking operations, hardware failures and human failures.

However, the malicious attacks are due to Denial of Service, Falsification of Service and Leak of Service[5].

6.1. Denial of Service (DoS)

DoS essentially imply that any data and control services are rendered useless by the attack. It prevents the gateway and actuators to receive meaningful data or control signals. It mainly jeopardizes the availability of resources and vast number of threats triggers DoS attacks. Some important DoS attack types are:

- Destruction
- Jamming
- Exhaustion
- Hello flood
- Spoofed Routing
- Sinkhole Attack
- Selective Forwarding
- Wormhole Attack

6.1.1. Destruction: Nodes are vulnerable to physical harm, such as destruction, which allows the attacker to put the device out of service altogether.

6.1.2. Jamming: A node or set of nodes are typically jammed by transmitting a radio signal where the radio frequencies are interfered by a sensor network. In this process,a node can be isolated or the communication between nodes can be disturbed.

6.1.3. Exhaustion: In a wireless low power network, the life span of the end-devices is limited by the power of the battery. Further, the nodes cannot operate when the power is exhausted.

6.1.4. Hello flood: HELLO messages with high transmission power can be received from the malicious nodes. By being a neighbor to many nodes, it creates a type of illusion in the network and also it confuses the routing of the network very badly.

6.1.5. Spoofed Routing: In general, corruption of the routing tables due to control information leads to spoof routing.This results in data not reaching the destination or depletion of the network energy.

6.1.6. Sinkhole Attack: The main work of this attack is making a compromised node which looks attractive to the surrounding nodes with regard to the routing algorithm and the entire traffic is attracted from a particular place by the compromised node.

6.1.7. Selective Forwarding: Nodes behave like a black hole and may refuse to forward particular messages. The attacker concludes that the neighboring nodes have failed and they have to check for an alternate route.

6.1.8. Wormhole Attack: The messages from adversaries are received over a low latency link in one part of the network and are replayed in another part of the network. An enemy located near the last gateway might disrupt the routing by this type of attack.

6.2. Falsification of Service

It implies that data and control services are falsified by the attack. It does not stop the gateway and actuators to receive meaningful data, but it may be falsified. It mainly jeopardizes integrity and a vast gamut of threats triggering FoS are given below:

- Camouflage
- Sybil (multiple identities)
- Node Replication (duplication)
- Acknowledgement Spoofing

6.2.1. Camouflage: Node is inserted by the enemies in the sensor network, so that these nodes can pretend as a normal node and attract the packets towards it to take a wrong routing decision.

6.2.2. Sybil (multiple identities): An adversary can be present in more than one place at a time as a node; that is, a single node presents multiple identities in a network that reduces the fault tolerant schemes.

6.2.3. Node Replication (duplication): As in the case of impersonation, a node is added to the existing sensor network by an attacker by copying a node ID of an existing sensor node. If the attacker is able to copy the network of the node, then the node replication attack occurs. So it leads to packet corruption, misrouting and delaying.

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

6.2.4. Acknowledgement Spoofing: Sensor network routing algorithms rely implicitly and explicitly on link layer acknowledgements.

The last attack is Leak of Service type:

6.3. Leak of Service

Leak of Service implies that the data exposure and services to the attacker are controlled. It does not prevent the gateway and actuators to receive data or control signals, but it leads to leakage of information. It mainly jeopardizes confidentiality and a vast gamut of threats triggering leak of service are summarized below:

- Tampering
- Eavesdropping
- Traffic Analysis

6.3.1. Tampering: Tampering is an attack where the nodes are vulnerable to access physically so that the attacker is allowed to gain access to the node and the network.

6.3.2. Eavesdropping: The communication content is discovered by the attackers by listening to the data. Network traffic suspect both monitoring and eavesdropping.

6.3.3. Traffic Analysis: Monitoring and eavesdropping are combined with traffic analysis. Some sensors with special roles and activities can be identified and attacked by the traffic analysis.

This section briefly discussed about the security threats in M2M communication devices and the type of attacks. The next section briefs the significant defense mechanisms for these malicious attacks.

7. Defense Mechanisms for Malicious Attacks

Most of the threats discussed above are malicious in nature. This chapter discusses about the various defense mechanisms for malicious attacks [6].

7.1. Defense Mechanisms for Denial of Service

The different defense mechanisms for Denial of Service are given below:

- Tamper Proof Hardware
- Ultra-Narrow Band (UNB), Ultra-Wide Band (UWB), Surfing Channel Techniques
- Node Authentication, Message Verification and Message Encryption
- Identity Verification Protocol
- Authentication prior to Data Encryption
- Geographic Routing Protocol
- Multi-hop Acknowledgement Security Scheme
- Trust Scheme for identifying and isolating malicious nodes

7.1.1. Tamper Proof Hardware

The physical access opens up a number of attacks including destroying or stealing the nodes, removing them from their original locations, inserting malicious code and retrieving secret information. Tamper proof hardware is sometimes seen as a viable option to protect the sensors, but this is expensive and may not be very effective against an attacker.

7.1.2. Ultra-Narrow Band (UNB), Ultra-Wide Band (UWB), Surfing Channel Techniques

An adversary transmitting at high power and same frequency used by the nodes disturbs a point-to-point link. Several countermeasures are available. First, an UNB emergency channel is maintained that costs extra bandwidth and extra hardware requirements. Narrowband channels are likely to have more susceptibility which allows the nodes to communicate through the interference potentially. Second, for communications use an ultra-wideband (UWB) radio that is generally resistant to interference of less bandwidth. Third, frequency hopping or surfing techniques are some of the embedded systems on the market which may help as long as all hopping bands are jammed. Lastly, a link layer channel code can be used which is very strong and a combination of suitable link layer retransmission schemes may be enough to help communication.

7.1.3. Node Authentication, Message Verification and Message Encryption

Exhaustion typically happens due to collisions. A defense mechanism would be aimed to design a suitable link-layer, which avoids fatigue mechanisms. Additive measures are node authorization, node authentication, message verification and message encryption.

7.1.4. Identity Verification Protocol

A defense mechanism for hello flood attack is Identity Verification Protocol where every node authenticates each of its neighbors using trusted base stations [5]. The hello flood attack can be prevented if the malicious node has a powerful transmitter, because the bi-directionality of the link is checked by the protocol.

7.1.5. Authentication prior to Data Encryption

Ensuring whether the communicating nodes are authenticated prior to data encryption applied in the networking operation is the countermeasure for this type.

7.1.6. Geographic Routing Protocol

Sinkhole attacks that are resisted by the geographic routing protocols use a forwarding mechanism to move the packets from the source to the nearest destination node. This is possible only in a dense network as it is necessary that the nodes should know their location and their neighbor’s location.

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

7.1.7. Multi-hop Acknowledgement security Scheme

Multi-hop Acknowledgement security scheme has been proposed by Xiao et al to detect selective forwarding nodes. Hop-by-hop is a way by which ACK packet is sent from receiving node to sending node.

7.1.8. Trust Scheme for identifying and isolating malicious nodes

Trust scheme for identifying and isolating malicious nodes is the defense mechanism for wormhole attack. The accuracy and sincerity of each and every neighboring node is measured by the network nodes.

7.2. Defense Mechanisms for Falsification of Service

The different defense mechanisms for Falsification of Service are:

- Authentication prior to Data Encryption
- Unique Symmetry Key
- Randomized Multicast and Line-Selected Multicast
- Node Authentication, Message Verification and Message Encryption

7.2.1. Authentication prior to Data Encryption

Ensuring whether the communicating nodes are authenticated prior to data encryption applied in the networking operation is the countermeasure for this type.

7.2.2. Unique Symmetry Key

The node identity is stolen and it is used as a shared key to communicate in the network. If each and every node shares a unique symmetry key in the network with the base station, then it can be mitigated.

7.2.3. Randomized Multicast and Line-Selected Multicast

The information of a node location to selected witnesses is distributed by randomized multicast. Topology related information is used to detect node replication attack.

7.2.4. Node Authentication, Message Verificationand Message Encryption

Node Authentication, Message Verification and Message Encryption are similar to DoS attack handling methods.

7.3. Defense Mechanisms for Leak of Service

The different defense mechanisms for Leak of Service are

- Self-destructing mechanism, code attestation, code obfuscation
- Omni-directional antennas
- Insertion of dummy packets

7.3.1. Self-destructing mechanism, code attestation, code obfuscation

It allows for various personification attacks. Once the physical intrusion is detected then self-destructing mechanism can be used as a defense mechanism. Code attestation is the best method to counteract a physical attack on the microcontroller. Moreover, in case of physical attack on the external memory like EEPROM, a mechanism called code obfuscation can be used.

7.3.2. Omni-directional antennas

In wireless M2M networks, omni-directional antennas are used which transmit or receive radio signal in all directions. Propagating signal only in one direction is called unidirectional antennas. So by this way, it is protected against eavesdropping.

7.3.3. Insertion of dummy packets

The activity of links is monitored by an adversary and concludes on the choice of routes and networking topology. Insertion of dummy packets into unused routes is the countermeasure for traffic analysis.

7.4. Classification of severe attacks and their defense mechanisms

In a nut shell, the most severe attacks discussed above and their severity are listed with details and some of the existing defense mechanisms are also listed. Table 1 presents the classification of severe attacks, defense mechanisms and its severity in machine to machine communicating devices [7].

Table 1: Classification of Attacks

Attack Name	Attack Definition	Attack Effects	Defense Mechanisms	Severity
Black hole attack (DOS)	Attracting all the possible traffic to a compromised node.	• Causes various attacks like wormhole, eavesdropping. • Exhausts all the network resources. • Corruption in the packets. • Changes in the routing information.	Identity certificates	High

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

Denial of Service attack (DoS)	Users are prevented from using network services.	• Availability of WSN is reduced.	Priority Messages	High
Wormhole (DOS)	Tunneling and replaying messages from one place to other place through low latency links where two WSN nodes are connected.	• Changes normal message stream. • Falsification of nodes or routing will be forged. • Changes the network topology.	Trust Scheme for identifying and isolating malicious nodes	High
Hello Flood (DOS)	Transmission of a message by malicious node with an abnormally high transmission power	• False routing • Route disruption • Packet loss • Confusion	Identity Verification Protocol	High
Grey hole (DOS)	Selective dropping of packets by attracting packets to a compromised node	• Suppresses messages in an area. • Packet loss and information fabrication.	Authentication	High
Camouflage (FOS)	Malicious nodes masquerade as normal nodes to attract packets	• Corruption in the packets • Data to the network will be false	Authentication prior to Data Encryption	Low
Sybil(FOS)	Impersonation by malicious nodes like fake identities	• Packet loss / corruption. • Modification of routing information.	Unique Symmetry Key	High
Eavesdropping (LOS)	Overhearing the communication channel to gather confidential data	• Reduces data confidentiality. • Extracts vital WSN information. • Threatens privacy protection of WSN.	Omni-directional antennas	Low
Traffic Analysis (LOS)	Monitoring the network traffic and computing parameters that affect the network	• Degrades the performance of network. • Packet collision is increased. • Increased contention. • Traffic distortion	Insertion of dummy packets	Low

Volume: 08 Issue: 05 Pages: 3224-3231 (2017) ISSN: 0975-0290

This section discussed the M2M communicating device threats elaborately. The observations on different types of threats and similar defense mechanisms are summarized.

8. Conclusion and Future Enhancement

IoT is the current area of research. In todays world, IoT is used everywhere and has a great concern for the quality of human life. The devices connected to IoT are important segments of IoT research. IoT devices can be broadly classified into four types among which machine to machine communicating devices is very important and it brings benefit to both telecom operators and vendors. Security is a major concern in such devices. This paper presented the different types of security attacks and their respective countermeasures present in machine to machine communicating devices.Different types of attacks and identification of the severe attacks are also done. The entire observations are summarized in a table.

References

1.OvidiuVermason, Peter Friess *From Research and Innovation to Market Deployment*(River publishers series in communications, pg.39-61, 2014).

2.Karen Rose, Scott Eldridge, Lyman Chapin *The Internet of Things-An Overview(*pg. 20-43, October 2015).

3.Alejandro González García, Manuel Álvarez Álvarez, Jordán Pascual Espada, Oscar Sanjuán Martínez, Juan Manuel Cueva Lovelle, Cristina Pelayo G-Bustelo *Introduction to Devices Orchestration in Internet of Things Using SBPMN, International Journal of Artificial Intelligence and Interactive Multimedia,1(4).*

4.White Paper on *Machine-to-Machine Communication (M2M)*http://tec.gov.in/pdf/Studypaper/White%20*Paper%20on%20 Machine-to-Machine%20(M2M) Communication.pdf*

5.Andrea Bartoli*, Security Protocols Suite forMachine-to-Machine Systems* (UniversitatPolitècnica de Catalunya (UPC) pg. 24-29, Barcelona, April 2013).

6.RobertEržen, *Review of main security threats in Smart Home networks*(Study programme: Information Communication Technology, pg.5-12, 2012)

7.DeepaliVirmani, AnkitaSoni, ShringaricaChandel, ManasHemrajani *Routing Attacks in Wireless Sensor Networks-A Survey* (BhagwanParshuram Institue of Technology, India).

Authors Biography

R.Vijaithaa is pursuing her M.Sc Computer Science at Avinashilingam University for women, Coimbatore. Her areas of interest include Cyber Security and Network Security.

G.Padmavathi is the Professor, Department of Computer Science, Avinashilingam University for women, Coimbatore. She has 29 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has more than 100 publications in her research area. Presently, she is guiding M.Phil researchers and Ph.D Scholars. She has been profiled in various organizations for her academic contributions. She has been the Principal Investigator of four projects funded by UGC and DRDO and Scientific Mentor for one project funded by DST. She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE and ACRS.