ISTANBUL TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF SCIENCE, ENGINEERING AND TECHNOLOGY

THESIS PROPOSAL

Ahmet Arış

504122501

Department of Computer Engineering

Computer Engineering Programme

December 2014

THESIS TITLE:Denial of Service Attacks Detection and Mitigation in Internet-of-Things

MEMBERS OF THESIS STEERING COMMITTEE:

Thesis Advisor : Prof. Dr. Sema F. Oktuğ
Istanbul Technical University

Co-Advisor (if any) : Assoc. Prof. Dr. Sıddıka Berna Örs Yalçın
Istanbul Technical University

Member : Prof. Dr. Bülent Örencik
Istanbul Technical University

Member : Assoc. Prof. Dr. Feza Buzluca
Istanbul Technical University

CONTENTS

Page

IOT IRAN
Internet of Things

1. INTRODUCTION

1.1. Significance of the Thesis

Internet of Things (IoT) is a network of sensors, actuators, mobile phones, embedded and wearable computers in which each node has Internet connection. Nodes in this network have unique IDs. By means of standardized protocols, components of IoT will able to communicate with each other and with the Internet and share their state information [1].

Cisco Internet Business Solutions Group is expecting IoT to have 25 billion devices by 2015, and 50 billion by 2020 [2]. In a few decades time, billions of devices will cover agriculture, environment, healthcare places, learning environments, business services, public security, buildings, streets, infrastructures, industry and automation systems, transportation systems and safety critical environments in the concept of IoT [1]. This huge network will include variety of elements with different CPU, memory and battery characteristics, but most of them will be constrained devices. Although in some specific places, components will form an homogeneous environment(i.e., a sensor network), but the general view will highly be heterogenous [3]. Realizing such a large network will not be easy in terms of interoperability, stardardization, privacy and security issues.

IoT is a self-configuring network in which new devices are inserted to the network automatically. The open nature of IoT will be the major weakness for it, causing it to be highly prone to the attacks [1]. Security holes in information systems and attacks targeting computer networks will turn their attention to IoT, specifically Internet-connected resource constrained devices that are working in aforementioned environments. One of the most notorious attacks are Denial of Service (DoS) attacks with no doubt. DoS attacks target any information system by temporarily or completely disrupting services and causing the system to be bound hand and foot. When DoS attacks are launched from multiple places, it is called as Distributed DoS (DDoS). Wired networks are not the only target for DoS/DDoS attacks. Wireless networks including sensor networks, cellular networks, vehicular networks, Wi-Fi are other candidates for these attacks as well.

IoT, as an emerging next-generation network, will surely receive its share from DoS/DDoS attacks. The scenario in which billions of IoT devices covering all around us without no

immunity to DoS/DDoS attacks has been the driving factor for this thesis. The significance of the thesis comes from the fact that, it is very crucial to research, identify and mitigate such attacks in IoT environments as quickly as possible before the actual physical deployments start to take place. Otherwise, a naive deployment of IoT on previously mentioned environments may have catastrophic outcomes due to various DoS/DDoS attacks targeting both from the actual IoT network and from rest of the world by means of Internet connection. Batteries of IoT devices may deplete earlier than expected. IoT components aiming to provide a smarter environment may turn into smart agents spying on us. Our lives may suffer from unreliable transportation systems, safety critical systems, health services, etc. all because of attacks.

1.2. Purpose and Scope of the Thesis

The purpose of the thesis is researching DoS/DDoS attacks targeting IoT environments and proposing efficient algorithms/mechanisms/prototypes which successfully identify such attacks and minimize the attacks' effects on the actual IoT devices and network. Based on this purpose, the scope of the thesis includes but not limited to:

- Creating a standards-compliant and fully functional IoT environment both in real life and on a simulation environment,
- Researching both insider and outsider DoS/DDoS attacks targeting IoT networks,
- Performing DoS/DDoS attacks to the IoT environment both in simulation and on physical network,
- Analyzing the effects of attacks and performance of the IoT devices and actual network,
- Researching efficient techniques to detect the attacks successfully and developing algorithms,
- Evaluating performance of algorithms against attacks by means of simulations,
- Enhancing the algorithms according to the feedback from the previous step,
- Analyzing the simulation performance and implementing the system both in software and hardware,
- Performing final tests.

The devices in IoT environment will be heterogeneous in terms of sensor nodes, actuators, cameras, smart meters and mobile devices. Candidate communication technologies for components include IEEE 802.15.4, ZigBee, Bluetooth, and IEEE 802.11.

The targeted IoT platform will employ IEEE (Institute of Electrical and Electronics Engineers) and IETF (Internet Engineering Task Force) standards for various network layers. With this aim, the standardized protocol stack for IoT is given in Table. 1.

IETF CoAP
IETF ROLL(RPL)
IETF 6LoWPAN
IEEE 802.15.4e MAC
IEEE 802.15.4-2006 PHY

Table 1: Standardized Protocol Stack for IoT

The standardized protocol stack [4] includes IEEE 802.15.4 [5] for physical and MAC layers. 6LoWPAN (IPv6 for Low Power Wireless Personal Area Networks) [6] standard was suggested by IETF as an adaptation layer between MAC and network layers. IETF IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) [7] constitutes the network layer standard for IoT. For the application layer, IETF standard Constrained Application Protocol (CoAP) [8] is proposed.

Contiki [9] and RIOT [10] are operating systems that specially aim the devices in IoT. They provide IETF and IEEE standards' implementations and support reliable and energy-friendly communication and operation for IoT components. The devices within the target IoT platform will be running Contiki operating system which has proven itself both in academia and in proprietary world.

2. UNIQUE ASPECT

The Internet of Things research is closely related to many fields, including RFID, Wireless Sensor Networks (WSN), Machine-to-Machine(M2M) communications, distributed systems, ambient intelligence research, sensor/actor networks [11].

M2M is analogues to IoT in terms of smart devices communicating with each other autonomously, using technologies like 3GPP, Bluetooth, Zigbee and WiFi [12].

Among the mentioned research fields, WSN might be the closest field to IoT. Although they are close to each other in terms of resource constrained nodes, sensing applications, multihop communication and wireless medium characteristics, there are major differences between them. These differences can be summarized as follows [13, 14]. Nodes in IoT can connect to Internet directly, whereas nodes in WSNs have no Internet connection. In IoT, border routers are assumed to be always on, whereas this is not applicable to the sinks in WSNs. In WSNs, sink is the end-point of the communication. In IoT, border routers are acting like only gateways, not like end points. In IoT, message security is mandated by IPv6. In WSNs, message security is not a must. While WSN nodes cannot be identified globally, IoT nodes have globally identified IPv6 addresses.

DoS/DDoS attacks have been studied in WSN community for over a decade. Mechanisms developed for WSNs to detect/mitigate attacks cannot be directly applied to IoT due to the unique characteristics of it. With this reason, so as to protect the IoT network from the DoS/DDoS attacks, novel analysis, techniques, algorithms have to be developed, which keeps the similarities and differences of IoT and WSNs in mind. Contribution of the thesis will be crucial in terms of expected massive numbered deployments of IoT networks and devices.

3. IMPACT

The possible contributions of the thesis will highly affect not only the scientific knowledge, but also economy and wealth.

From the scientific knowledge point of view, IoT and attacks to IoT are emerging research areas. Any contribution that proposes new attacks or effective countermeasures is extremely important and may help researchers to realize new research dimensions. Incorporation of techniques from machine learning, data mining, statistics, bio-inspired computing, information theory to detect the attacks in IoT environments would be very valuable and may bring new dynamics to these disciplines.

In terms of economy and wealth, DoS/DDoS attacks may cause inefficient use of resources. Big investments may be made to realize widespread IoT deployments. But because of attacks, expected yield from the deployments may not be obtained. IoT idea may not be accepted by crowds successfully. These are indirect affects of DoS/DDoS attacks. On the other hand, attacks may have direct catastrophic effects in health services, transportation systems, critical infrastructures and industial automation systems. So, defending these critical environments against attacks is extemely important.

The possible outcomes of the thesis in terms of academy may be conference proceedings and journal papers. By means of the experience and knowledge gained, new BSc, MSc and PhD theses may be generated. The thesis may be the basis for new research projects as well.

The possible outcomes of the thesis in terms of economy and wealth may be obtainment of patents, formation of startup companies or possible cooperation with companies so as to make the DoS/DDoS identification/mitigation system profitable.

4. LITERATURE SUMMARY

Although IoT is a new and an emerging topic of research, researchers proposed several works in recent years. Proposals can be grouped into three sets: applications, DoS/DDoS attacks to IoT network layers and Intrusion Detection Systems(IDS) respectively.

4.1. Applications of IoT

Many proposals applied IoT to various environments with different aims. Some of these works can be classified as infrastructure monitoring ([15] and [16]), environment and wildlife monitoring ([17]), healthcare system ([18] and [19]), education environments ([20] and [21]) and equipment monitoring and maintenance ([22]).

Ding et al. proposed a real time safety and early warning system which is based on the IoT in order to prevent accidents in an underground cross passage construction in Yangtze Riverbed Metro Tunnel [15]. Their work makes use of a sensor system and RFID based labor tracking system to improve safety and to thwart accidents.

The proposal [16] brings smart grid and IoT together. Layered architecture model with sensor networks collecting data from the objects in smart grid(household equipments, RFID tags, security cameras, etc.) provides information about transmission, substantion, distribution and usage of electricty in their work.

[17] presented a wetland monitoring system based on the IoT. System tries to remotely monitor the wetlands that are shrinking in size and facing with damage. A WSN collects data and through GPRS, data is sent to the center for analysis.

Hu et al. lists the application of IoT in medical and health care in their work [18]. They call the resulting system as medical IoT. Embedding sensors to the medical devices and objects and combining medical information systems, sensors and Internet together, patients, doctors, nurses, etc. will gain great benefits in the applications, such as patient monitoring, patient information management, medical emergency management,

blood information management, medical equipment traceability, telemedicine, mobile medical care, etc.

[19] implements an IoT e-health service prototype. The proposed system tries to manage the medications given to elderly people, make sure that they follow the medical prescriptions regularly. Majorly, RFID tags are used to retrieve patients' and medications's information quickly and by means of the services built upon IoT, patients, nurses, caregivers are notified about exact times of medications.

[20] presents an IoT system that includes objects possessing information about how they work, how they can be used, etc. They tagged the internal parts of a personal computer with QRCODES and NFC so as to help students learn system engineering better.

Barthel et al. researched the effects of IoT in the field of aumented memory systems [21]. Within their project, Tales of Things, they placed QRCODEs and RFID tags to the objects. By means of IoT technology, people can listen the stories and memories that were associated with that objects, display, read and alter information by means of applications on their mobile devices.

[22]'s contribution presents a design based on IoT aiming to remotely monitor the important equipments, collect statitistics and produce health reports, predict possible failures and remotely understand the reason of the faults and fix them if possible.

4.2. DoS/DDoSAttacks to IoT Layers

In terms of proposals targeting IoT from the DoS/DDoS attacks point of view, there has been many contributions. According to the IoT network layers, attacks can be classified as follows [28]:

4.2.1. Physical Layer Attacks:

These attacks include jamming [29], node replication [14], node capture and spamming attacks. Jamming attacks try to cause interference to the communicating parties. In spamming

attacks [24], attackers place malicious tags to the IoT environments and try to redirect users to the specific places or websites. In node replication or cloning attacks, attacker copies a physical node and places several copies of it to different parts of the network. When there are several copies of a physical node, packets targeting the actual node may not reach to the intended destination. Attacker uses these attacks so as to gain control of large parts of the network. When combined with other attacks, cloning attacks' effects may be doubled.

4.2.2. Link Layer Attacks:

Attacks targeting frames [23] and slots [25]. Frame collision attacks' effects can be seen as exhaustion of resources and unfairness among nodes in IoT by forced frame collisions [23]. Attacks to time slots include Guaranteed Time Slot (GTS) attacks. In this kind of attack, attacker tries to disrupt the communication between the normal operating nodes and the PAN coordinator during GTS setup phase. Disruption of communication of willing nodes causes them not to be able to acquire the GTS for their transmissions [25].

4.2.3. 6LoWPAN Layer Attacks:

Fragmentation attacks [26]. In fragmentation attacks, attacker tries to prevent the IoT node(s) to successfully reassemble the fragments by sending duplicate fragments [26]. Attack may also cause depletion of memory resource of the nodes, which is occupied by incomplete fragments waiting to be reassembled.

4.2.4. Network Layer Attacks:

Attacks to routing protocols include sinkhole attacks [13, 31], selective forwarding [13, 14], spoofing/altering/replaying the routing information [33], wormhole attack [14, 37], sybil attack [14, 34], rank attacks to RPL [32, 35], version number attacks [30, 36], local repair attacks [13, 27, 32] and hello flood [14]. These attacks try to alter the operation of the routing protocol, attempt to change the path of the packets so as to provide a beneficial place to the attacking node, selectively forward/drop packets and cause inefficient use of resources.

In Sybil attacks, one physical node acts like many logical nodes, advertises itself as multiple nodes to the neighbors [13, 14]. This attack is usually used with other routing attacks to get the control of large segments of the IoT network without deploying actual nodes.

Sinkhole attacks advertise benefical routing parameters to the neighbor nodes in an IoT network so as to be a preferred parent [14]. It does not disrupt the network operation but when it is combined with selective forwarding attacks, it shows its effects. Such malicious nodes may selectively drop packets. So as to show the network operating, attacker node may forward only the routing control packets (i.e., DIO, DAO, DIS), but drop the rest of the data packets. In RPL, the easiest way to perform this attack is using the RPL rank parameter, which is used by IoT nodes to select the preferred parents.

RPL rank parameter is also used in rank attacks. In such attacks, rank verification feature of RPL for a consistent and loop-free Destination Oriented Directed Acyclic Graph (DODAG) topology is altered so as to cause an inconsistent and inefficient DODAG formation which may have loops or routing problems [32].

Rank is not the only RPL routing parameter that has been the target of the DoS/DDoS attacks. RPL version number has also been used for such attacks as well. DODAG root makes use of version number so as to form a new DODAG topology. The network wide repair mechanism is initiated by the root when inconsistencies (i.e., loops, movement of nodes) are detected and when local repair mechanisms does not provide the solution. RPL version parameter is changed by malicious nodes so as to cause a new DODAG topology to be formed. Many RPL control messages (DIO, DAO, DIS) are sent among nodes when there is no actual need.Version number attacks result in inefficient use of resources and DODAG inconsistencies.

4.2.5. Transport Layer Attacks:

Attacks to IoT transport layer include flooding and desynchronization [23]. In flooding attacks, attacker sends many connection requests so as to tire the receiving side out. Desynchronization attacks cause the retransmission of segments by means of spoofing.

4.2.6. Application Layer DoS/DDoS attacks:

Completely legitimate and large volume of requests are sent in application layer attacks. There are vulnerabilities with protocol parsing, processing URI, proxying and caching, risk of amplification and cross-protocol attacks [27].

4.3. IDSs for IoT

There are some proposals [13, 38-42] which neither analyze the effects of the attacks to IoT environment, nor target a specific network layer. These works develop Intrusion Detection Systems for IoT networks. Intrusion Detection System (IDS) tries to detect attacks or anomalies by means of analyzing the network/system activities. IDSs can be classified into three classes:

- **Signature-Based:** Signatures of attacks are stored in a database. IDS tries to match attack signatures and thus detects the attacks. Only the attacks that have a signature present can be detected.
- **Anomaly-Based:** Ordinary behavior of the system is modeled. Any significant deviation from the model is interpreted as an anomaly and attacks are detected in this way.
- **State-Based:** Operations of the protocols are defined by means of state transitions. Activities which do not obey the state transitions or try to break the ordinary operation are detected as attacks.

Signature-based systems and anomaly-based systems are the most common IDSs. Signature-based IDSs suffer from storage cost. Their advantage is they can detect the known attacks successfully but their drawback comes from the same point. Novel attacks cannot be detected by these systems. They are not adaptive to new attacks or new environments. On the other hand, anomaly-based IDSs do not have such a drawback, that they can easily adapt themselves to changing attacks and new threats. They do not need to store any signature. However, labelling behaviors according to thresholds causes systems to have high false positives and high false negatives. They can label a completely normal behavior/connection as an attack (false positives), and they can just skip an actual attack connection thinking as a normal behavior (false negative).

IDSs in literature make use of several techniques from multiple disciplines including probability & statistics, machine learning, data mining, information theory, bio-inspired computing.

Raza et al. proposed SVELTE [13] which is an IDS for IoT environments. Their work tries to detect RPL routing attacks (sinkhole and selective forwarding) by analyzing the DODAG topology and end-to-end packet losses. SVELTE places resource intensive modules to 6LoWPAN border router and lightweight modules to constrained IoT nodes. Thus balances the computation and resource capabilities. The IDS module placed in border router forms the current DODAG tree on border router by means of the messages coming from lightweight IDS modules placed on each IoT node. DODAG tree is analyzed and inconsistencies are detected which may mean DoS/DDoS attacks. SVELTE was implemented on Contiki Cooja simulator.

Le et al. developed a specification-based IDS [32] to detect RPL topology attacks (i.e., rank attacks and local repair attacks). In local repair attacks, attacker causes the IoT nodes to start local repair proces over and over causing to misuse their resources. Le's proposal places dedicated monitoring nodes to the IoT network. Monitor nodes employ RPL finite state machine implementations, which tries to detect any behavior that does not comply RPL routing rules (i.e., strict rank rules).

5. METHODS OR TECHNIQUES TO BE USED

Firstly, standards compliant IoT network will be created both on a simulation environment (i.e., Contiki Cooja, Opnet) and on a physical environement. In simulations, emulated IoT nodes will be employed with state of the art IoT protocol stack implementations. On the physical IoT deployment, nodes similar to simulation environment will be accomodated. If the same nodes are not obtained successfully, then IoT nodes will be created either from scratch (by obtaining low power, low cost CPU boards, sensor boards, 6LoWPAN compliant radio) or will be obtained as compact IoT nodes (boards including IoT supported CPU, sensors, radio and IoT standardized protocol stack implementation).

In order to develop the DoS/DDoS detection and mitigation system (hardware and software) for IoT, statistical techniques and heuristics are planned to be used. IoT network performance parameters related to IoT protocols, flows and packets are going to be analyzed by the targeted system/module and when significant behavioral deviations – anomalies – are detected, system will start reacting against the detected anomaly.

DoS/DDoS detection & mitigation system will be firstly implemented on the simulation environment. After the successful simulation results, actual system will be designed and implemented by hardware/software codesign techniques. Computation intensive modules will be implemented on hardware. Implemented hardware modules will be sharing the same FPGA chip with a softcore CPU module running the rest of the detection/mitigation system.

6. EQUIPMENT AND SOFTWARE TO BE USED

The ContikiOS and the network simulator, Cooja are both open source and free of charge. With this reason, there is no cost of the simulation environment for this study. If, Opnet simulator is needed to be obtained, then it has to be bought for the thesis with required license and necessary Opnet software modules.

The physical IoT deployment needs IoT nodes to be obtained. These nodes may be obtained in two different ways:

- IoT nodes that are the same nodes in the simulation environment (i.e., Tmote Sky motes, Wismote, MicaZ motes, EXP430F5438 motes, etc.) may be bought,
- If these nodes can not be obtained due to unexpected reasons, then IoT nodes may be created from scratch. With this aim, a CPU module that supports Contiki OS may be obtained. Then, sensory board that is compatible with the obtained CPU board must be acquired. 6LoWPAN compliant radio that is also compatible with Contiki and obtained CPU has to be bought. Finally, Contiki OS and its inherent IoT protocol implementations can be installed on IoT nodes.

In addition to the IoT nodes, Raspberry Pi boards are planned to be used as IoT network analyzers. These cards are nothing but small computers that support various GNU Linux distributions and support many radio modules for wireless communications. Network analysis tools such as Wireshark can be run on Raspberry cards easily, which makes them ideal for IoT network analysis.

IoT network may not just include Raspberry Pi boards and sensory boards. Smart phones can be used both as a sensory board and an IoT device. In this study, smart phones and small actuator modules, cameras are planned to be included to the targeted IoT network.

Hardware/software codesign process may require tools such as CoWare or Enterprise Architect. Both of these tools are neither open source, nor free. Similar to the Opnet case, licenses and required modules have to be bought.

The last requirement for the system is an FPGA chip, which needs to big enough to accommodate a softcore CPU module and all detection&mitigation hardware implementation. In addition to the FPGA board, 6LoWPAN radio that is compliant with the FPGA board has to be obtained. For FPGA designs, Xilinx Vivado Design Suite has to be bought, which lets softcore CPU modules, ready-to-use IP modules and custom hardware modules to be implemented, placed&routed, simulated&analyzed.

The template equipment list and expected prices is given the Table 2 below. This list does not include all of the equipments, as it does not include the final prices. This table is intended to give idea about the budget of the study.

Name / Model	Intended Use	Cost (TL)
ASUS G30AB-TR006S desktop PC	Software development, Opnet server and simulations	5117
Samsung U28D590D monitor	For desktop PC	1629
Microsoft CSD-00016 mouse and keyboard	For desktop PC	142
Toshiba X70-A-13N laptop computer	Hardware and software development and simulation environment	4499
Logitech 910-002142 mouse	For laptop	61
Apple iPhone smart phone	For test environment	2299

Sony XPeria smart phone	For test environment	2199
Nokia Lumia smart phone	For test environment	1799
Seagate STDA4000200 external HDD	In order to backup the data	809
Virtex-5 OpenSPARC FPGA board	For hardware software codesign	2297,31
5 x Raspberry Pi B+ Ultimate Kit	Network analyzer in test environment	1416 (5x283,20)
3 x Raspberry Pi Camera Modules	Will be used with Raspberry Pi boards in test environments	248,55 (3x82,85)
5 x XBee Explorer USB	For ZigBee modules for Raspberry Pi boards	424,8 (84,96x5)
14 X XBee Pro 868 MHz 1mW to 315mW antenna	For Raspberry Pi, MSP430 and Arduino boards.	2432,08 (14x173,72)
5 x MSP430 Rev 1.5 development kit	Will be used to create sensory nodes	242,15 (5x48,43)
8 x LDR light sensor	Sensors for sensory boards	66,48 (8x8,31)
8 x DHT21 heat and humidity sensor	Sensors for sensory boards	194,24 (8x24,28)
3 x OV7725 camera module and AL422B board	Camera modules for boards	298,98 (3x99,66)
8 x RN41-XV BlueTooth Module-Chip Antenna	BlueTooth modules for MSP430 boards	944 (8x118)
2 x Arduino Yun development kit	For test environment	438,24 (2x219,12)
2 x CC2541 Bluetooth 4.0 Serial Module	For Arduino cards	127,46 (2x63,73)
2 x PmodWiFi - 802.11b WiFi Interface	WiFi interface for FPGA board	351,78 (2x175,89)
2 x PmodRF2 - IEEE 802.15 RF Transceiver	ZigBee interface for FPGA board	214,12 (2x107,06)
2 x PmodBT2 - Bluetooth Interface	BlueTooth interface for FPGA board	377, 23 (2x188,61)
2 Years Opnet License	Network simulator for simulations	27842,84 (2*13921,42)
4 x Toshiba 16GB MicroSD memory card	Memory cards for Arduinos	144 (4x36)
Enterprise Architect	For hardware/software codesign	1439,59 TL
Xilinx Vivado Design Suite	For FPGA development environment	6945,10 TL
		Total 64998,85 TL

Tablo 2 Equipments, Software and Cost

7. TIME PLAN

The time plan for the study is given in the Thesis Time Schedule Table, which is at the end of the thesis proposal.

8. PROJECT INFORMATION

9. REFERENCES

1. S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in Internet of Things," in Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ser. ITHINGSCPSCOM '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 114–122.
2. D. Evans, "The Internet of Things how the next evolution of the internet is changing everything," Apr 2011, White Paper. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT IBSG 0411FINAL.pdf
3. M. Covington and R. Carskadden, "Threat implications of the internet of things," in 2013 5th International Conference on Cyber Conflict (CyCon), June 2013, pp. 1–12.
4. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," IEEE Communications Surveys Tutorials, vol. 15, no. 3, pp. 1389–1406, Third 2013.
5. McInnis, M. editor-in-chief, 802.15.4 - IEEE Standard for Information Technology, Institute of Electrical and Electronic Engineers, New York, 1 October 2003.
6. J. Hui, P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, IETF, RFC 6282, ISSN: 2070-1721, September 2011.
7. T. Winter et al. , RPL: IPv6 Routing Protocol for Lower Power and Lossy Networks, IETF, RFC 6550, ISSN: 2070-2721, March 2012.
8. Z. Shelby, K. Hartke, C. Bormann, The Constrained Application Protocol (CoAP), IETF, RFC 7252, ISSN: 2070-1721, June 2014.
9. Contiki: The Open Source OS for the Internet of Things, (2014), http://www.contiki-os.org/, [Online; accessed 23-December-2014].
10. RIOT: The Friendly Operating System for the Internet of Things, (2014), http://riot-os.org/, [Online; accessed 23-December-2014].

11. D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497 – 1516, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674
12. K.-C. Chen and S.-Y. Lien, “Machine-to-machine communications: Technologies and challenges”, Ad Hoc Networks, vol. 18, no. 0, pp. 3 – 23, 2014.
13. S. Raza, L. Wallgren, T. Voigt, SVELTE: Real-time intrusion detection in the Internet of Things, Ad Hoc Networks, Volume 11, Issue 8, November 2013, Pages 2661-2674, ISSN 1570-8705.
14. L. Wallgren, S. Raza, and T. Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of Things,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 794326, 11 pages, 2013.
15. L. Ding, C. Zhou, Q. Deng, H. Luo, X. Ye, Y. Ni, and P. Guo, “Real-time safety early warning system for cross passage construction in yangtze riverbed metro tunnel based on the internet of things,” Automation in Construction, vol. 36, no. 0, pp. 25 – 37, 2013.
16. L. Zheng, S. Chen, S. Xiang, and Y. Hu, “Research of architecture and application of internet of things for smart grid,” in 2012 International Conference on Computer Science Service System (CSSS), Aug 2012, pp. 938–941.
17. S. Xiaoying and Q. Huanyan, “Design of wetland monitoring system based on the internet of things,” Procedia Environmental Sciences, vol. 10, Part B, no. 0, pp. 1046 – 1051, 2011, 2011 3rd International Conference on Environmental Science and Information Application Technology {ESIAT } 2011.
18. F. Hu, D. Xie, and S. Shen, “On the application of the internet of things in the field of medical and health care,” in 2013 IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things (iThings/CPSCom) and IEEE Cyber, Physical and Social Computing, Aug 2013, pp. 2053–2058.
19. I. Laranjo, J. Macedo, and A. Santos, “Internet of things for medication control: Service implementation and testing,” Procedia Technology, vol. 5, no. 0, pp. 777 – 786, 2012, 4th Conference of {ENTERprise} Information Systems aligning technology, organizations and people (CENTERIS 2012).
20. J. Gmez, J. F. Huete, O. Hoyos, L. Perez, and D. Grigori, “Interaction system based on internet of things as support for education,” Procedia Computer Science, vol. 21, no. 0, pp. 132 – 139, 2013, the 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH).
21. R. Barthel, K. Leder Mackley, A. Hudson-Smith, A. Karpovich, M. de Jode, and C. Speed, “An internet of old things as an augmented memory system,” Personal and Ubiquitous Computing, vol. 17, no. 2, pp. 321–333, 2013.
22. X. xiaoli, Z. Yunbo, and W. Guoxin, “Design of intelligent internet of things for equipment maintenance,” in 2011 International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 2, March 2011, pp. 509–511.
23. L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa, and J. Lloret, “Denial of service mitigation approach for ipv6-enabled smart object networks,” Concurrency and Computation: Practice and Experience, vol. 25, no. 1, pp. 129–142, 2013.
24. F. Razzak, “Spamming the internet of things: A possibility and its probable solution,” Procedia Computer Science, vol. 10, no. 0, pp. 658 – 665, 2012, {ANT } 2012 and MobiWIS 2012.

25. R. Sokullu, O. Dagdeviren, I. Korkmaz, I, "On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack," Second International Conference on Sensor Technologies and Applications, 2008. SENSORCOMM '08., vol., no., pp.673,678, 25-31 Aug.
26. R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, “6lowpan fragmentation attacks and mitigation mechanisms,” in Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec ’13. New York, NY, USA: ACM, 2013, pp. 55–66.
27. P. Kasinathan, C. Pastrone, M. Spirito, and M. Vinkovits, “Denial-of-service detection in 6lowpan based internet of things,” in 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Oct 2013, pp. 600–607.
28. H. Kim, "Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer," International Conference on Convergence and Hybrid Information Technology, 2008. ICHIT '08., vol., no., pp.796,801, 28-30 Aug. 2008.
29. C. Balarengadurai, S. Saraswathi, "Detection of jamming attacks in IEEE 802.15.4 low rate wireless personal area network using fuzzy systems," Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on , vol., no., pp.32,38, 13-14 Dec. 2012.
30. A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schnwlder, “A study of RPL DODAG version attacks,” in Monitoring and Securing Virtualized Networks and Services, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, vol. 8508, pp. 92–104.
31. K. Weekly, K. Pister , "Evaluating sinkhole defense techniques in RPL networks," 20th IEEE International Conference on Network Protocols (ICNP), 2012, vol., no., pp.1,6, Oct. 30 2012-Nov. 2 2012.
32. A. Le, J. Loo, L. Yuan, A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," Wireless Days (WD), 2011 IFIP , vol., no., pp.1,3, 10-12 Oct. 2011.
33. A. Sehgal et al., "Addressing DODAG inconsistency attacks in RPL networks," Global Information Infrastructure and Networking Symposium (GIIS), 2014, vol., no., pp.1,8, 15-19 Sept. 2014.
34. Z. Kuan et al., "Sybil Attacks and Their Defenses in the Internet of Things," *Internet of Things Journal, IEEE* , vol.1, no.5, pp.372,383, Oct. 2014 doi: 10.1109/JIOT.2014.2344013.
35. L. Anhtuan et al., "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," IEEE Sensors Journal, vol.13, no.10, pp.3685,3692, Oct. 2013.
36. A. Dvir, T. Holczer, L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2011, vol., no., pp.709, 714, 17-22 Oct. 2011.
37. F. I. Khan et al., "Wormhole attack prevention mechanism for RPL based LLN network," Fifth International Conference on Ubiquitous and Future Networks (ICUFN), 2013, vol., no., pp.149,154, 2-5 July 2013.
38. R. Chen, C. Liu, C. Chen, “An Artificial Immune-Based Distributed Intrusion Detection Model for the Internet of Things”, Advanced Materials Research, 2012, vol. 366, pp.165-168.
39. F. Rongrong, et al., "An intrusion detection scheme based on anomaly mining in internet of things," 4th IET International Conference on Wireless, Mobile & Multimedia Networks (ICWMMN 2011), vol., no., pp.315,320, 27-30 Nov. 2011.

40. P. Kasinathan et al., “DEMO: An IDS framework for internet of things empowered by 6LoWPAN”, In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (CCS '13). ACM, New York, NY, USA, 1337-1340.
41. J. Chen, C. Chen, "Design of Complex Event-Processing IDS in Internet of Things," Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 2014, vol., no., pp.226,229, 10-11 Jan. 2014.
42. L. Caiming et al., "Research on immunity-based intrusion detection technology for the Internet of Things," Seventh International Conference on Natural Computation (ICNC), 2011, vol.1, no., pp.212,216, 26-28 July 2011.

THESIS TIME SCHEDULE

Work Package Name/ Definition	MONTHS																																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Creation of the test environment (both physical and simulation)																																				
Making the test environment to be fully compliant with standard IoT protocols																																				
Scenario generation for DoS/DDoS attacks and analyzing the effects of the attacks to IoT																																				
Development of anomaly detection algorithms and performance evaluations																																				
Hardware-software codesign of the system and prototype development and performace evaluation																																				
Publication of the thesis outcomes																																				