ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

# Identification and Removal of Jelly Fish Attack in IOT

Neha Rani[1], Manmeen Kaur[2]

Department of Computer Science Engineering, SVIET, Punjab, India[1,2]

**ABSTRACT:** IOT is the internet of things where various small utility based networks interconnects to each other. So that they can share the data amongst each other. Because small IOT based network for its network utility share the data to the remote network. This way the network can have vulnerability to various types of attacks. While there is a attack situation the network performance will be downgraded. Trust based scheme has been used for detection of the sibal and the jellyfish attacker node. This technique will be based on self cooperation between the nodes. where each node mark the trust value of he other node. Only trusted nodes will be marked as intermediate node. In result no malicious node can be the part of the network. The performance can be enhanced using the trust based technique. This performance has been measured under two different parameters like end to end delay and the throughput.

**KEYWORDS:** Sibal, Jellyfish, ESCT, IOT, Trust

## I. INTRODUCTION

Internet of Things (IoT) is a group of inter-connected devices and around people which communicates each other using different devices without intervention. IoT is a system of connected physical objects that are accessible through internet. It is also new opportunities for huge growth, innovation and exchanging the information between entities. These Entities is known as “Objects” or “Things”. The Objects or “Things” use for connection through internet, these connected devices such as digital watches, TV’s, vehicles, machines etc. The Thing or object could be person with a monitor or automate with built in- sensors, actuators i.e objects that have been assigned an IP (Internet Protocol) addresses and have the ability to collect and transfer data over network without human interaction.

As we know Internet of Things Established a network with number of connections through internet, so definitely threats comes to mess up or steal the information. Now a days so many attacks found which affects in Network such as Denial of service attack, Botnet attack , Sybil, Jelly Fish, zombie attack etc, and enormous techniques designed to improve , detect and remove his misuse.

The main aim of this paper to solve a Jelly-Fish attack in IoT. This attack is part of Denial of service and these kind of attacks hard to detect.In this paper, we considered the some defenses techniques which overcome the Jf-Node attacks, JF attacks targets a closed loop as TCP and exploit the whole network. According (Sapna Hans and Jitendra Kumar et al,2015) to analyzed JF effects are:

- JF-Reorder
- JF Delay Variance
- JF-Drop packets

JF produced the delay before data transmitted and exchange incorrect information .Over all JF destroy whole performance of IoT network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

JF Reorder attack is mis-ordering the data packets or change the routing path. Thus all received or delivered data scrambling order or called reorder.

JF Delay Variance attack is the type of attack which delays the order of packets. When it entered successfully, it changes the order of data to be sent to destination, it creates congestion.

The failure of one or more packets in network transmitted to destination, caused by congestion traffic or some affects and loss the data is called JF dropping packets.

In this paper, we implemented Sybil Defenses techniques with improvised way to remove JF attack in IoT.

## II. RELATED WORK

A.Rajan et.al, 2017 IoT is an develop an architecture in Information Technology (IT) that organized some advancements capabilities such as communication, sensing and computing, RFID via sensor network and wearable devices etc. to offer and serves in IoT of our daily life. IoT systems are extremely vulnerable to Sybil attacks, where create fake identifies or steal identifies of legitimate nodes. In this paper, using a Sybil attack to evaluate the performance and behavior implemented defense mechanism based on profiling of nodes. As well as we build an enhanced ad-hoc- distance vector (EAODV) protocol with behavior approach which obtained optimal routes and detect the selects this node based on trust value and evaluate the trust value of each node in the network .In conclusion, we calculate the trust value using detection technique based on profiling nodes of each node in the network and also we proposed using this protocol detect and isolates the Sybil nodes without affecting network throughput and delay variance.

Mian.M Ahemd et al,2017 In this paper analysis the IoT security challenges and solutions proposed 2010 to 2016.It describes the working of four layers of IoT (Perception Layer, Network Layer, Processing Layer and Application Layer) architecture which define challenges of security ,effects counter measures , exploitation of network and his proposed solutions. Also suggested the more improvements in IoT network to make secure and overcome the threats issues.

Surapon Kraijak1 et al.,2016 In this paper fully explained the whole architectures, protocols security and privacy which uses in real world application. It means that describes the outcome of uses of IoT in daily life such as home applications, machines, sensor devices TV's, Wristwatches with connected Smartphone's etc. They used MQTT Message Queue Telemetry Transport): protocol which works on transport layer. CoAP (Constraint Application Protocol): CoAP is a Specialized web transfer protocol for use in network. These are based on lightweight communication for IoT

M. Todd Gardner(2017) et al. One of the powerful denial of service attack spread in IoT worms like Mirai and the vulnerability that is called Botnet Attacks and it affects the connected devices through internet in October 2016.In this paper ,build a model which define the behavior of Botnet attack, what is the way and how it is affected IoT network. Here this model is called a Susceptible-Exposed-Infected-Recovered-Susceptible (SEIRS) epidemic model to describe the IoT botnet or so called the Stole information and changes the behavior. Another notable result defines the IoT-BAI model which is predicting the attacks behaviors.

Vipindev Adat(2017) et. al This paper describes the security challenges in IoT infrastructure increases the Distributed Denial of Service attacks created lots of disruption to exchange the information due to advancement of Technology. Thus, It is difficult to established the safe connection and hard to detect the threats.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Suman Sankar Bhunia (2018) et. al This paper explains the methods to prevent the security threats in IoT infrastructure . Thus design techniques of the Software Defined Network (SDN) addressed the threats and detect the abnormal "Soft Things" attack and Mitigate it. As well as We talking about the Machine learning which interact the hardware devices without human being. This is used to control the various devices and learn the behavior of Machine Learning of IoT.
Sujatha Sivabalan(2017) et al. This paper generalized the services to poor configuration of Web Servers where analysis the malicious attacks and worms such as Zombie Attack entered into system where loss the legitimate nodes for user connection . The problem occurred in real time systems whose attacks harm the authorization such kind of attacks which measured the power of usage of web servers.

## III. PROPOSED ALGORITHM

ESCT is the approach used in two basic steps one is the self detection and other is the neighbor detection. Under self detection each node detect itself and broadcast the information to its neighbors. This self detection is followed by the cooperative detection. In cooperative detection node will send the hello msg. To the neighboring node. So that each node on receiving the hello messages detect itself and its neighbors.

Step1 node x sends the hello messages to its neighbors.
Step2 on receiving the request packet neighbors y checks for the history. If the neighbor history has the number of requesting node x, it will reply to the x. and increase the trust value of x.
Step3 on receiving the route reply the node x checks for the replied node and if the number is found the will increase the trust value of y.
Step4 this cooperative trust based scheme will be followed at each occasion before the actual transmission will be taken place.
Step5 end.

## IV. FLOWCHART

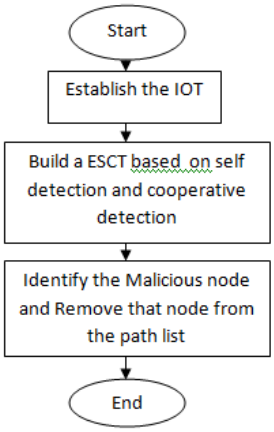


*Fig. 1 Flowchart*

In first step building of the IOT will be taken place. It includes private network of various wireless nodes. Each node is sharing the signals to other node for transferring the data. While communication there may be a chance of malicious

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

node into the network. Which can destroy the communication. Using self detection and cooperative detection malicious node is identified.

## V. PERFORMANCE PARAMETERS

The analysis of routing protocols is done using two important performance metrics named as throughput and end to end delay.

- Average End-to-End Delay: It is the average time taken by a data packet to arrive at the destination. It includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation transfer times.

  $D=\Sigma (Tr-Ts) / \Sigma$ No. of Connections

  Where Tr is received time and Ts is sent time.
- Throughput: It is the average rate of successful message delivery over a communication channel. It is also called as packet sent per unit interval of time. The throughput is usually measured in bits per second or data packets per time slot.

  Throughput=Total packet received / Total time

These parameters are calculated and drawn as graphs so that the performance can be compared. Many other performance parameters are also present to analyze the performance of wireless networks. Packet delivery ratio, normalized load and jitter are some parameters that define the credibility of network.

## VI. RESULTS AND ANALYSIS

6.1 Network Configuration

The simulation scenario and parameters used for performing the detailed analysis is described below. This facet represents that how the effective performance parameters have been analyzed to simulate the protocols. Following steps have been used for simulation.

- Inputs to Simulator:- Scenario File having movement of nodes, traffic pattern file, simulation TCL file
- Outputs File from Simulator:- Trace file, Network Animator
- Output from Trace Analyzer:- xgr file

Table.4.1.Simulation parameters

| SIMULATION PARAMETERS | |
|---|---|
| COVERAGE AREA | 1000m x 1000m |
| PROTOCOLS | AODV,DSR |
| NUMBER OF NODES | 50 |
| SIMULATION TIME | 100 seconds |
| TRANSMISSION RANGE | 250m |

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

| | |
|---|---|
| MOBILITY MODEL | RANDOM WAY POINT MODEL |
| LOAD | 5 Kb-UDP Packets |
| MOBILITY SPEED(variable) | (80,90.100,150)Seconds |
| TRAFFIC TYPE | CBR,UDP,FTP,TCP |
| PACKET SIZE | 512 Kbps |
| PAUSE TIME | 10 ms |

6.2 Results

6.2.1 End to End Delay Comparison under different number of jellyfish attackers

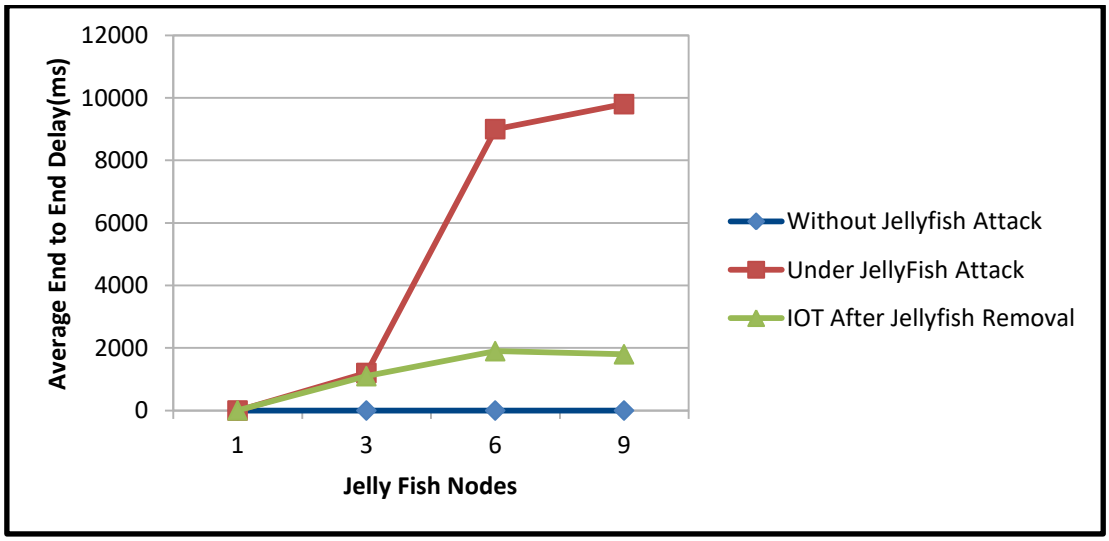


*Fig.2 Average End to End Delay*

In fig. 2 the IOT under different number of attacker nodes having three situations one is without jelly fish attack, under jelly fish attack and after the removal of jelly fish attacker. Once the jellyfish is removed the performance will be upgraded for end to end delay. Green line shows the end to end delay after the jellyfish removal.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

6.2.2 Throughput comparison under different number of jellyfish attackers

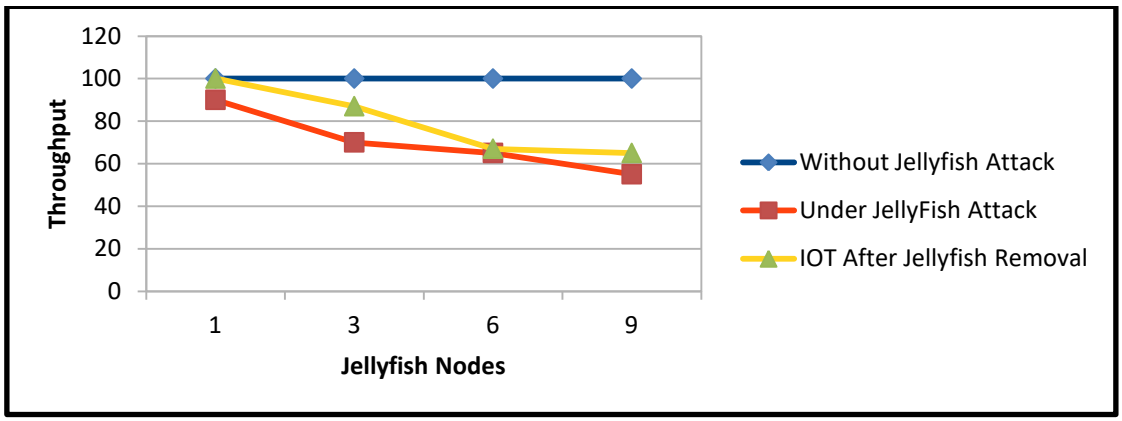


*Fig. 3 Throughput comparison*

Fig. 3 shows the performance comparison of the throughput under different number of jellyfish attacks. The performance will be improved once the jellyfish node has been identified. Yellow line is showing the performance once jelly fish node has been identified.

6.2.3 End to End delay under Different number of sibal attackers

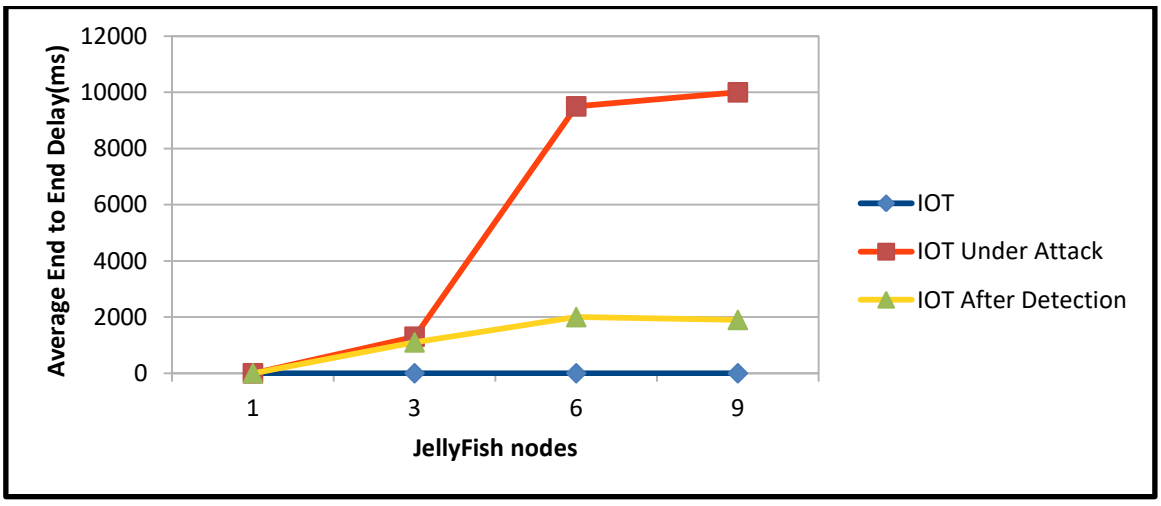


*Fig. 4 End to End Delay for Sibal attack*

Fig. 4 shows the End to End delay under sibal attack in IOT. This performance has been checked against the 1,3,6 and 9 attackers. Once the attacker node will be detected the performance for end to end delay has been enhanced.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

6.2.4 Throughput Under different number of sibal attackers

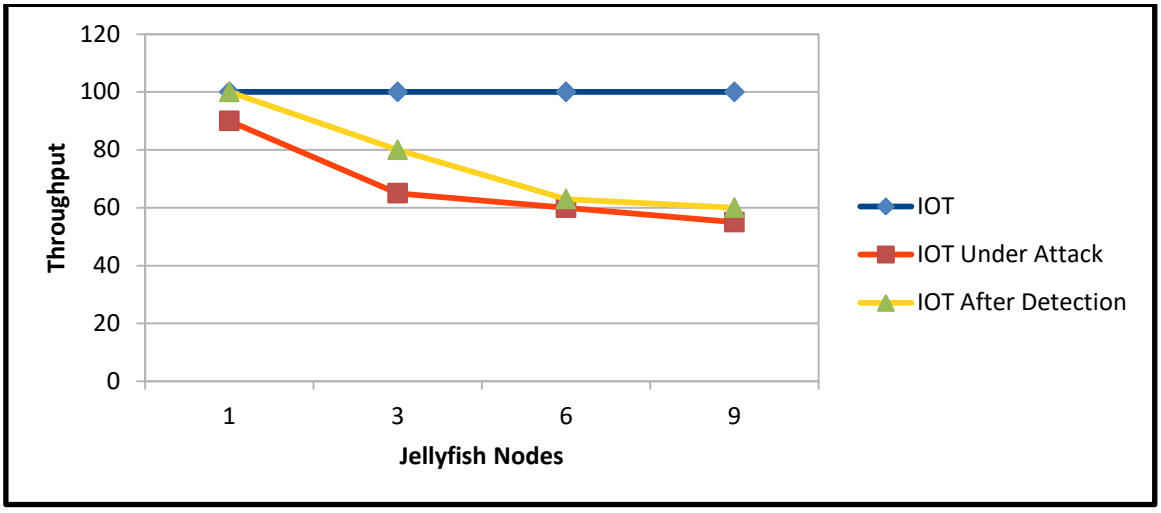


*Fig. 5 Throughput comparison*

Fig.5 shows the performance of throughput under sibal attack. This sibal attacker has been identified the performance of the throughput has been enhanced.

## VII. DISCUSSION

Self trust based scheme is useful in detection of both types of attacks. While forwarding the packets the trust value will be incremented by one by the owner node. If the packet is delayed or not forwarded then the trust value will be decremented. If the trust value is decremented beyond the threshold then the jellyfish is suspected. Else will be considered as normal node. Using this technique network performance has been enhanced in both the context.

## VIII. CONCLUSION

IOT is internet of things. Where small network for their utility connects to the other smaller network or to the internet for remote data sharing. While connecting to the internet it is highly vulnerable to various kinds of attacks. One is sibal attack and other is jellyfish attack. If any of the attack in the network then the performance will be downgraded. To protect the network from such situations trust based technique is used. Where each node mark the trust value of the next neighbor. If the neighbor node forward the packets then the trust value will be marked as incremented else will be decremented. Of the trust value drops beyond the threshold value then the node will be marked as malicious node. Else will be marked as trusted node. The performance of the network under different number of attackers has been tested. In all the cases the performance parameters like end to end delay and throughput has been enhanced. So trust based technique will be useful in all the situations.

## IX. FUTURE WORK

IOT under different types of attacks is being handled using trust based scheme. In all the scenarios the performance is upgraded. In future various other types of attacks can also be tested with the same trust based scheme.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

## REFERENCES

[1] Dave Eastman, Sathish A.P Kumar," A Simulation Study to Detect Attacks on Internet of Things",issue 113,2017.
[2] Vipindev Adat, and B. B. Gupta," A DDoS Attack Mitigation Framework for Internet of Things",issue 978,2017.
[3] Sana BENZ ARTI, Bayrem TRIKI and Ouajdi KORBAA," A Survey on Attacks in Internet of Things Based Networks",issue 978,2017.
[4] Prachi Shukla," ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things",issue 978,2017.
[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review," 2012, in Proc. of Intl. Conf. on Computer Science and Electronics Engineering (ICCSEE), vol. 3, no., pp. 648-651
[6] J. Granjal, E. Monteiro, and J. S´a Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," 2015, IEEE Communications Surveys & Tutorials Volume: 17, Issue: 3, pp. 1294-1312.
[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", Computer Networks, Vol.54, 2010, p. 2787-2805
[8] O. Novo, N. Beijar, M. Ocak, J. Kjallman, M. Komu, and T. Kauppinen," Capillary Networks – Bridging the Cellular and IoT Worlds," 2015, IEEE 2nd World Forum on Internet of Things
[9] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, and D. Valletta, "Security implementation in heterogeneous networks with long delay channel," 2012, IEEE 1st AESS European Conference on Satellite Telecommunications, ESTEL 2012, Rome, Italy, p.1-5
[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements and future direction", 2013, Future Generation Computer Systems, Vol.29, p. 1645-1660
[11] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, Volume 76, 15 January 2015, Pages 146-164
[12] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, Vol. 26, No. 1, Jan. 2010, pp. 23-30
[13] J. Yun, Il-Y. Ahn, N.-M. Sung, and J. Kim, "A Device Software Platform for Consumer Electronics Based on the Internet of Things", 2015, IEEE Transactions on Consumer Electronics, Vol. 61, No. 4
[14] Shulong Wang, Yibin Hou, Fang Gao1 and Xinrong Ji," Access Features Analysis of Things in the Internet of Things", 2016, IEEE, 978-1-5090-2534-3
[15] Archudha Arjunasamy, Thangarajan Ramasamy," A Proficient Heuristic for Selecting Friends in Social Internet of Things", 2016, ISCO, 3294794
[16] Minchul Shin, Inwhee Joe," Energy management algorithm for solar-powered energy harvesting wireless sensor node for Internet of Things", 2016, IET Commun., Vol. 10, Iss. 12, pp. 1508–1521
[17] Kun Wang, Xin Qi, Lei Shu, Der-Jiunn Deng, and Joel J. P. C. Rodrigues," Toward Trustworthy Crowdsourcing in the Social Internet of Things", 2016, IEEE, 1536-1284
[18] Dongsik Jo and Gerard Jounghyun Kim," ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", 2016, IEEE Transactions on Consumer Electronics, Vol. 62, No. 3
[19] David Linthicum," Responsive Data Architecture for the Internet of Things", 2016, IEEE, 0018-91 62
[20] Jun Qi, Po Yang, Martin Hanneghan, Dina Fan, Zhikun Deng, Feng Dong," Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment", 2016, IET Netw., Vol. 5, Iss. 5, pp. 107–113
[21] Haojun Huang, Jianguo Zhou, Wei Li, Juanbao Zhang, Xu Zhang, Guolin Hou," Wearable indoor localisation approach in Internet of Things", 2016, IET Netw., pp. 1–5