IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-5, Jun 2018 E-ISSN: 2347-2693

Identification and Removal of Jelly-Fish Attack in IoT

Manveen Kaur[1*], Jashanpreet Kaur[2]

[1] Department of Computer Science and Engineering,Guru Kashi University, Talwadi Sabo,Bathinda,(PB),India
[2] Department of Computer Science and Engineering, Guru Kashi University, Talwadi Sabo,Bathinda,(PB,) India

Corresponding Author: er.manveenkaur@gmail.com

Available online at: www.ijcseonline.org

Accepted: 15/Jun/2018, Published: 30/Jun/2018

Abstract—IoT is the internet of things where various small utility based networks interconnect to each other. Thus, they can share the data amongst enormous connected devices and small IoT based network for utility share the data to the remote network. This way the network can have the vulnerability to various types of attacks. While there is an attack situation the network performance will be downgraded. The trust-based scheme has been used for detection of the Sybil and the Jellyfish attacker node. This technique will be based on self-cooperation between the nodes. Where each node mark the trust value of the other node. Only trusted nodes will be marked as the intermediate node. In consequently, no malicious node can be the part of the network. The performance can be enhanced using the trust based value technique. This performance has been measured under two different parameters like the end to end delay and the throughput.

Keywords— Ad-hoc ,Sybil, Internet of Things. Jellyfish, ESCT, Trust Value , Security Challenges, Delay variance, end to end encryption,Throughput**.**

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 [1]. 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 [9].

As we know Internet of Things Established a network with number of connections through internet, [3,6] 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, [10] 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) [8] 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.
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 [15].

II. RELATED WORK

A. Rajan [15] 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 behaviour implemented defense mechanism based on profiling of nodes. As well as we build an enhanced ad-hoc- distance vector (EAODV) protocol with behaviour 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.

Sakshi Sachdeva et al., **(2017)** indicates that the presence of Jellyfish attacker node degrades the performance of network in terms of throughput and end to end delay. A scheme is proposed to detect and prevent JF attacker node from ordering the network and effectiveness of scheme is evaluated on ns2 simulator. Jellyfish delay variance attack on AODV is analyzed by JFDV detection algorithm that analyzes.

Mian.M Ahemd et al,2017 In this paper [14] 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.

RuoJun Cai,Xue Jun Li,and Peter Han Joo Chong[16] et al 2017 Here we used ESCT scheme which is conventional scheme used with DSR protocol , Basically ESCT schemes used tow types: self and cooperative detection independently and then detect the results. This is reliable routing protocols for communication networks. The Evolutionary self Cooperative Trust based schemes (ESCT) optimize the trust level information and prevent various disruptions attacks.

Patel Pooja Munish Megha et al,[17] 2017 Above we define the JF Attack briefly and in this paper discussed about his detection and prevention about cluster based techniques (CBIDPT), it considered this fairness , efficiency of selected cluster head. Super cluster based techniques (SCBIDPT); it checks authority to remove the cluster head form the network. Overall it covers the delay variance for some amount of time and data which results comes better form end to end delay in the network. Also improves the performance of network by reducing the congestion and malicious nodes.

Surapon Kraijak1 [13] 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

III. Proposed Algorithm

ESCT is the approach used in two basic steps one is the self detection and other is the neighbor detection [16]. Under self detection each node detects 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 message to the neighboring node. Therefore, each node on receiving the hello messages detects itself and its neighbors [5]. Then Increase the trust value depending below steps:-

Step 1.The node x sends the hello messages to its neighbors.

Step 2.On receiving the request packet neighbors y checks his 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.

Step 3. 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.

Step 4. This is cooperative trust value based scheme will be followed at each occasion before the actual transmission will be taken place.

Step 5. End.

IV. FLOWCHART

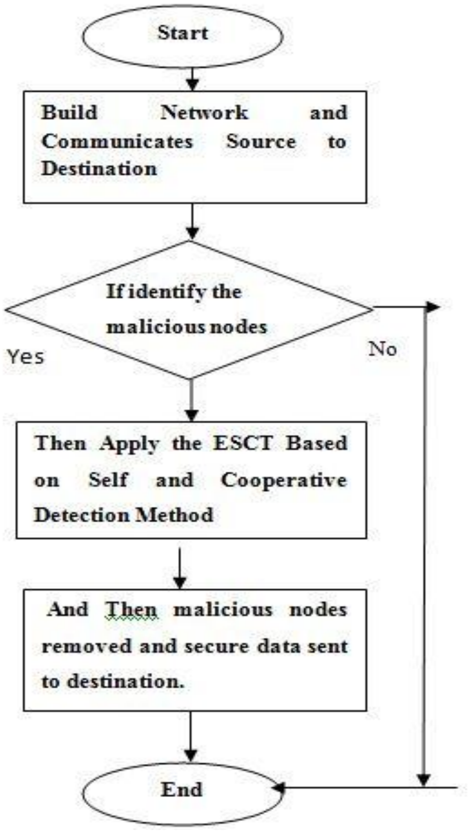
Start
Build Network and Communicates Source to Destination
If identify the malicious nodes
Yes
No
Then Apply the ESCT Based on Self and Cooperative Detection Method
And Then malicious nodes removed and secure data sent to destination.
End

Figure :1 Flowchart

V. PSEUDOCODE

```
P: Broadcast packet
Count=2
T: Timer
For each node
{
Create a packet P
Broadcast the packet to its neighboring nodes
}
For each node
{
If (P received) {
If (T expired) {
Jellyfish attacker suspected
Count= Count -1
If (Count < 0) {
Node is a jellyfish
node
}}}}
For each node
{
While (route discovery)

{
If (RREP from jellyfish attacker)
{
Reject RREP
}}}
```

VI. PERFORMANCE PARAMETERS

The analysis of routing protocols [11]is done using two important performance metrics named as throughput and end to end delay.

1. 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.

2. *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.

VII. RESULTS AND ANALYSIS

7.1 Implementation Strategy

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

a) *Inputs to Simulator*:- Scenario File having movement of nodes, traffic pattern file, simulation TCL file

b) *Outputs File from Simulator:*- Trace file, Network Animator

c) *Output from Trace Analyzer:*- xgr file.

Table.7.1.Simulation Parameter

Parameters	Value
Platform	UBUNTU-14.04
Simulator	NS-2.35
Coverage Area	1000mX1000m
Protocols	AODV, DSR
Number Of Nodes	50
Simulation Time	100 seconds
Transmission Range	250m
Mobility Model	Random Way Point Model
Load	5kb- UDP Packets
Mobility Speed(Variable)	(80,90,100,150) Seconds
Traffic Type	CBR,UDP,TCP, FTP
Packet Size	512kbps
Pause Time	10ms

7.2 Results

In results Figs defines the jitters without JF attack as well as with JF nodes. We implemented some defences techniques in IoT where describes the IoT Jelly Fish Attack Removal.

7.2.1 End To End Delay Comparison Under Different Number Of Jellyfish Attackers

In fig. 7.2.1 the IoT under different number of attacker nodes having three situations one is without jelly fish attack ,

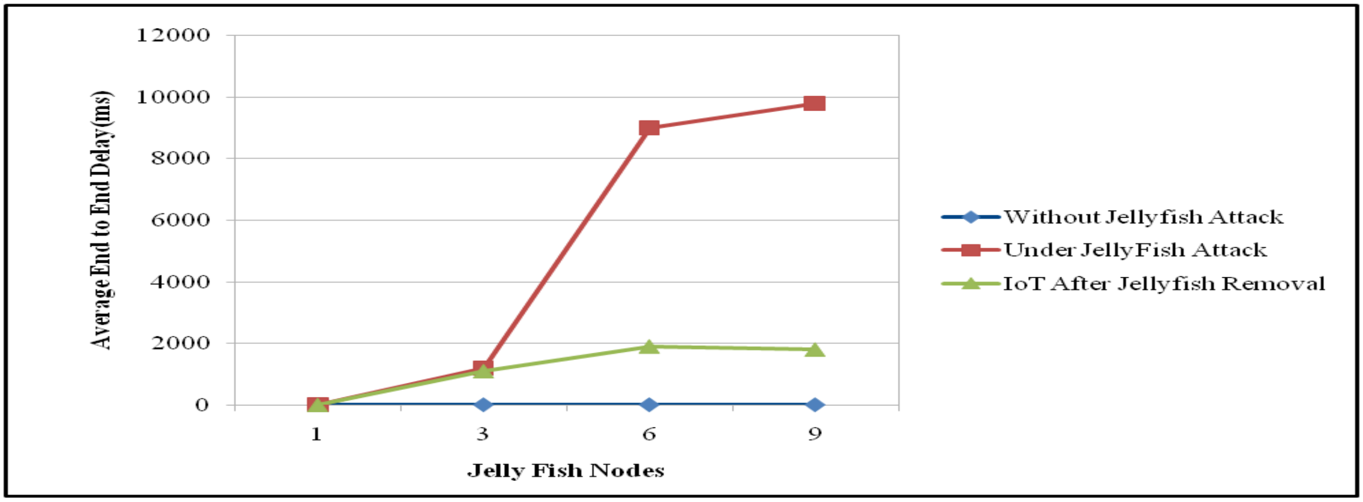

Figure .7.2.1 Average End to End Delay

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. When there is no attack occurred it gives the result per node between the numbers of nodes communication as well as table values considered the difference between remove the malicious nodes

AVERAGE END TO END DELAY IN JELLY-Fish ATTACK (ms)			
Random Positioned Attacks	**Without Jellyfish Attack**	**Under JellyFish Attack**	**IoT After Jellyfish Removal**
1	0	0	3
3	0	1200	1100
6	0	9000	1900
9	0	9800	1800

Table 7.2.1 Average End To End Delay

Also when remove the attack using defense technique then Green line shows the end to end delay after the jellyfish removal, gives efficiency output. The Red lines increased level under jelly fish attach which degrade the performance of communication. Apart from both of order Without Jellyfish attack upgrades the performance analysis.

7.2.2 Throughput Comparison Under Different Number Of Jellyfish Attackers

Fig and Table.7.2.2 shows the performance comparison of the throughput under different number of jellyfish attacks. When network have a no malicious node, it gives results stable. Another condition is when possibilities occurred in attacks such as delay processing, packet drop or re-ordering. As red lines show same, the performance will decline below then other Different Conditions. The performance will be improved once the jellyfish node has been identified

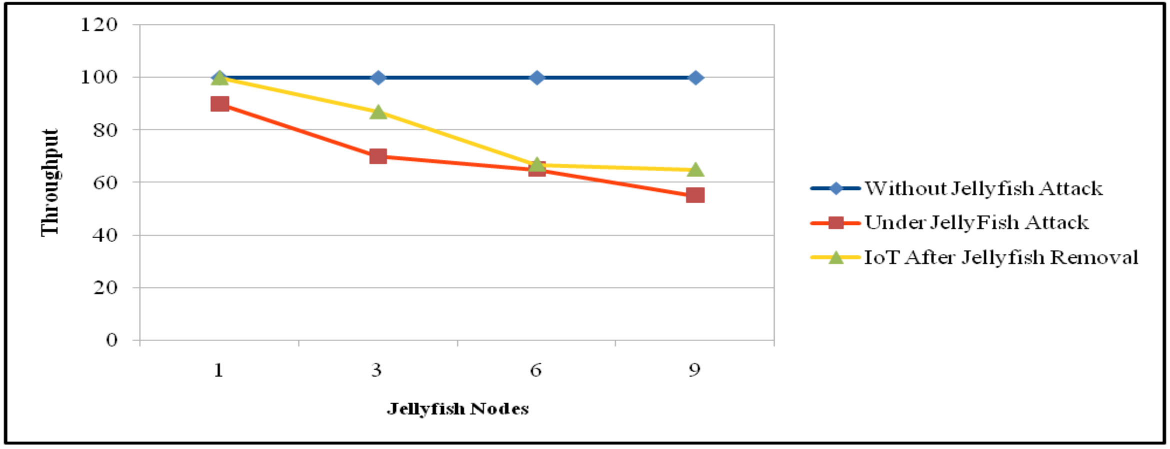

Figure .7.2.2 Throughput Comparison

THROUGHPUT COMPARSION IN JELLY-FISH ATTACK (bytes)			
Random Positioned Attacks	**Without Jellyfish Attack**	**Under JellyFish Attack**	**IoT After Jellyfish Removal**
1	100	90	100
3	100	70	87
6	100	65	67
9	100	55	65

Table: 7.2.2 Throughput Comparison

. Yellow line is showing the performance once jelly fish node has been identified.

7.2.3 End To End Delay Under Different Number Of Sybil Attackers

Fig. 7.2.3 shows the End to End delay under Sybil attack in IoT. This performance has been checked against the

1,3,6 and 9 attackers. It defines the under IoT attacks or After detection of attacks and trust nodes established in the network.

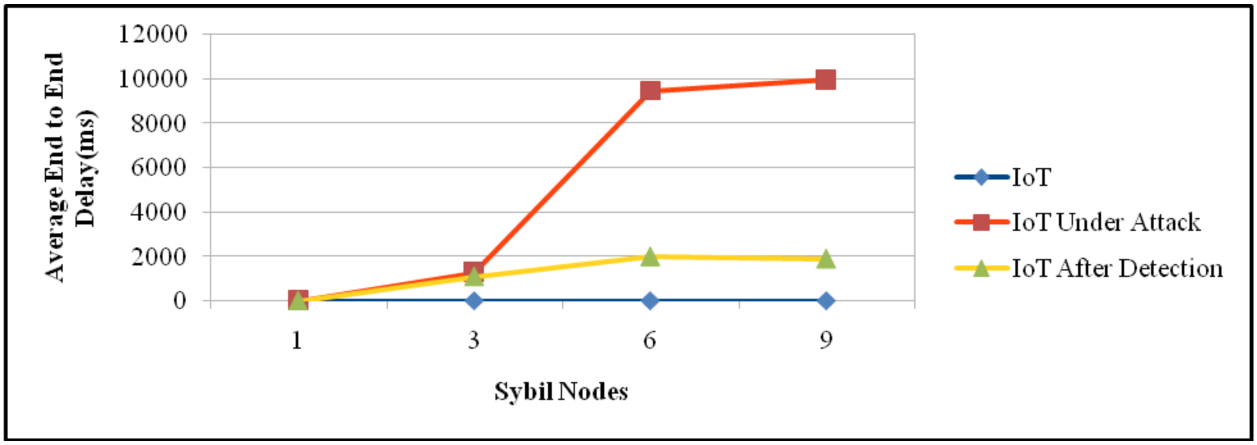

Figure . 7.2.3 End to End Delay for Sybil attack

AVERAGE END TO END DELAY IN SYBIL ATTACK (ms)			
Random Positioned Attacks	**Without Attack**	**Under Attack**	**After Detection**
1	0	0	3
3	0	1300	1100
6	0	9500	2000
9	0	10000	1900

Table 7.2.3 End to End Delay for Sybil attack

Fig and Table 7.2.3 shows the Simple IoT Random networks established the clean communication as shows in Blue line graph IoT End to End without Delay Variance .If Sybil attacks comes into network, it is obliviously result slow and with consume time to transfer information source to destination End to End delay under Sybil attack in IoT. This performance has been checked against the 1,3,6 and 9 attackers. Once the attacker node will be detected, yellow lines shows the performance for end to end delay has been enhanced.

7.2.4 Throughput Under Different Number Of Sybil Attackers

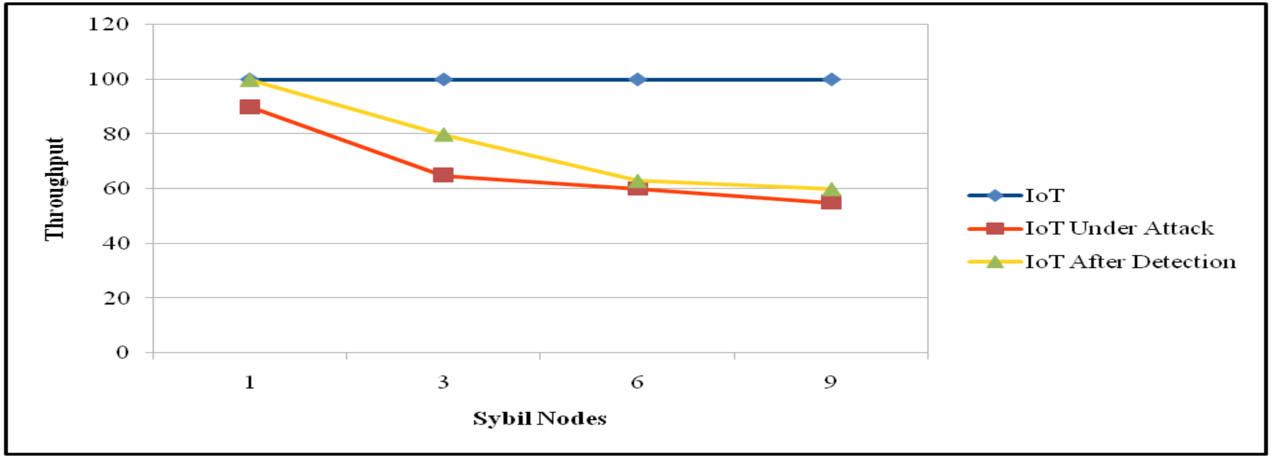

Figure. 7.2.4 Throughput of IoT Sybil Attack

THROUGHPUTOF IoT IN SYBIL ATTACK(bytes)			
Random Positioned Attacks	**Without Attack**	**Under Attack**	**After Detection**
1	100	90	100
3	100	65	80
6	100	60	63
9	100	55	60

Table 7.2.4 Throughput of IoT Sybil Attack

A Fig and Table.7.2.4 shows the performance of throughput under Sybil attack. This Sybil attacker has been identified the performance of the throughput has been enhanced. After detection of Sybil nodes,
data. The throughput graph represents the different malicious nodes as mentioned names 1,3,6,9. They conclude the after detection and removal results are better efficiency.

VIII. 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.

IX. CONCLUSION

IoT is internet of things basically it is value added services which connects different devices with different places and with different purposes. While connecting to the internet it is highly vulnerable to various kinds of attacks. One is Sybil attack and other is jellyfish attack. If any of the attack in the network then the performance will be declined to low. To protect the network from such situations trust value based technique is used. Where each node marks as a the trust value of his 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.

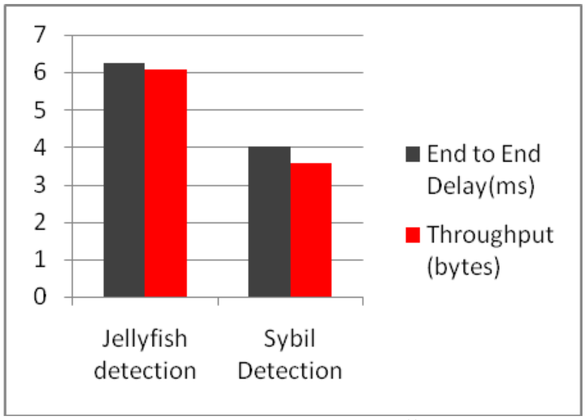

Figure 9.1 Percentage Difference

Figure 9.1 shows the differences between Sybil and Jellyfish Attack after detection performances analysis results. It gives remarkable difference and efficient results after detect and removal the malicious nodes and data transfer end to end communication.

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. Thus, trust value based technique will be useful in all the situations.

X. FUTURE WORK

IoT under different types of attacks is being handled using trust based schemes. 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.

REFERENCES

[1] Hamdan , Husam Tibor , László "Survey of Platforms for Massive IoT", 2018 IEEE, 978-1-5386-1208-8

[2] Vipindev Adat, and B. B. Gupta," A DDoS Attack Mitigation Framework for Internet of Things",issue 978,2017.

[3] Sujatha Sivabalan, Dr P J Radcliffe et al. "Detecting IoT Zombie Attacks on Web Servers",2017 ,27th Int. Telecommunication Networks and Applications Conference (ITNAC) pp 1-3.

[4] 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, pp. 648-651

[5] 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.

[6] M. Todd Gardner, Cory Beard, Deep Medhi "Using SEIRS Epidemic Models for IoT Botnets Attacks" 2017 ISBN 978-3-8007-4383-4 pp 1-8 IEEE DRCN CONFERENCE 2017.

[8] Sapna Hans and Jitendra Kumar," A Review on Jellyfish Attack in MANET", 2015 Int. Journel of Engineering, Applied and Management Sciences Paradigms, Vol 24, Issue 01.

[9] 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

[10] 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

[11] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, Vol. 26, No. 1, Jan. 2010, pp. 23-30

[12] 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

[13] Surapon Kraijak1 "A Survey On IoT Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation And Future Trends" 2016 IEEE 978-1-78561-035-6 pp 1-6

[14] Mian.M Ahemd," IoT Security: A Layered Approach for Attacks & Defenses" ,2017 IEEE - 978-1-5090-5984-3 pp-104-110

[15] A.Rajan" Sybil Attack in IoT : Modeling and Defenses ", 2017 IEEE- 978-1-5090-6367-3/17 pp 2323-2327

[16] Ruo Jun Cai,Xue Jun Li,and Peter Han Joo Chong "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs " 2017, IEEE - 1536-1233 pp.1-1

[17] Patel Pooja Munish Megha ,"Jelly Fish Attack Detection and Prevention in MANET", 2017, IEEE- 978-1-5090-4929-5

[18] Sakshi Sachdeva ,"Detection and analysis of Jellyfish attack in MANETs", 2017, IEEE pp1-5

.

Authors Profile

Er . Manveen Kaur , Completed B.Tech in Computer Science and Engineering ,2016 from Guru Kashi University, Bathinda. I pursuing M.Tech in CSE same University. I interested in Internet of Things, Security, Networking etc. and I published two Papers related to IoT and Biometrics based IoT infrastructure. I am also Member of Journal of Emerging Technologies and Innovative Research.