# Detection and Prevention of Black Hole Attack in RPL Protocol Based on the Threshold Value of Nodes in the Internet of Things Networks

**Vikram Neerugatti, A. Rama Mohan Reddy**

***Abstract*****: *Due to the technology of IOT the human daily life services were became easier. With this technology the scalability will become very more to handle this kind of networks 6LOWPAN protocol was used, In this 6LOWPAn networks the RPL protocol was used to route the packets. The RPL protocol is constrain protocol particularly suits for the constrain node. Due to this constrain behavior this protocol may leads to many attacks. The attacks may be a black hole, wormhole, sinkhole etc. This paper was focused on Black hole attack. The black hole attack was simulated in the Contiki cooja simulator and proposed an detection approach based on the threshold value of each node in the network, to this black hole attack and the results was generated by using the contiki cooja simulator the results shows the effectiveness of the proposed technique in terms of the packet delivery rate, detection rate of attack.***

***Index Terms*****: *IOT, attack, black-hole, detection, prevention, Threshold Value***

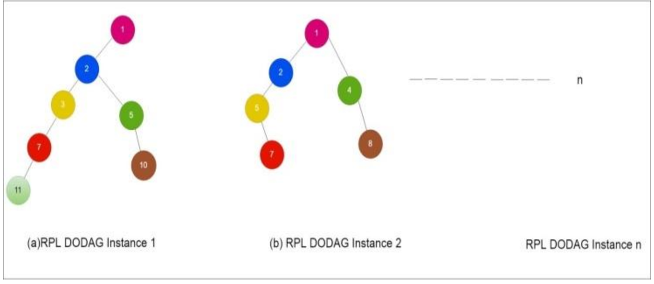
## I. INTRODUCTION

IoT is a network of billions of big and small communicating devices. WSN are subnet of IoT. Devices in WSN are small sensor nodes having memory and power constraints and addressed using IPv6. Sensor nodes communicate with each other as per specifications provides by IEEE 802.15.4. Protocols corresponding to physical and data link layer are specified in IEEE 802.15.4. Specialized task group formed by IETF has defined header compression and framing technique to facilitate communication between sensor nodes using IPv6 over a network of low power and low rate devices is called 6LoWPAN [1].

In future IoT is a billion of sensing, actuating, and smart devices with processing these able to connect internet. Combining of various social networks into the Internet of Things was leads to the Social IoT (SIoT) which enables people connected devices to interact, and also facilitate to share the information [2]. The IoT architecture consists of different layers first one is object layer or perception layer aim of these layer is to collect and process the information. Second layer is object abstraction layer used to collect data that produced by the objects/things in first layer to the server management layer through secure channel. Third layer is server management layer it is also known as middleware layer which will pair a services with its requests based on names and addresses. Fourth layer is application layer provides by the services requested by customers. And final layer layers is business layer it is also called as management layer the overall services and activates done by these layer only [3].

RPL is a routing protocol used to send and receive packets from and to the source and destination nodes. This protocol is particularly designed by the IETF for the 6LoWPAN based networks, which is in the adaptation layer of the IoT protocol layered structure. This RPL is constrained protocol with the loop free topologies with the DODAG structure. DODAG stands for the destination oriented directed acyclic graph as shown in the Figure 1 [4].

6LoWPAN is a hybrid protocol. It is a combination of the both the compression versions of IPv6 and wireless personal area networks. So this is called as a compressed protocol. This is used to establish connectivity among things in the IoT networks. IPv6 is a internet protocol which will provide the unique address to the things in the network and the WPAN is a wireless personal area network, which will establish a connectivity among things with in the area of the in and around the persons. Here the RPL was used for routing. As this are constrained protocols, which will leads to the many attacks. [5]. some of the attacks in RPL protocol, but their main contribution consists in an IDS (Intrusion Detection System) goal is to detect these attacks. Presents an evaluation in the emulation environment Cooja using the contiki OS2 of four attacks targeting the RPL protocol [6].



(a)RPL DODAG Instance 1 (b) RPL DODAG Instance 2 RPL DODAG Instance n

**Figure 1: RPL routing protocol DODAG Instances**

As the RPL works in the manner of DODAG to establish a communication between nodes, it was done based on the Rank of every node in the network. The rank is a physical distance of a node with respect to the root node and the neighbor nodes to itself. While establishing the route among nodes, the nodes in network will select the lesser rank node[7]. RPL is a constrained protocol and it has vast applications in the fields like Agriculture, Healthcare, etc. the applications like smart home, smart school, smart industry, smart city, etc.[8].

RPL was standardized by the IETF as a constrained routing protocol for the low power and lossy networks

**Revised Manuscript Received on July 22, 2019.**

**Mr. Vikram Neerugatti,** Research scholar, Department of CSE, Sri Venkateswara University, Tirupati, Andhra Pradesh

**Dr. A. Rama Mohan Reddy,** Professor, Department of CSE, Sri Venkateswara University, Tirupati, Andhra Pradesh

.

*DOI: 10.35940/ijitee.I3060.0789S319*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

like the 6LoWPAN. This protocol as a security features like the integrity and confidentiality while transmitting the packets from source to destination. [9]. Due to the constrained behavior of the RPL protocol, it may affect with the attacks like Rank attack, Wormhole attack, Black hole attack, Selective forward attack, etc. The nodes will advertise the wrong rank to attract the other nodes for establishing the route, this is called as the rank attack. In the worm hole attack the tunneling will be formed for transmitting of the data. In the black hole more packets will be dropped, whereas in the selective forwarding attack the packets will be forwarded selectively and remaining packets will be dropped [10].

RPL will support the topologies like DODAG; will be in the form of One to One or one to many. As in the DODAG every node will be point towards the root node. Based on the Rank of the nodes in DODAG, the nodes in the network may be act as root node, child nodes and parent nodes. The nodes may be a storing nodes or non-storing nodes, but the root node will be always storing node [11]. Attacks may be a internal or external, the existing security mechanisms of the RPL protocol can mitigate the external attacks but not the internal attack. The mitigation techniques for the internal attack in the RPL are a Research gap [12].

RPL is a Constrained protocol which suits for the constrained devices. The constrained devices means where the computing power, electric power, size will be low compared to the traditional devices. Due to this constrained behavior, it leads to one of the major attack like the black hole attack. It is an attack which drops the packets instead of sending to the other nodes. The solutions to mitigate these attacks are very less and which will not cover the colluding of the black hole attack. So need to develop the approached to mitigate the black hole attack [13].

With the power of the IoT technology, most of the industries are using this technology, the industries like factories, constructions, health care, agriculture, etc. with this can develop the vast applications like the smart wearable, remote controlling of the patients, remote controlling of the agriculture fields, etc. [14].

In the RPL protocol the IETF has defined two objective functions 1. Objective function zero (OFO) 2. Minimum Rank with hysterias objective Function(MRHOF) like the traditional protocols AODV, OSPF the RPL has no security mechanism to avoid the attacks[18].

The nature of the black-hole attack is dropping the packets without forwarding it to other node. This attack is of two types single black-hole attack and colliding black-hole attacking as shown in figure.

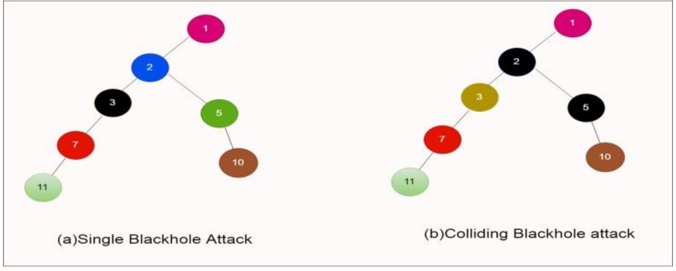


**Figure 2: Black hole attacks (black color ones is an attack nodes)**

In the single black-hole attack only one node will drop the packets where as in the colliding attack two nodes will collaborate and try to drop the packets [13].

## II. RELATED WORK

In [13] author proposed an approach that which detect the black hole attack by consuming low power and with high reliability. The proposed approach is the two step approach. First step is the verification process and the send phase is the detection phase. In the verification process the nodes in the network will verify the routing behaviors of the nodes. Based on that, in the send phase the root node will detects the malicious black hole attack nodes in the network.

In [14] author proposed a technique based on the trustiness of the nodes by considering the past behaviors of the nodes. With this parameter the black hole attack was detected. Here every node past behaviors was checked, if it drops the packets more than 50 percentage, then that particular node was not considered for constructing the DODAG.

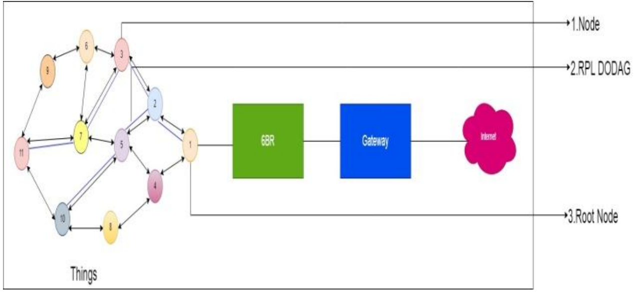


**Figure 3 : RPL Protocol in IoT Network**

In this paper [15] the author has simulated the RPL protocol in 6LOWPAN networks, by using the contiki cooja simulator then they simulated the black-hole attack in that RPL protocol. They noticed that the delay was increased the packet delivery rate was decreased etc. and they finally concluded that the RPL protocol with the black-hole attack will disturb the healthy network in terms of the delay and ratio of the packet delivery rate.

In this paper[16] authors has analyzed the behavior of the routing attacks like black-hole, clone attack, civil, sinkhole attack, and selective forwarding attacks and concluded that due to this attack the network may damage in terms of network throughput the experimental results was shown by using the netsim2.

In this paper [17] proposed an deep learning approach to detect the routing attacks in the internet of things to simulating the proposed system contiki cooja to simulator was used. Here the proposed system will detect the routing attacks like hello flood, version number modification attack and decreased rank attack.

## III. PROPOSED WORK

Here proposed an algorithm for detection of the black-hole attack based on the threshold value of each node in the RPLDODAG. The Threshold value will be calculated based on the packet drop ratio of every individual node. The packet drop ratio was calculated by formula (1)

$PDR=N_{in}-N_{out}$ ----------------------------------(1)

Where,

$N_{in}$ is the number of in packets of each node.

$N_{out}$ is the number of out packets of each node.

Threshold Value=TV=$\frac{PDR}{\text{Nin}}$ x 100

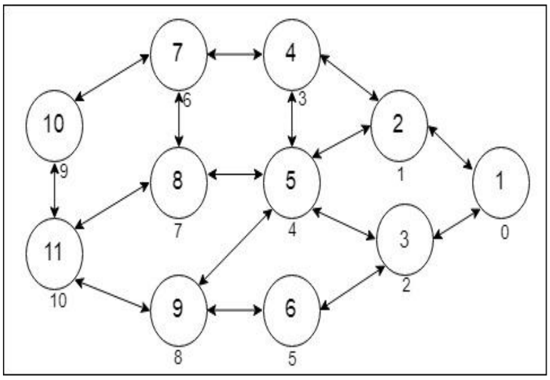
Where, ‘TV’ is threshold value.

The Steps of algorithm was shown in algorithm 1.

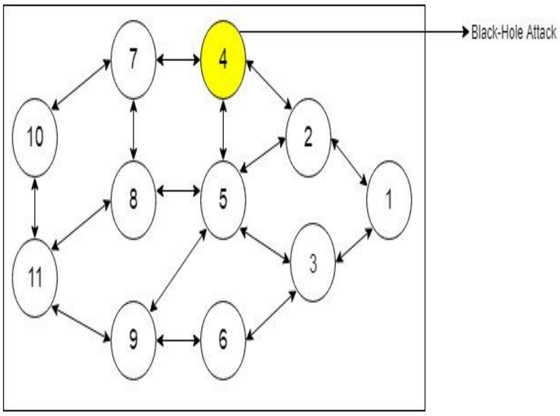
**Algorithm 1:** Proposed Algorithm for detection of Black-hole Attack.

/* Where X is a root node and Y is other nodes, is the black-hole node, TV is the threshold value of individual node, N is the Normal node.*/

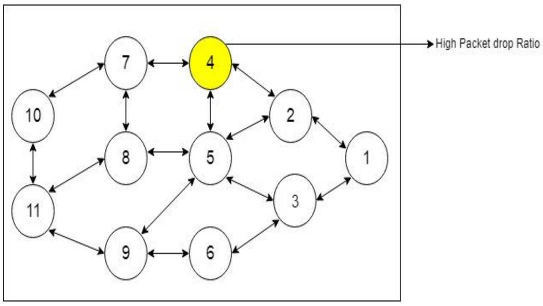
```
0:  Start
1:  root node 'X' broadcast the DIO
2:  Other node 'Y' this is the message DIO
3:  Other node 'Y' send the DAO to the root node 'X'
4:  root node 'X' multicast the DAO-ACK to node 'Y'
        IF
            Can join the DODAG
        ELSE
            Cannot join the DODAG
5:  The DODAG will constructed by repeating the steps 1-4
6:  The node 'X' sends the DIO (to collects the threshold value of each node).
7:  Node 'y' will send the DAO(Threshold value)
8:  Node 'X' sends the DAO-ACK
        IF  Threshold value>60 % (PDR)
            Malicious node detected make as 'Z' Black-hole node).
        ELSE
            Normal nodes(make as 'N')
9:End
```



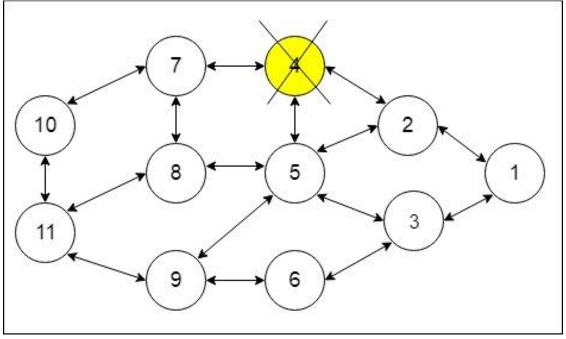
**(a) Things Network**



**(b) Node 4 has a black hole code**



**(c) Detected black hole attack**



**(d) Removed the detected malicious node from the DODAG of the RPL**

**Figure 4: Working Scenario of the Algorithm**

## IV. RESULTS & DISCUSSION

The proposed system was simulated in the cooja simulated with the simulation parameters that mention in table1

**Table 1: Simulation Parameter**

| Parameters | Values |
|---|---|
| Normal Nodes | 30 |
| Malicious Nodes | 3 |
| Node Type | Sky Mote |
| Objective Function | OFO |
| Simulation Time | 20 minutes |
| Event Triggering | Every 1 minute |

The various simulation scenarios are below

Simulation Scenarios:

Scenario1: With 30 Normal Nodes.

Scenario2: 30 Normal Nodes with 3 black hole attack nodes.

Scenario3: 30 Normal Nodes with 3 black hole attack nodes with proposed system.

The three scenario results where shown in the figure 4,5,6,7

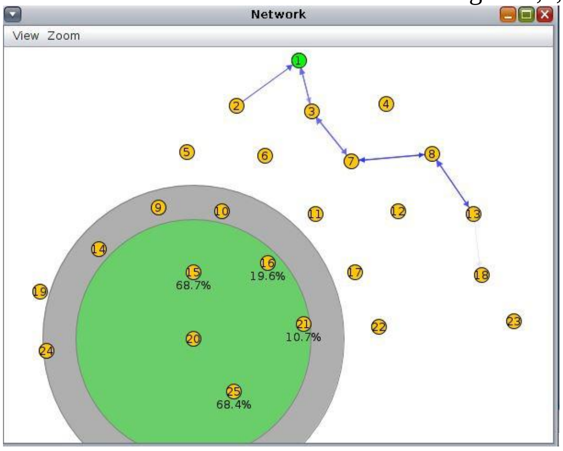


**Figure 5: Nodes on Cooja Simulator**

The packet delivery ratio, the end to end delay, true positive rate and false positive rate was calculated by using the formula 1, 2,3

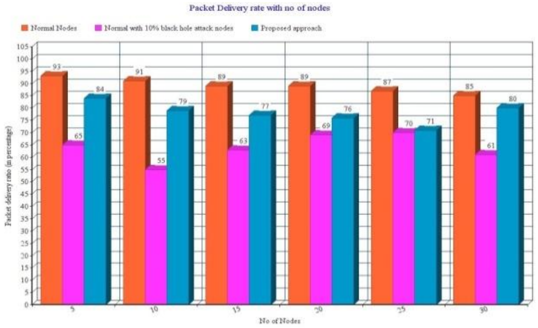


**Figure 6: Packet delivery Rate**

End to End Delay= ETED($N_i$)=$N_iP_i$- $N_iP_o$ --------------------------------------------(2)

Where,

$N_iP_i$ is the packet received time of each node.

$N_iP_o$ is the packet transmitted time of each node.

ETED= ETED($N_1$)+ ETED($N_2$)+--------------------+ ETED($N_n$) ------------------------------(3)

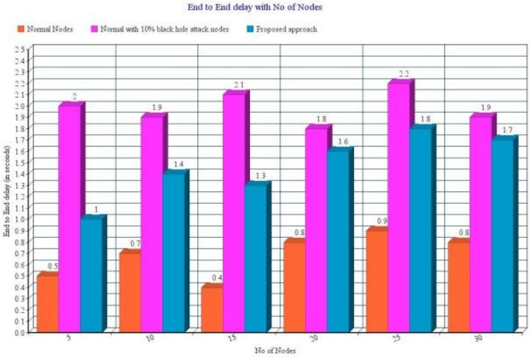


**Figure 7: End to End delay**

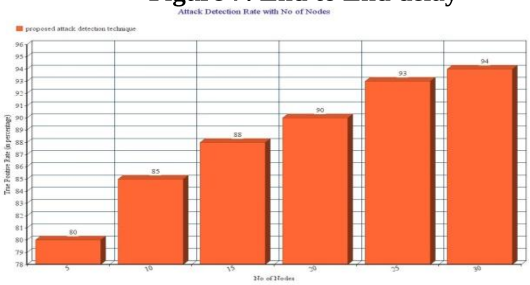


**Figure 8: Attack Detection Rate for the proposed system**

## V. CONCLUSION

An efficient detection and prevention algorithm was proposed for the black-hole attack in the RPL based 6LOWpan networks in the IOT technology. Here the detection of Black-hole was done based on the threshold value of each node in the RPL DODAG. The threshold value was calculated based on the packet drop ratio of every node. The experimental setup was done by using the coontiki cooja simulators in three scenarios. In Scenario 1, with all normal nodes, where as in scenario 2, with attack nodes and in scenario 3, attack nodes with the proposed technique. The results were proved the effectiveness of proposed system in terms of the attack detection rate, End to End delay and packet delivery rate.

## REFERENCES

1. Chugh, Karishma, L. Aboubaker, and Jonathan Loo. "Case study of a black hole attack on LoWPAN-RPL." Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012). 2012.
2. Frustaci, Mario, et al. "Evaluating critical security issues of the IoT world: present and future challenges." IEEE Internet of Things Journal 5.4 (2018): 2483-2495.
3. Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE Communications Surveys & Tutorials 17.4 (2015): 2347-2376.
4. Mayzaud, Anthéa, et al. "A study of RPL DODAG version attacks." IFIP international conference on autonomous infrastructure, management and security. Springer, Berlin, Heidelberg, 2014.
5. Pongle, Pavan, and Gurunath Chavan. "A survey: Attacks on RPL and 6LoWPAN in IoT." Pervasive Computing (ICPC), 2015 International Conference on. IEEE, 2015.
6. Mayzaud, Anthéa, Rémi Badonnel, and Isabelle Chrisment. "A Taxonomy of Attacks in RPL-based Internet of Things." International Journal of Network Security 18.3 (2016): 459-473.
7. Matsunaga, Takumi, Kentaroh Toyoda, and Iwao Sasase. "Low false alarm attackers detection in RPL by considering timing inconstancy between the rank measurements." IEICE Communications Express 4.2 (2015): 44-49.
8. Mayzaud, Anthéa, et al. "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks." International Journal of Network Management 25.5 (2015): 320-339.
9. Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things." International Journal of Distributed Sensor Networks9.8 (2013): 794326.
10. Le, Anhtuan, et al. "The impact of rank attack on network topology of routing protocol for low-power and lossy networks." IEEE Sensors Journal 13.10 (2013): 3685-3692.
11. Perrey, Heiner, et al. "TRAIL: Topology authentication in RPL." arXiv preprint arXiv:1312.0984 (2013).
12. Dvir, Amit, and Levente Buttyan. "VeRA-version number and rank authentication in rpl." Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on. IEEE, 2011.
13. Ahmed, Firoz, and Young-Bae Ko. "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks." Security and Communication Networks 9.18 (2016): 5143-5154.
14. Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism." Telecommunication Networks and Applications Conference (ITNAC), 2016 26th International. IEEE, 2016.
15. Chugh, Karishma, L. Aboubaker, and Jonathan Loo. "Case study of a black hole attack on LoWPAN-RPL." Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012). 2012.
16. Verma, Abhishek, and Virender Ranga. "Analysis of Routing Attacks on RPL based 6LoWPAN Networks." INTERNATIONAL JOURNAL OF GRID AND DISTRIBUTED COMPUTING 11.8 (2018): 43-56.
17. Yavuz, Furkan Yusuf, Devrim Ünal, and Ensar Gül. "Deep learning for detection of routing attacks in the internet of things." International Journal of Computational Intelligence Systems 12.1 (2018): 39-58.
18. Semedo, Felisberto, Naghmeh Moradpoor, and Majid Rafiq. "Vulnerability Assessment of Objective Function of RPL Protocol for Internet of Things." Proceedings of the 11th International Conference on Security of Information and Networks. ACM, 2018.

## AUTHORS PROFILE

**Mr Vikram Neerugatti,** Research Scholar, Department of Computer Science and Engineering, Sri Venkateswara Univrsity, Tirupati. Mr Vikram Neerugatti, is Working on Internet of Things on IoT at Sri Venkateswara University, Tirupati. He Pursuing his PhD in the area of Internet of Things (IoT) and his research Contributes are to provide detection and prevention mechanisms for RPL attacks like Sinkhole, Black hole, Wormhole, Rank attack, etc in IoT. He completed his Bachelors (B.Tech) & Master's (M.Tech) Degree in the Specialization of Computer Science and Engineering at JNTUA. He has M.S Degree from Brain wells University, London, UK. He has more than 10 years teaching experience from various Institutions like NIT, Goa, Sri Vidyanikhethan, A. Rangampeta, Sri Venkateswara University, Tirupati and Sri Venkateswara College of Engineering, Chittoor. He has more than 5 years of Research Experience form NIT Goa and S. V University, Tirupati. He has attended more than 50 Workshops specifically in the area of IoT. He has published 15+ National and International Conferences and Journals. He got 6 best research paper awards. Recently he got Dr. B.R. Ambedkar Research Fellowship award for his innovative research contributions. His research areas are Internet of Things, Fog Computing, Cloud Computing, etc. He acted as a Resource person for more than 20 workshops specifically in the domain of the IoT & Fog Computing in various institutions like Sri Venkateswara University, Sri Padmavathi Mahila Viswavidyalam, Tirupati, Chdalavada venkata subbamma engineering college, tirupati, Sir Vidyanekithan Engineering College, etc.

**Dr. A. Rama Mohan Reddy** He **r**eceived his B.Tech Degree from JNT University Anantapur in 1986, Masters in Computer Science and Engineering from NIT, Warangal in 1991 and Ph.D. in Computer Science and Engineering from Sri Venkateswara University, Tirupati in 2007. He is currently working as a Professor of Computer Science and Engineering, SV University College of Engineering, Tirupati, India. His research interests are Software Engineering, Software Architecture, Cloud Computing, Operating System and Data Mining. He is life member of ISTE, IETE, ISC and CSI. He has more than 30 years of experience in teaching, 7 scholars completed Phd.'s under his guidance. He has 100+ publications and presented 78+ papers in National and International conferences