# A Low Power Malicious Node Detection Processor Using Crossbar Architecture

**K. Yogitha[1], V. Alamelumangai[2]**
[1,2]*Department of Electronics and Instrumentation Engineering,*
[1,2]*Annamalai University, Chidambaram, India*
*E-mail: krishyogitha@gmail.com*

***Abstract:*** *The main issue in wireless sensor network is its security and it must prevent the message leakage during the transmission of the data to other nodes or cluster head in the network. The node called as malicious node act as a faulty or attacker node which generates the false report to the nearby nodes in network environment. In this paper, malicious node detection processor is designed using crossbar architecture. This proposed architecture contains the crossbar architecture and it is used to transfer the packets to the output ports in an efficient manner. Each port controller receives the packet and extracts the two control bits. Based on the control bits the port enable is activated and it can have the permission to transfer the packets from other output ports of the crossbar architecture. The performance of the proposed architecture is simulated using Modelsim and synthesized using Xilinx software tool. The power consumption of the proposed architecture is compared with state of arts methods.*

*Keywords:* **Malicious node, detection processor, crossbar, performance, power consumption**

## Introduction

Sensor networks can be categorized into wired and wireless. Former one requires more components and not supporting the fast communication. The wired sensor networks are not suitable for unattended environments such as earth quake and flooding environment. At these times, the network will be corrupted due to the faults in their transmission lines. The wireless sensor networks (WSN) are preferred in this environment. WSN consists of large number of sensor nodes spread over the entire area of the network and all these sensors are connected to the centre node, called as cluster head and all the cluster heads are connected to the sink in the network. Each sensor node in WSN must have certain individual characteristics and each node has sensor unit, converter unit and transmitter and receiver unit. The sensor unit in sensor node senses the surrounding environment and sends these details to the converter. It converts the measured analog value into digital data and these datas are transmitted through the antennal available in the sensor networks.

The main issue in WSN is its security and it must prevent the message leakage during the transmission of the data to other nodes or cluster head in the network. The node called as malicious node act as a faulty or attacker node which generates the false report to the nearby nodes in network environment. It generates more numbers of control signals and these control signals are sent to the other nodes in the network which make confusion to the other nodes. The performance of the WSN will be degraded due to the presence of the malicious nodes and it also consumes more energy.

The paper is structured as follows. Section 2 discusses various methodologies or techniques for detecting the malicious nodes in wireless sensor networks. Section 3 proposes a hardware architecture for malicious node detection. Section 4 discusses the results and its simulation. Finally, Section 5 concludes the research.

## Literature Survey

Hossein Jadidoleslamy [1] used hierarchical technique for detecting the suspicious nodes in wireless area networks and the authors further utilized intrusion detection technique to analyze the behaviour of the network. The authors use clustering approach for identifying the characteristics of the node behaviour in sensor networks. Feng et al. [2] developed a trust estimation methodology for analyzing the behaviour of the nodes in wireless sensor environment. The authors applied evidency technique on each node in the network to analyze the characteristics of the node. The trust methodology proposed in this work was based on the characteristics of the individual node in WSN environment. Babu et al. [3] predicted the nodes characteristics using recommendation algorithm for trust values estimation on each individual node in WSN environment. The authors extracted the quality of service parameters for individual node analysis to detect the malicious nodes among the set of nodes in wireless network topology.

Chang et al. [4] proposed malicious node detection system using cooperative bait technique which efficiently detects the abnormal nodes in larger network area. The authors solved the limitations in dynamic source routing protocol of the present malicious node detection system. The authors achieved 97% average packet delivery ratio in their proposed methodology for malicious node detection. Patel et al. [5] proposed the methodology for detecting the malicious nodes in smart wireless sensor networks. The authors used passive eavesdropping reduction algorithm to prevent the message leakage in network environment. Haripriya et al. [6] proposed an efficient framework for the detection of malicious nodes in wireless sensor networks. The nodes behaviour was identified over the certain period of time and the charecteristics features were used further to differentiate the behaviours of the normal node from malicious nodes. Fenye Bao et al. [7] used hierarchical trust management algorithm for the identification of malicious nodes and hidden nodes in larger networks.

## Proposed Methodology

In this paper, malicious node detection processor is designed using crossbar architecture. Fig. 1 shows the nodes in wireless sensor network and their interfacing with each other. The nodes are represented as n1, n2, n3, n4, n5 and n6, which are spread as shown in Fig. 1. The centralized node is called as malicious node detection processor node which detects the malicious node in the WSN environment. The centralized node P receives the packet from all of its surrounding nodes n1, n2, n3 and n4. The nodes are connected through the wireless communication path as a bidirectional link between all nodes in WSN environment.

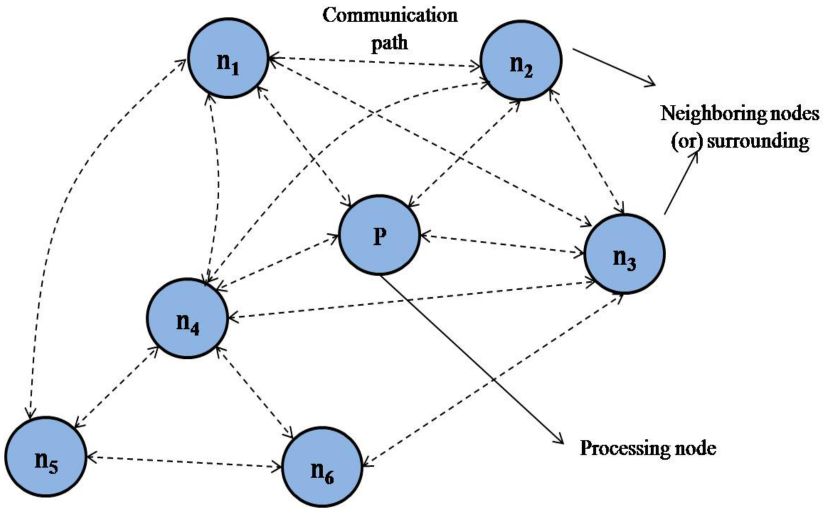


**Fig. 1: Nodes and its interfacing in WSN**

Fig. 2 shows the data verification circuit in malicious node detection processor which detects the malicious node in the WSN environment. Initially, this circuit receives the packet and then extracts the eight bit data from it. This circuit will produce a single bit output as data_out, which may have the value either ‘0’ or ‘1’. The malicious node is identified if the value is ‘1’ and the non-malicious node is identified is the value is ‘0’.

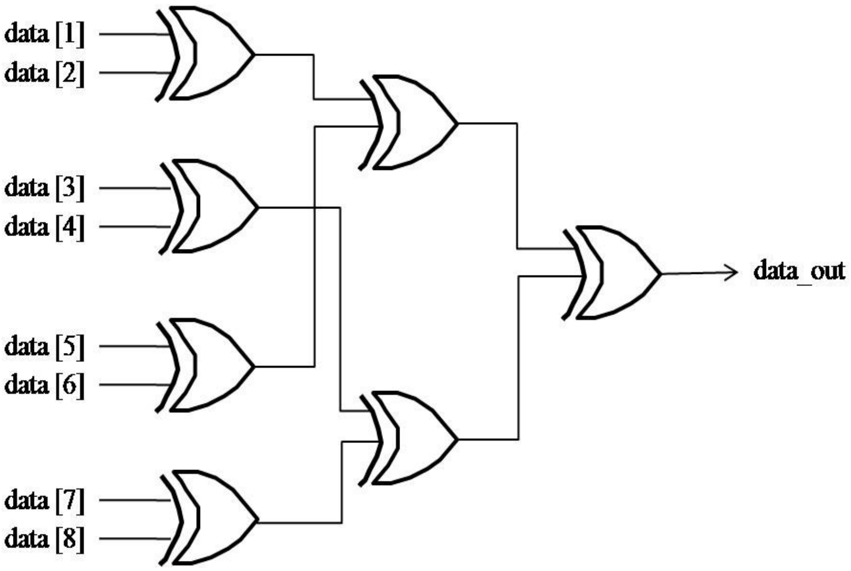


**Fig. 2: Data verification circuit in malicious node detection processor**

Fig. 3 shows the address verification circuit in malicious node detection processor which detects the malicious node in the WSN environment. Initially, this circuit receives the packet and then extracts the five bit address from it. This circuit will produce a single bit output as addr_out, which may have the value either ‘0’ or ‘1’. The malicious node is identified if the value is ‘1’ and the non-malicious node is identified is the value is ‘0’.

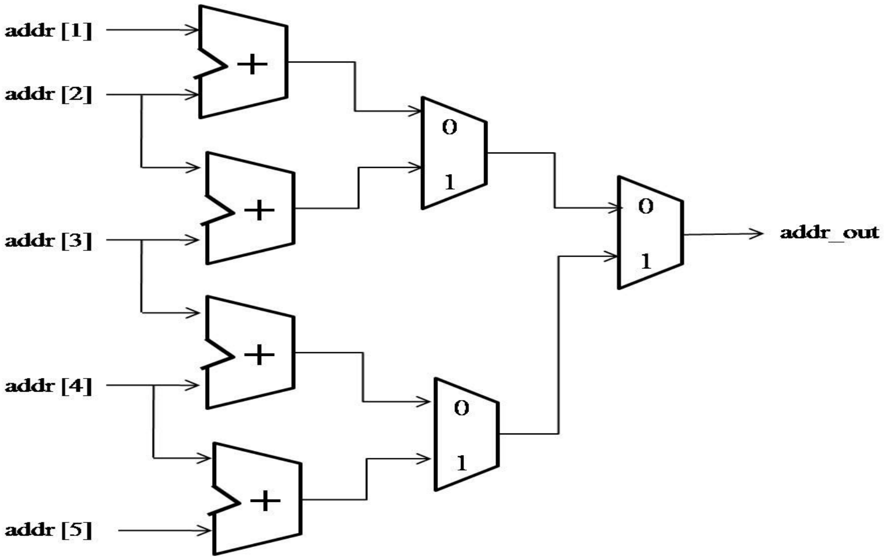


**Fig. 3: Address verification circuit in malicious node detection processor**

The input and output ports of the cross bar architecture is shown in Fig. 4. Here, we have four numbers of input ports as n1, n2, n3 and n4 and four numbers of output ports as n1, n2, n3 and n4 as shown in Fig. 4. The input port n1 can receive the data and it may send the data to any one of the output ports if the node 1 is identified as non-malicious node. If it is identified as malicious node, then the port may be terminated and it does not have any option to transfer the packets from one port node to any one of the output port nodes.

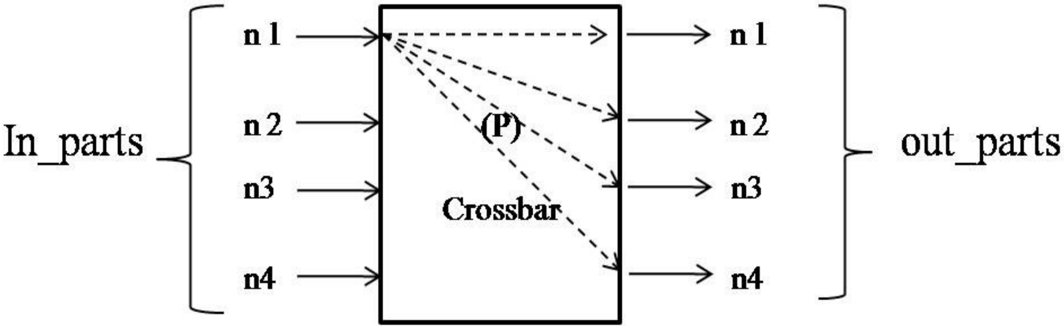


**Fig. 4: In and out ports interfacing through crossbar**

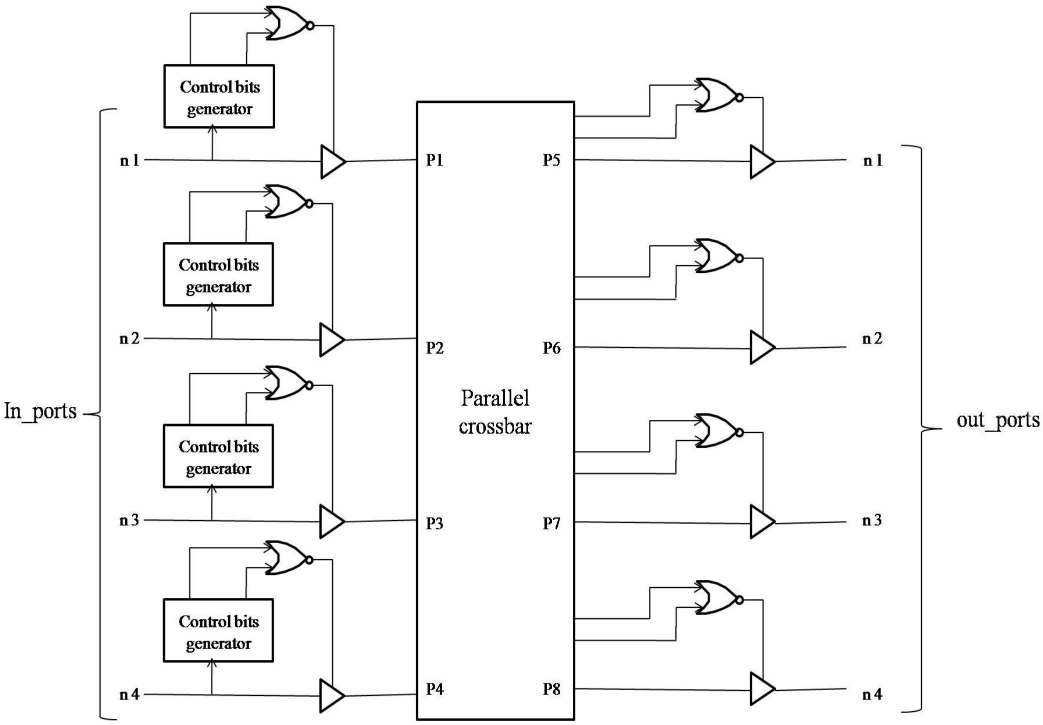
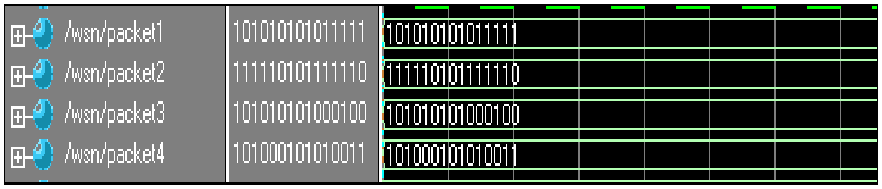


**Fig. 5: Crossbar architecture**

The crossbar architecture of the proposed malicious node detection processor is shown in Fig. 5. It has four numbers of input ports and output ports as shown in Fig. 5. Each port controller receives the packet and extracts the two control bits. Based on the control bits the port enable is activated and it can have the permission to transfer the packets from other output ports of the crossbar architecture.

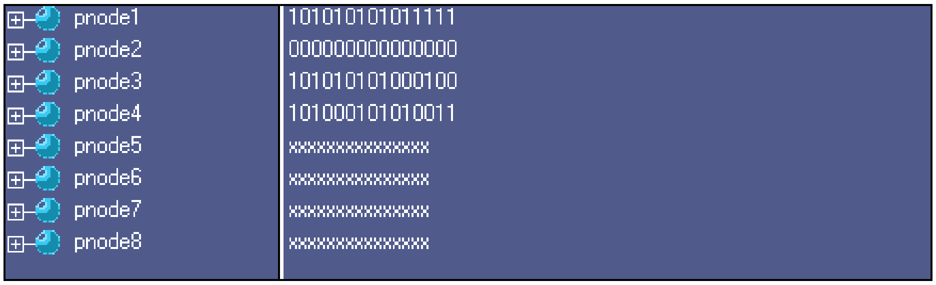
## Results and Discussion

In this paper, the performance of the malicious node detection processor is analyzed in both simulation and synthesis hardware tool. Modelsim 5.5e tool is used for simulating the behaviour of the malicious node detection processor and it shows the input and outputs as a waveform for automatic verification of their logical functionalities. Xilinx Project Navigator 9.2i is used for synthesizing the behaviour of the malicious node detection processor and it shows the cross and front view of the designed processor in wireless sensor networks.



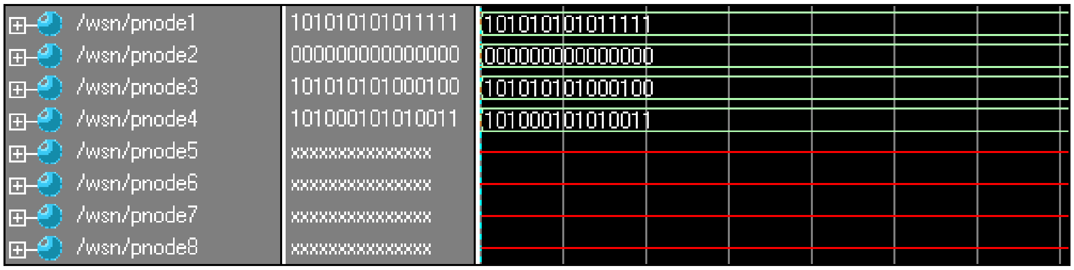
```
/wsn/packet1   101010101011111   101010101011111
/wsn/packet2   111110101111110   111110101111110
/wsn/packet3   101010101000100   101010101000100
/wsn/packet4   101000101010011   101000101010011
```

(a)



```
pnode1   101010101011111
pnode2   000000000000000
pnode3   101010101000100
pnode4   101000101010011
pnode5   xxxxxxxxxxxxxxx
pnode6   xxxxxxxxxxxxxxx
pnode7   xxxxxxxxxxxxxxx
pnode8   xxxxxxxxxxxxxxx
```

(b)

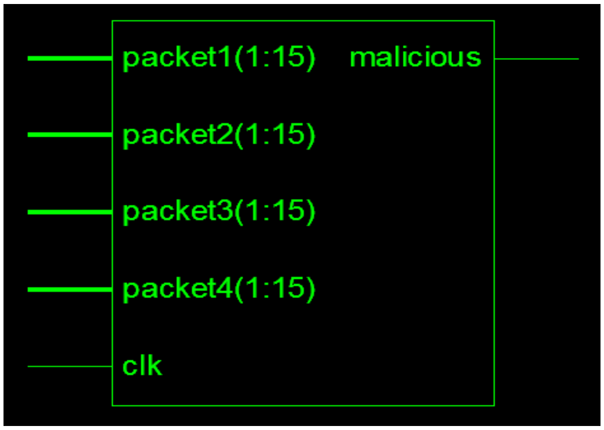


```
/wsn/pnode1   101010101011111   101010101011111
/wsn/pnode2   000000000000000   000000000000000
/wsn/pnode3   101010101000100   101010101000100
/wsn/pnode4   101000101010011   101000101010011
/wsn/pnode5   xxxxxxxxxxxxxxx
/wsn/pnode6   xxxxxxxxxxxxxxx
/wsn/pnode7   xxxxxxxxxxxxxxx
/wsn/pnode8   xxxxxxxxxxxxxxx
```

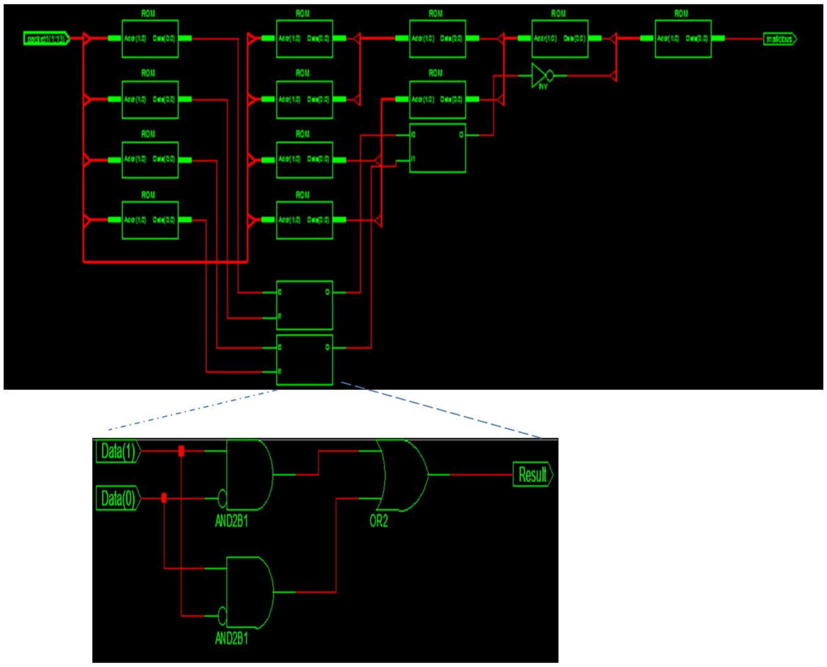
(c)

**Fig. 6: (a) Input packets of the designed processor (b) Signal window of the simulation (c) Waveform window of the simulation window**

Fig. 6(a) shows the packets structure of the input ports which are the input packets received from the surrounding nodes of the designed malicious nodes detection processor. The packet length is 15 bits long. First eight bits represent the packets data and next five bits represent the address bits. Final two bits are the control bits of the packets, which decide the output port, where the packets flow to the output. Fig. 6(b) shows the signal window achieved through the simulation of the designed processor and Fig. 6(c) shows the waveform window achieved through the simulation of the designed processor.



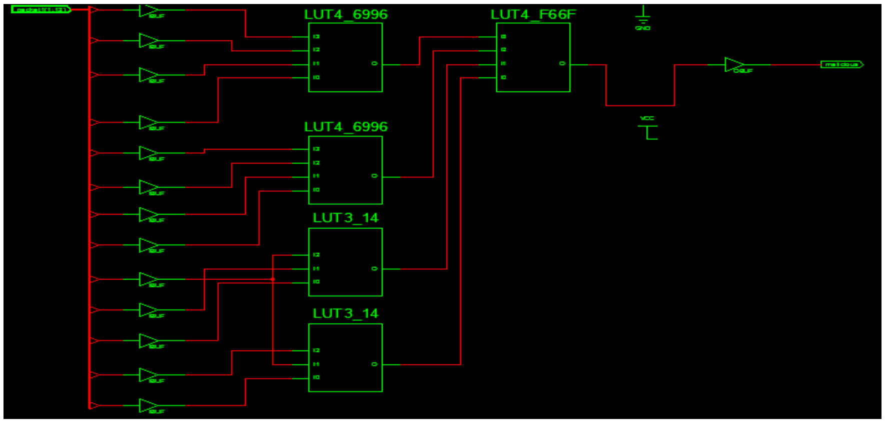
(a)



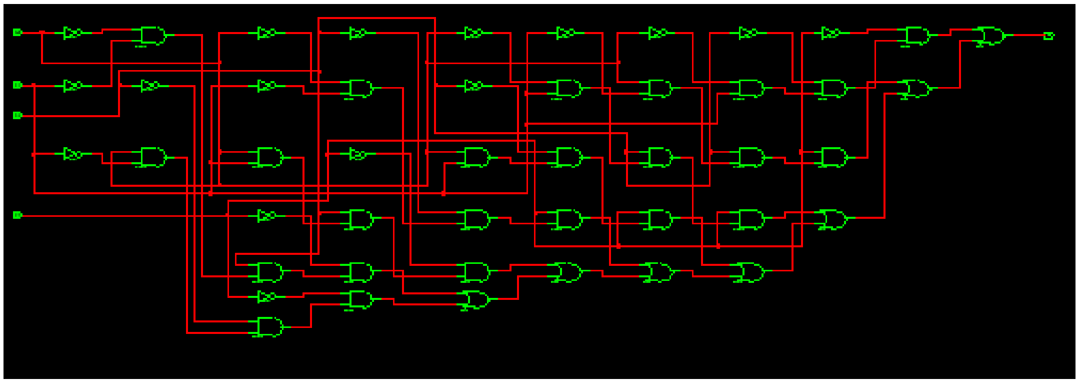
(b)

**Fig. 7: (a) Designed processor view (b) RTL schematic view**

Fig. 7(a) shows the view of the designed malicious nodes detection processor in wireless sensor networks. It receives the packets from the surrounding nodes in WSN and gives the output as either malicious or non-malicious nodes in WSN. Fig. 7(b) Illustrates the Register Transfer Logic (RTL) of the designed malicious nodes detection processor which contains lot of inbuilt slices and each slice is represented by a set of gates. Fig. 8(a) illustrates the technology schematic representation of the designed malicious nodes detection processor which contains lot of inbuilt Look Up Tables (LUTs) and each LUT is represented by a set of gates. The LUT representation of the malicious nodes detection processor is shows in Fig. 8(b).



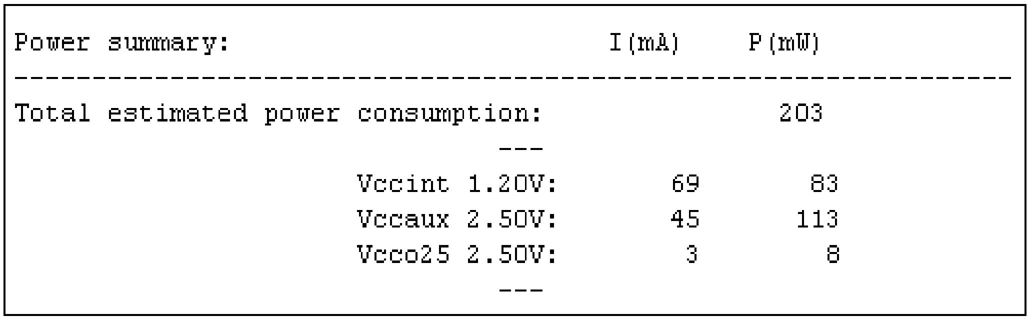
(a)



(b)

**Fig. 8: (a) Technology schematic view (b) Internal view of LUTs**

**Fig. 9 shows the power analysis report of the proposed architecture.**



```
Power summary:                                I(mA)     P(mW)
-----------------------------------------------------------------
Total estimated power consumption:                         203
                                           ---
                           Vccint 1.20V:        69         83
                           Vccaux 2.50V:        45        113
                           Vcco25 2.50V:         3          8
                                           ---
```

**Fig. 9: Power consumption report on Spartan 3E- XC3S1600E processor**

**Table 1: Analysis of power consumption of the proposed malicious nodes detection processor**

| FPGA Family | Device specifications | Package Specifications | Power Consumption (mW) |
|---|---|---|---|
| Spartan 3E | XC3S1600E | FG320 | 203 |
| Spartan 3E | XC3S500E | FT256 | 81 |
| Spartan 3E | XC3S100E | VQ100 | 60 |

Table 1 shows the power consumption of the proposed malicious nodes detection processor in terms of different device specifications and package specifications. Spartan 3E- XC3S1600E achieved 203 mW of power consumption, Spartan 3E- XC3S500E achieved 81 mW of power consumption and Spartan 3E- XC3S100E achieved 60 mW of power consumption. Table 2 shows the performance comparisons of the proposed malicious nodes detection processor in terms of power consumption.

**Table 2: Performance Comparisons of the proposed malicious nodes detection processor**

| Methodology | Year | Power Consumption (mW) |
|---|---|---|
| Proposed work | 2016 | 60 |
| Feng R et al. | 2011 | 76 |
| Babu et al. | 2014 | 82 |
| Patel et al. | 2015 | 74 |

## Conclusion

This paper proposes a novel low power malicious node detection processor which efficiently detects the malicious nodes in wireless sensor networks. This proposed architecture contains the crossbar architecture and it is used to transfer the packets to the output ports in an efficient manner. Each port controller receives the packet and extracts the two control bits. Based on the control bits the port enable is activated and it can have the permission to transfer the packets from other output ports of the crossbar architecture. The proposed architecture consumes 60mW of power consumption.

## References

[1] *Hossein Jadidoleslamy. Hierarchical intrusion detection architecture for wireless sensor networks. International Journal of Network Security & Its Applications (IJNSA), 3(5), 2011.*

[2] *Feng, R., X. Xu, X. Zhou and J. Wan. A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory. Sensors, 11: 1345-1360, 2011.*

[3] *Babu, S.S., A. Raha, and M.K. Naskar. Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN. Wireless Sensor Network, 6: 157-172, 2014.*

[4] *Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao, and C.F. Lai. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1), 2015.*

[5] *Patel, K.S., and J.S. Shah. Detection and avoidance of malicious node in MANET. International Conference on Computer, Communication and Control (IC4), pp: 1-4, 2015.*

[6] *Haripriya, Y., K.V. Bindu Pavani, S. Lavanya and V. Madhu Viswanatham. A Framework for detecting Malicious Nodes in Mobile Adhoc Network. Indian Journal of Science and Technology, 8(S2), pp: 151–155, 2015.*

[7] *Fenye Bao, Ing-Ray Chen, Moon Jeong Chang and Jin-Hee Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9(2), 2012.*