Worm Hole-Black Hole attack Detection and Avoidance in Manet with Random PTT using FPGA

Arun Kumar K A
Centre for Development of Advanced Computing
Trivandrum, India
arunkumarka@cdac.in

***Abstract*—Manet or Mobile Ad-Hoc Networks are self-forming networks which does not require a fixed infrastructure for its communication. Manet plays a critical role in Military Communication and Disaster Management system. Initially there will be multiple nodes with separate address assigned from an address pool, which will form the network when needed. Worm-hole attack and black-hole attack are the severe security issues faced by Manet. The normal security mechanisms like encryption and authentications have no big roles in these types of attacks. The paper discuss the FPGA implementation of black hole-worm hole detection and avoidance algorithm. The packets from a black-hole or worm-hole are detected in the MAC-Physical layer itself by randomly varying the Packet Travel Time (PTT). The Mac layer and the physical layer are implemented using Partial-Reconfiguration technique so that the symbol rate, modulation schemes and coding rate can be changed randomly while the system is running without using extra hardware. Probe request and probe response messages are used to ensure authentication for the nodes for forming the network.**

Key words-PTT,FPGA,RTL,Manet ,Back-off,Black hole and Worm hole.

I. INTRODUCTION

Mobile Ad-Hoc networks are capable of forming and deforming wireless networks on the fly without any installed equipment like a Base station or a mobile tower. As Manet uses open air medium for network forming and communication they are very much vulnerable to security attacks with Black-hole and Worm-Hole attacks play the major role. In Manet multiple nodes can communicate either directly or indirectly. The nodes within the range can communicate directly and the nodes outside the range will use the intermediate routes to transfer the data. If one node has a range of 1 kilometer, then N-nodes can form a network with a maximum range of N- kilometer. The mode of attacks in Manet can be passive or active. In passive attacks packets will be obtained by the malicious nodes without affecting the system, where in active attacks the packets will be dropped or altered. In worm-hole attack the malicious nodes will record the packets and passes the packets to its corresponding pair by forming a tunnel and the receiving node will sent to an authenticated node in the network. The tunnel can be a wired link or a wireless link. As a result the network topology of the two out-off range nodes will get disturbed [1], [2]. Figure 1 shows a worm-hole attack. Here the probe request message from the node D or A will be received by the attacker node W1 and tunnel the packet to its colluding node W2.

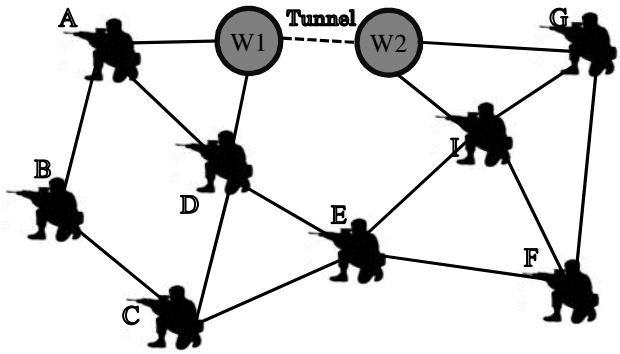

Fig 1: Worm-hole attack in Manet

Similarly the probe response from the nodes G or I will be received by node W2 and transferred to node W1 and it rebroadcast it the other nodes.

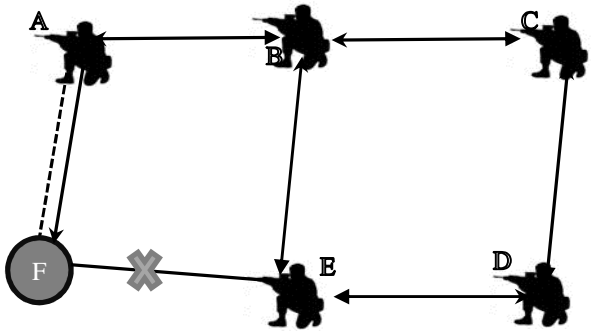

Fig 2: Black-hole attack in Manet

As a result node A will select the route A-W1-W2-I to communicate with I and a network will be formed between these two nodes with the attacker nodes W1 and W2.In

Black-hole attack the malicious node declare itself as the shortest route to the destination nodes.When a route is established with a black node the packets will be dropped by the attacker node may be selectively or completely. Figure 2 shows the black hole attack in Manet. Here the attacker node F will advertise itself as the shortest path for A to communicate with D [3], [4].

II. Proposed Solution for Worm-Black Hole

A. Partial Re-configuration

Partial reconfiguration (PR) is an implementation technique available in Xilinx FPGAs.The technique allows the user to switch between the implemented applications in minimum time if the algorithms have minor differences. This technique can be used to switch between different physical layers having different modulation schemes and coding techniques. In the PR implementation technique there is a static part and dynamic part. When the user want to switch between different modules only the bit file for the dynamic part is loaded which small in size [5].

B. Solution for Worm-hole

The solution for the Worm-hole attack is implemented in the MAC-Physical layer. The IEEE 802.11 standard is referred for the implementation of the MAC layer. The solution achieved by implementing the MAC layer and the physical layer using partial reconfiguration. In the MAC layer the total Packet Travel time (PTT) is computed and stored in a register, which will be changed randomly by the user.

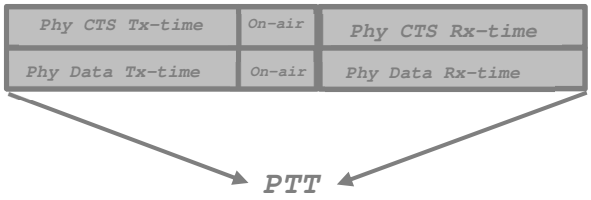

Fig 3: PTT Computation

All nodes have to send a Request to send (RTS) message to the destination message for sending a packet. This message will be generated by the MAC layer, when a new packet arrives from the upper layers. After sending the RTS message a timer PTT_{cts} will be set in the MAC layer with timeout value equal to the PTT value. The receiving node will make a CTS and set a new PTT_{pckt} timer. If the clear to send message (CTS) reaches after a specific time period the CTS packet will be dropped and retry is initiated [5]. If the CTS is reached in time the transmitting node will send the packet and will set the acknowledgement timer. If the PTT_{pckt} is timed out then the packet will be dropped.

$$ptt_{cts} = cts_{tx} + cts_{rx}$$

$$ptt_{pkt} = pckt_{tx} + pckt_{rx}$$

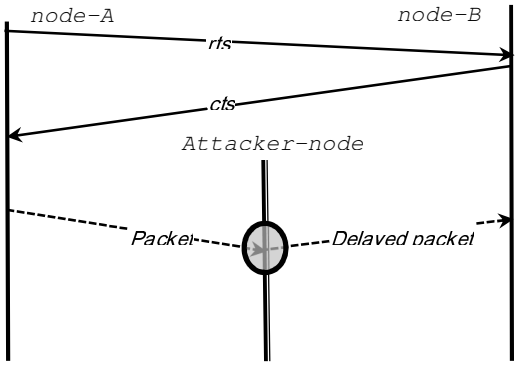

Fig 4: Node attack

But through a training process the packet travel time can be computed by the attacker node. In this paper we discuss a novel technique to solve this issue.

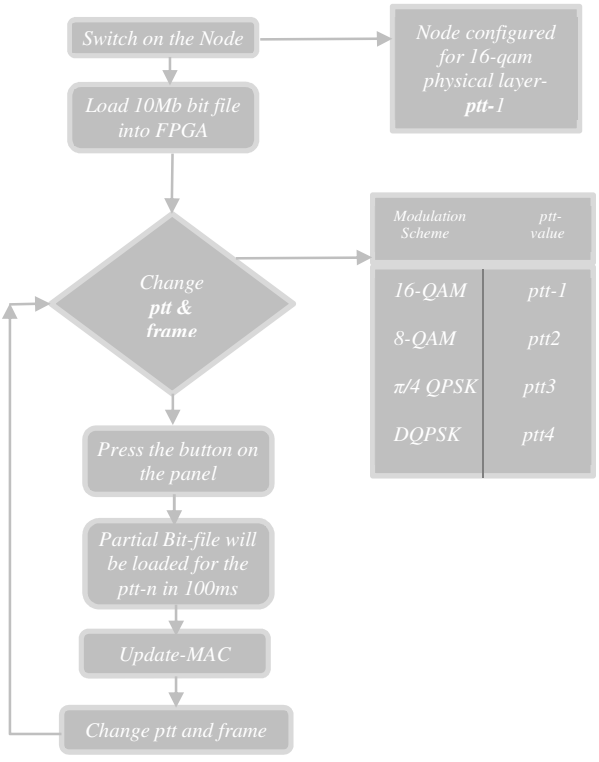

Fig 5: Flow-Diagram

Figure 5 shows the flow diagram for system configuration. Whenever the user presses push button a modulation with particular PTT will be loaded into the FPGA randomly. The mac layer and the physical layer is implemented using Xilinx partial reconfiguration. The majority modules of the Mac layer and Physical layer will form the static part and other modules will be implemented as dynamic part. Through PR the user can change the modulation schemes

and symbol rate randomly in 1s so that the PTT will also change which will be updated to the MAC layer. The Physical layer includes 16-QAM, 8-QAM, π/4 QPSK and DQPSK modules with different PTT, but only one module will run at a time. Since the PTT and packets are changed and modified randomly it is difficult for the malicious nodes to calculate the round trip time and knowing the packet structure.

C. *Solution for Black-hole*

To solve the Black-hole issue the entry of a malicious node should be stopped. Figure 6 shows the process diagram for forming a network and for data transfer. For each node to form a network a probe request message should be broadcasted and probe response message will be recovered from available nodes within the range. A specific frame structure is assigned for all the messages and packets. Figure 6 shows the frame structure for the messages, address fields are 2byte and other fields are 1 byte and the location of each field will change whenever a new partial bit file is loaded.

Fig 6: Frame-structure

The address value of the nodes are selected from an address table and the contents of the address field will change.

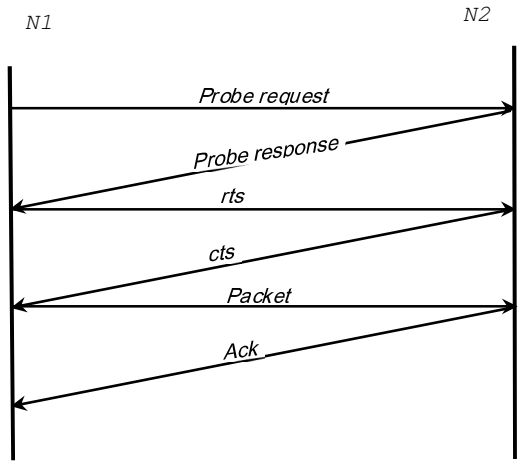

Fig 7: Process-Diagram

The address value will be any 25 values from 0 to 65536.It will be difficult for a malicious node to crack this varying frame structure and entering into the network. The MAC layer is also implemented using PR so that the frame structure of the probe request and probe response messages will be shuffled randomly. So each time when the user presses the push button a new partial bit file will be loaded which will contain a different frame structure from the previous communication. When a malicious node try to tunnel a data the PTT will change and if the PTT is above a predefined threshold the packets will be dropped with the assumption that a malicious node is in the network. Figure 7 shows the communication process.

III. SYSTEM DESIGN AND ARCHITECTURE

Figure 8 shows the architecture of the entire system. The entire system is implemented using Xilinx Artix7-200T FPGAs.The Lower MAC, a Random number Generator and the Lower Physical layer forms the Static part and the Upper MAC and the Upper Physical layer the Dynamic part. The UMAC Comprises of the Data pump and the filter MPDU module and the lower MAC modules comprises of the transmission coordination modules and the reception coordination modules.

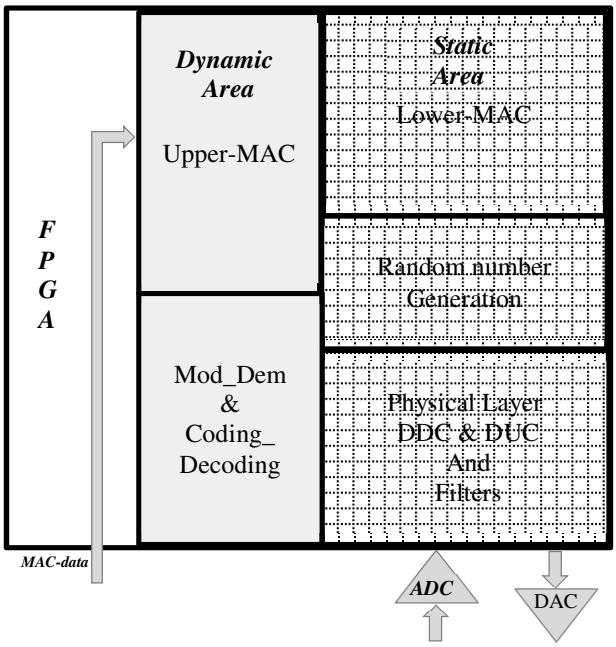

Fig 8: System Architecture

The lower physical layer comprises of the digital up-down converters and filters modules and the upper physical layer comprises of the modulation-demodulation modules and the coding-decoding modules. After final implementation there will be one master bit file and four partial bit files for different PPTs. The MAC layer is designed using VHDL and the physical layer is designed using the Xilinx system generator [6], [7].

A. *Hardware Design and Implementation*

The entire system is designed using Xilinx VIVADO, System generator, Modelsim and Matlab. Figure 9 and 10 shows the Modelsim models of the transmitter and recover respectively. The matlab environment is used to simulate the entire system and to verify the results. This model is designed using the EDA simulator Link for Modelsim in Matlab environment [8].

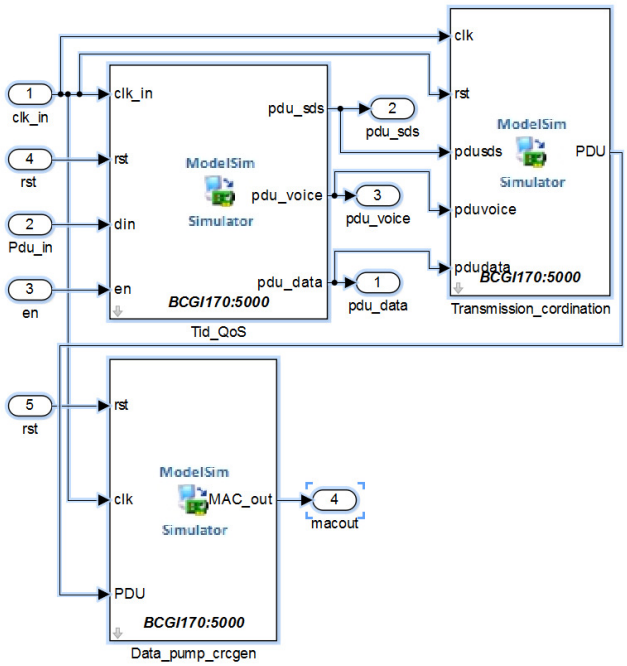

Fig 9: Modelsim Model-Transmitter

The link created by EDA simulator with the Modelsim environment is used for co-simulating the design with Matlab and Modelsim. Using the Matlab-Modelsim link the inputs can be given from the Matlab and results can be verified in the Matlab environment itself.

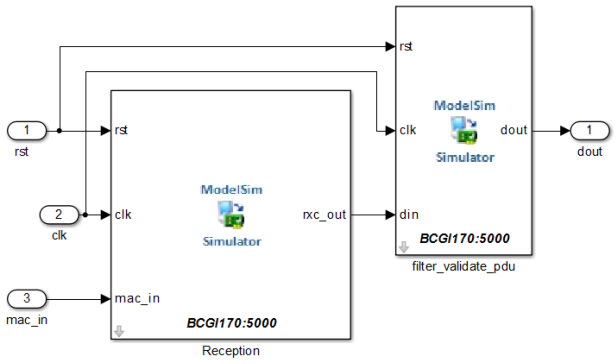

Fig 10: Modelsim Model--Receiver

Figure 11 shows the system generator model for the entire system. The black shaded module is the dynamic region of the physical layer and others are static region. System generator is a Xilinx model based design tool for FPGA implementation. The Filter modules are designed using FIR compiler modules available in system generator.

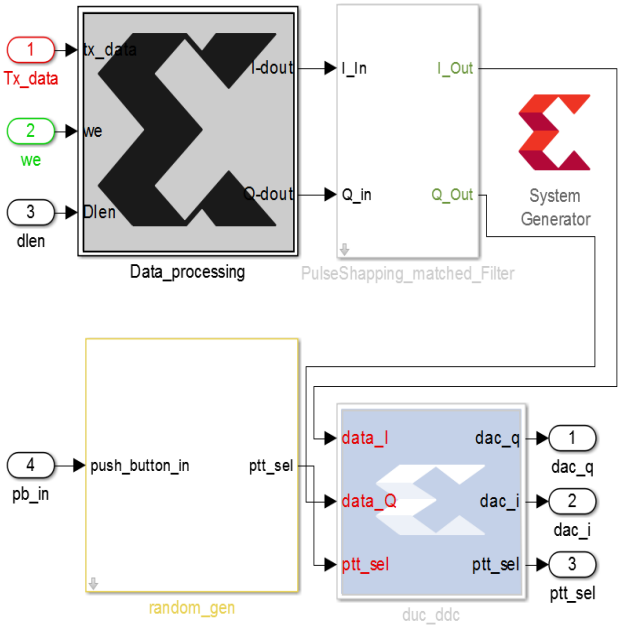

Fig 11: System Generator model

IV. IMPLEMENTATION ON XILINX FPGA

In the final implementation the Up-Converter modulated data in fed into a 16-bit DAC. The Digital Up-converter is implemented using 4-stage pipelined filters and filters with distributed arithmetic (DA) architecture.

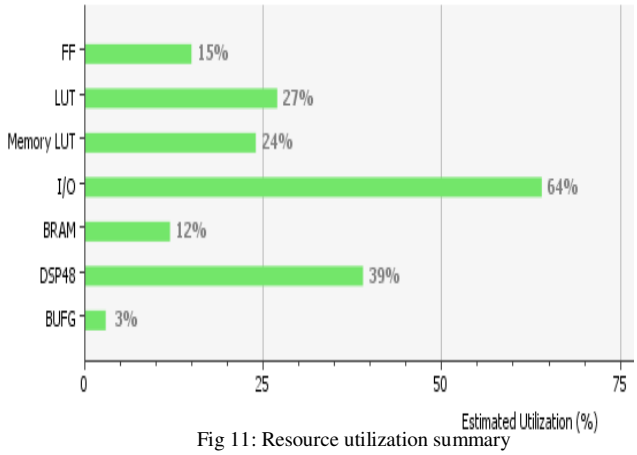

Fig 11: Resource utilization summary

In DA architecture power consumption is very low compared with pipelined architectures. The DDS module is implemented in FPGA itself for required carrier generation. Figure 11 shows the resource utilization summary of the entire system including the interfaces. The design can run at maximum operating frequency of 125 MHz

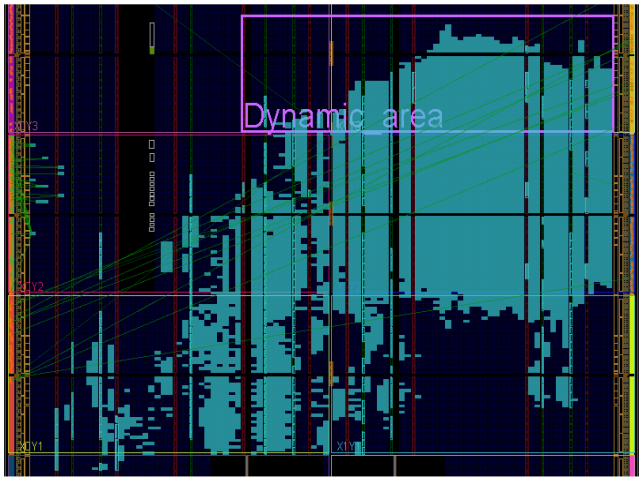

Fig12: On-Chip View

The final system integration test is done with a custom Artix-7 board. The board is integrated with a RF system and ADC-DAC system. Figure 12 shows the on-chip view of the MAC layer and the Physical Layer with the dynamic area highlighted.

V. TEST BED AND RESULTS

Three Manet nodes are used for testing purpose named as N1, N2 and N3. The test steps are

1. Two Manet nodes N1 and N3 are placed in a line within range and tested for normal communication.

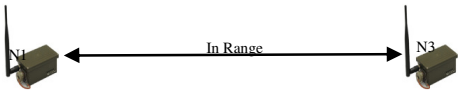

Fig13: Position1

2. Two Manet nodes N1 and N3 are placed in a line in out of range and tested for normal communication. Since the nodes are not in range packets will be loosed.

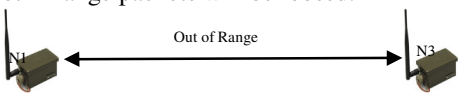

Fig14: Position2

3. Two Manet nodes N1 and N3 are placed in a line in out of range and node N2 placed in between N1 and N3.In this condition data will be transmitted in one hop. Here the address of the nodes will be changed randomly with varying modulation schemes and found normal communication taking place.

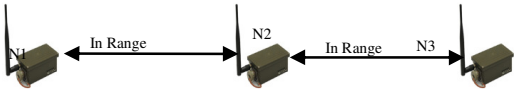

Fig15: Position3

4. Now N2 is replaced with a malicious radio R1 with no Manet properties. R1 will receive and transmit data but all the packets are dropped by N3 because of delay and address mismatch and R1 is declared as a malicious node.

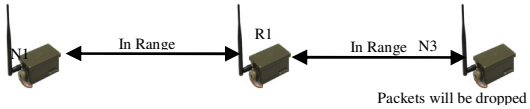

Fig16: Position4

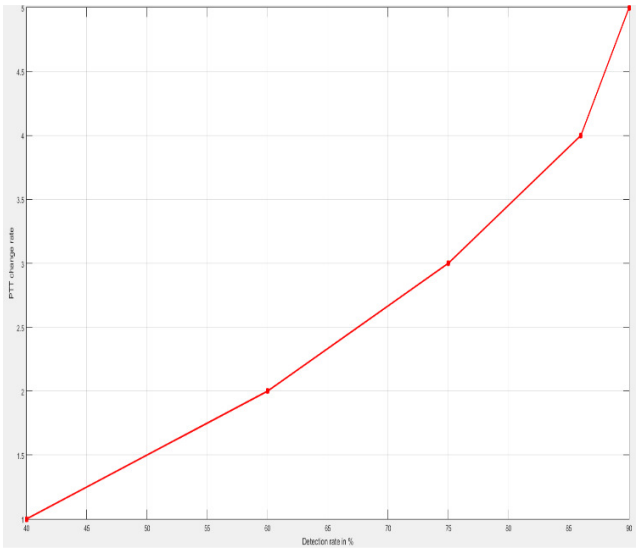

Fig17: Detection rate Vs PTT change rate

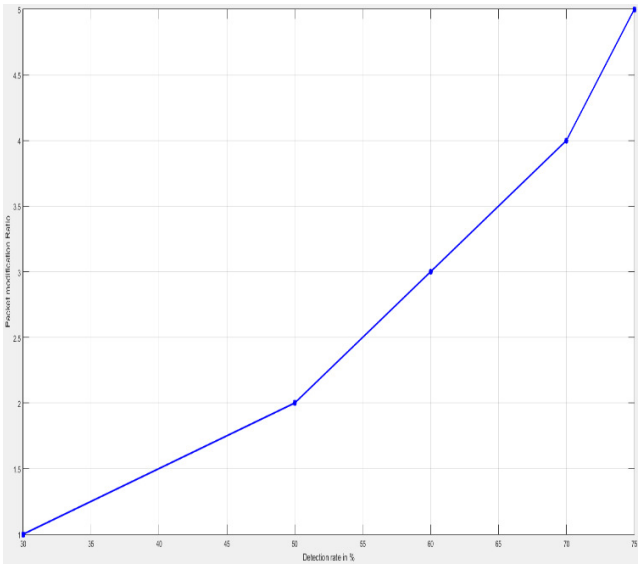

Fig18: Detection rate Vs PMR

Figure 17 and 18 shows the plots of malicious node detection rate Vs Packet modification rate and PTT change rate. The packet travel time is changed by changing the modulation scheme using partial reconfiguration. The packet modification includes modifying the address of the nodes, changing the address table etc.

CONCLUSION

Mobile-Adhoc Networks plays critical role in military communication and Disaster Management systems. Security is the major issue to this technology. This paper discussed a novel solution for the Worm-hole and Black-hole attack in Manet. By changing the nodulation schemes randomly using partial reconfiguration and modifying the packets accelerated the malicious node detection rate.

REFERENCES

1) Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE.T. Sel. Areas Commun., vol. 24, no. 2, pp. 370-380, Feb. 2006.
2) Reshmi Maulik and Nabendu Chaki , A Study on Wormhole Attacks in MANET, International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
3) Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu , Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks 1 ,Elsevier (2003) 13–64.
4) H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. IEEE *Wireless Communications*, 11(1):38–47, Feb 2004.
5) Partial Reconfiguration design with Plan ahead By: Brian Jackson version 2.1,March 2008.
6) Apichet Chayabejara, Salahuddin Muhammad Salim Zabir and Norio Shiratori, An Enhancement of the IEEE 802.11 MAC for Multihop Ad Hoc Networks, Research Institute of Electrical Communication, Tohoku University
7) J. G. Proakis, Digital Communications, 5th ed., New York: McGraw-Hill, 2008.
8) Xiaolong Li, Simulink-based Simulation of Quadrature Amplitude Modulation (QAM) System, Proceedings of the 2008 IAJC-IJME International Conference.
9) Xilinx VIVADO design suite user guide, UG 893 (v 14.3) October 10, 2014