Development of a secure and reliable Half Duplex network in FPGA.

<u>Introduction:-</u>

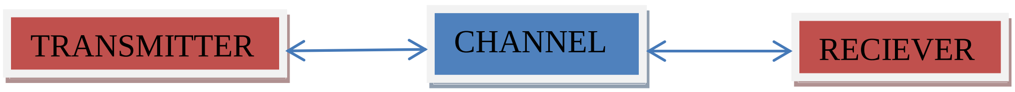
The aim of the problem is to establish a half-duplex connection which is both secure and reliable. The security in the connection is ensured by an effective encryption algorithm and secure key exchange. Reliability of the connection will be achieved through acknowledgement of the sent packet from the receiver.

To ensure security, you have to use **DH Key Exchange** for the secure key exchange and **Tiny Encryption Algorithm (TEA)** to encrypt the data.

To ensure reliability, you have to use some features of the **Transmission Control Protocol (TCP)**, a protocol used in Transport Layer in Computer Networking and few error correction techniques.

<u>Problem Specification:-</u>

- **<u>Module Layout :</u>**



Both Transmitter and receiver are to be implemented in the same FPGA kit and the virtual channel module will be provided by us.

- **<u>Connection Procedure :</u>**

Connection Establishment: Firstly, Transmitter should establish the connection with the receiver using the following handshake mechanism:
Transmitter will send SYN -----------------> and the receiver would reply with an ACK. This SYN signal generated by the transmitter should contain a random sequence number and the ACK signal should contain the acknowledgement number equal to the sequence number of the expected next packet.
After the connection is established, data transfer will take place. Since the channel is half duplex the data transfer will be unidirectional.

Data Transfer: After establishment of the connection, the transmitter and receiver will generate a key, which will be a private key known only to the transmitter and receiver. For this **Diffie–Hellman (DH) key exchange** is to be used, where the values of the required parameters is

P = 251 and **G = 11**

An 8 bit key is to be generated using this method.
For more detail about this key exchange mechanism, visit the following link

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange.

Security is ensured through **Tiny Encryption Algorithm (TEA).** For more detail about this algorithm visit

http://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm.

You just have to encrypt the 64 bit data part.The key obtained using DH key exchange is to be replicated appropriate number of times to get the required key which is to be used in TEA.

Now the encrypted data is to be taken and 2D parity checking (Error detection and correction technique) is to be applied on it and the corresponding row and column parities should be placed according to the packet specification given below.
After completing the other required details in the packet appropriately, the packet is ready to be sent through the channel.

GO BACK N ARQ protocol is to be used while sending the packets through the noisy channel. The data should be sent **serially** through the channel.

Connection Termination: The connection is to be terminated using **FIN** to be sent by the transmitter and receiver should reply with an **ACK**.

- **Transmitter :**

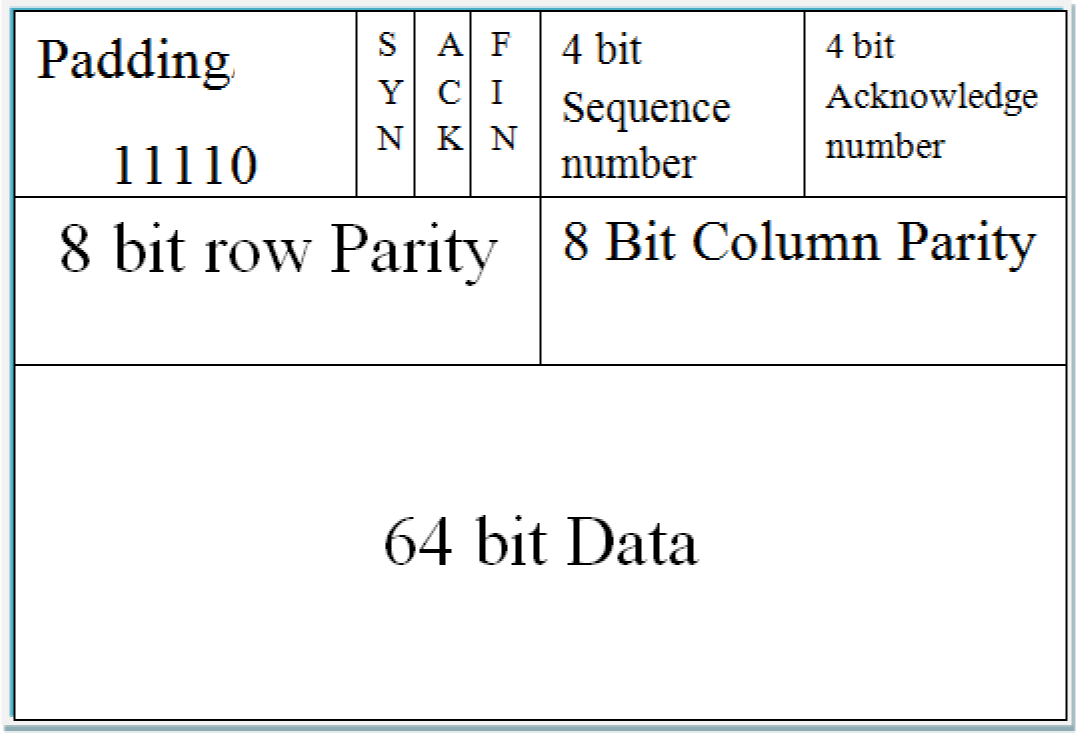
Firstly, Transmitter should establish the connection using **Connection Establishment** explained above. Then key generation is to be done by **DH key exchange**. Further data is to be encrypted using **TEA**. Then **2D parity checking** is also included in the list of work to be done by the transmitter. Then **random number sequence number** generation is also to be done within the transmitter module. Completely generated packets needs to be transmitted using **GO BACK N.**
Data should be sent **serially** through the channel**.**

- **<u>Receiver :-</u>**

  The receiver will decrypt the data, sent by the transmitter after passing through the noisy channel.
  If the data is correct and in order, the receiver will send an acknowledgement ACK of the packet it expects to receive next.
  If the data is incorrect or not in order, the receiver will discard the packet and send an ACK of the previous received packet.

- **<u>Channel :-</u>**

  The channel would be a simple combinational circuit to give the feeling of noise caused by the channel. It will be prepared by us and will be incorporated in your design at the time of event.



Padding 11110	S Y N	A C K	F I N	4 bit Sequence number	4 bit Acknowledge number
8 bit row Parity				8 Bit Column Parity	
64 bit Data					

Fig 1: Packet Specification

Total Packet size = 96 bits.
Padding sequence is used for synchronization and is fixed in our case.
64 bit data – is the data which you have got after encryption.
SYN, ACK, FIN – are of one bit each.

Important Points :

1. Data should be sent serially bit by bit through the channel. Transmitter should be followed by appropriate number of series of buffer (As per the Go Back N) and the output of the last buffer is to be used to send the data into the channel module (As of now you can consider the ideal channel and just connect it to the receiver). Receiver module should also accept the data serially.

2. Packet is to be recognized by the initial padding sequence (11110).After detecting the padding sequence the next (96-5) bits should be treated as of the same packet.

3. Channel may grab the packet, may corrupt the data part of the packet, may grab the acknowledgement, and may also cause the out of order delivery of packets. Your system should be robust to all these mishaps.

RULES AND REGULATIONS:-

1. There can be a maximum of 4 members in the same team. The members of the team need not be from the same institution. All members should be current students of a recognized educational institution. All teams and their members should register themselves at the AVISHKAR website (http://www.avishkar.in) failing which, their participation in the final rounds will not be considered.

2. The competition shall consist of two rounds. The first round, the preliminaries, will consist of the submission of an abstract that details the approach adopted by the team towards solving the problem and any progress made already. The abstract should clearly outline the following details:

   • Team details (members and their institutions, contact details including phone numbers and email addresses of each member and team name).
   • Brief introduction to the problem statement (to test your understanding of what is required).
   • Your approach towards solving the problem, including design decisions as well as technical details.
   • Work already completed (in which case a snapshot of current code is required).
   • Estimated time of completion.
   • Any other comments.

3. The final round of the competition will consist primarily of a presentation by the team, involving the following:

- Design decisions and implementation details.
- A test run on the reference software simulator and on the kit.
- A viva round.
- Any other specific request made by the judges.

4. Any kind of plagiary will lead to disqualification from ELECTROMANIA 2K11.

5. The deadline for abstract submission is 11:59pm, 10th Sept, 2011.

JUDGING CRITERIA :

- Judging will be done by faculty members of Electrical and Electronics department.
- The teams will be awarded points on the following aspects by the judges:
  - Design decisions and implementation.
  - Area used (no. of LUTs).
  - Maximum frequency achieved.
  - Presentation and viva.
  - Additional points.

Additional features:

1. LCD interfacing. The key generated using DH key exchange is to be displayed.
2. You can make more than two modules and introduce i/p layer.