CHAPTER 7

SUMMARY, CONCLUSION AND FUTURE SCOPE

7.1 CSCU BASED NODE AUTHENTICATION

In this research, a novel CSCU is implemented with check bits and tested for different combinations in the hardware control unit. Packet transmission to other nodes is prohibited until authenticated by the CSCU which controls the entry level node trustworthy check. CSCU decides the node reliability and deliver authentication signals to the node server for secure transmission and communication. CSCU is also possible to ensure mobile compatibility so that hand held devices can also join or leave the network (OTA deployment) and still the overall network will be secure.

7.2 ENCRYPTION TECHNIQUE WITH NODE AUTHENTICATION

In this work, a novel encryption technique is used for enhanced node packet network security, with a novel polarization encryption using polarised key to encrypt original node data and provide increased degrees of freedom. The ability to communicate with multiple distributed nodes in all the directions in a network topology, along with improved transmission rates is achieved.
7.3 METRICS STUDIED

Studied metrics include (but not limited to)

- Throughput
- Latency
- Response time
- Communication channel bandwidth
- Security against node data capture
- Queuing model based study
- Effects of arrival node and departure node packet rate
- Confliiction against node data replication
- Node inter packet transfer delay
- Variable node packet length transmission

7.4 HARDWARE IMPLEMENTATION OF CSCU AND ENCRYPTION

(i) CSCU check bit node based communication provides FCFS scheduler and powerful authentication facility to the node bits for data transfer.

(ii) Polarization encryption module in FL2440 board with integrated CSCU check bit that proceeds the transmission over the network.

(iii) Physical layer node authentication.

In this study work, secured node packet data transmission with CSCU network using polarization encryption is presented with relevant metrics obtained through simulation and experimentation on FL2440 hardware with Linux kernel. To enhance the node signal transmission performance $E_P$ technique is used and for enhanced network layer performance link states concept is exploited.
In this research work, the polarization encryption performed using embedded linux provides superior response and sufficient encryption bandwidth in a network to make robust node security based on cryptography technique. The polarization encryption server with FL2440 introduces a polarised key approach for scalable invariable bandwidth and also investigates an authentication scheme to avoid the entry of untrusted nodes and provide secure nodes in transmission system. The multicast node network approach is represented to cover all the directions with customize node arrangement in network and to provide shortest path between node to node link communication. Jitter effect is reduced to improve network performance, throughput and reduce packet transmission delay.

7.5 FUTURE SCOPE

Future direction of study shall focus on,

(i) Implementing alternate polarised encryption strategies and comparing its performance and effects with the proposed scheme.

(ii) Integration of CSCU and polarised encryption modules on hardware.

(iii) Study alternate strategies and compare the performance with the self-opt out strategy (proposed in this research) for energy aware routing in high availability network.

(iv) Explore the efficiency of the network by studying some more attacks on the network.