CHAPTER 1

INTRODUCTION

Wireless network is a large network system with a primary objective to provide nonblocking communication to everyone in the network and everywhere and share information among various trusted nodes in a secure manner. It represents a rapidly emerging area towards providing ubiquitous networking connections. Technologies are classified into different categories according to the range of the service area. On a worldwide scale, telecommunication companies are focusing in effective integration of multiple traffics over their node networks. Furthermore, the next generation infrastructure, aims to provide higher bandwidth, better quality for multimedia traffic, rapid data transfer and secure data transmission. Wireless systems provide information security through the mechanisms of cryptography such that computational complexity and pseudo-randomness are used with better results and improved security. The wireless networks are broadly used to support huge range of application key components in WSN design comprising of sensor nodes. Typically, the wireless network nodes monitor the surrounding environment and consist of,

(i) Processing unit
(ii) Communication unit to communicate with neighboring nodes
(iii) Onboard power supply

The node processors normally work in an unimpeded power supply environment with low cost general purpose microprocessors.
1.1 NODE AUTHENTICATION REQUIREMENTS

Node authentication in a network has gained increasing attention with necessity to provide security in different layers of the network with confidentiality and data availability. Wireless networks consist of data nodes with limited computational and communication capabilities. The expanding use of communication networks for various purposes is optimistic; however it also has developed many new serious security threats with increasing violations in the internetworking world. Secrecy is compromised if information is disclosed to users not authorized to access it. The encryption using novel schemes such as polarization methods have attracted much attention recently with high space-bandwidth product. Security is context dependent on different applications, among which the essential requirements includes;

(i) **Data Confidentiality and Integrity**: The replayed messages are recognized and discarded and shall pass the integrity check. These requirements can be satisfied by well-designed cryptographic functions and appropriate replay protection techniques.

(ii) **Authentication**: Based on the authentication results, flexible authorization and access control policies could be deployed to restrict the privilege of users (e.g. secure socket handling).

(iii) **Availability**: The network should be able to prevent an adversary from shutting down the connectivity for a legitimate individual or the entire system (DoS attack).

In this research work, hardware and software based node authentication techniques are incorporated using CSCU and encryption based technique. The cryptographic operations is compatible with the power concentrates of wireless devices; the authentication and key management protocols are scalable and ubiquitous to support user mobility and also, accommodate the inherent vulnerabilities of wireless channels.

The network should understand the security and communication environment to make decisions and manage network resources efficiently. The secure network needs to include the ability to recognize user, service provider and dynamic infrastructure. The appropriate action is to increase the optimal and efficient use of network resources in delivering high-quality
services. The different types of network layers which are necessary for a secure network adaptation process includes,

(i) End-User layer
(ii) Subscriber layer
(iii) Control layer
(iv) Network polarised encryption layer
(v) Data transmission layer

1.2 OBJECTIVES OF RESEARCH

(i) Perform node authentication before participating in the network.
(ii) Ensure secure data transmission using novel encryption method.
(iii) Implementation using hardware for fast and mobile compatible access.
(iv) The algorithms will be adaptive so as to accommodate dynamic entry and exit from the network.
(v) Transmit data from the node using shortest path, and
(vi) To incorporate intrinsic link state capabilities in the topology.

1.3 BENEFITS OF THE RESEARCH WORK

(i) The node authentication approach is modular, scalable and robust. Thus, any new design requirements can be accommodated without disturbing the existing structure.
(ii) The sequence of states forming the header (identification) data of a node, is novel and can be hard cored as a tiny chip and hence very effective.
(iii) The linux kernel of FL2440 based hardware is customized, so that proprietary soft core problems are eliminated and memory requirements are optimal.
(iv) The cycle state capture unit embedded with each node is simple and novel and transmits a sequence of cycle states. The signature generated by the individual CSCU’s are compatible both in the top-down and down-top architectures i.e. both little endian (i.e. intel) and big endian (i.e. Motorola) formats.
(v) Polarization based encryption $E_P$ provides improved degree of freedom without any increase in the number of bits.
(vi) The encryption with polarization can be performed with a third party vendor and does not require extra firewall architectures, since Ep can perform encryption even on watermarked, stegano or already encrypted data.

(vii) Individual node can communicate with one another with lesser delay (due to shortest path routing used intrinsically) and offer improved throughput, since overheads are absent.

(viii) Eliminate deadlock situations by proper synchronization schemes wherever required.

(ix) Eliminate jitter effects and increase network speed.

(x) The availability of increased degree of freedom (without increase in number of bits) makes it possible to implement the scheme using unsupervised network also. This eliminates the need for inversion or prime number factorization requirements in the analytical implementation.

1.4 PROBLEM STATEMENT AND PROPOSED SOLUTION

Problem 1

(i) Efficient scheme to identify trusted nodes in a dynamic topology environment and also facilitate contiguous working flow.

Proposed Solution

(i) Individual nodes have a unique cycle code pattern generated by respective node processor and this signature pattern is dynamic.

(ii) The cardinality of the set representing the number of possible transitions is finite and hence is realizable. However, the combinations are infinite and hence secure.

Problem 2

(i) To provide network end-to-end service with guaranteed data protection.
Proposed Solution

(i) To encrypt node data using simple encryption schemes.

Problem 3

(i) To have efficient hardware implementation.

Proposed Solution

(i) Integrate the best features of desktop architecture (toolchain requirements are minimized) and also retain the I2c, GPIO and SPI interface features of the embedded processors. In this context, FL2440 hardware with customized linux kernel and c/python userspace is used in this research. The choice of python userspace eliminates toolchain dependency. The customization of the kernel keeps the onboard memory optimum.

Problem 4

(i) To interconnect the various functional levels of dynamic topology and still provide reliable routing.

Proposed Solution

(i) Use Link state concepts and update the routing table periodically to determine the active nodes instantaneously.

(ii) This update of the routing table (in the backend) is done by hardware and hence jitter effects are eliminated.

Problem 5

(i) To avoid the need for trusted man-in-the-middle interface offering the encryption service.
Proposed Solution

(i) Geometrically polarised encryption scheme is used in this work. Hence, the data which is offered to the man-in-the-middle interface can be watermarked or hidden text (i.e. stegano) or already an encrypted data. Thus, the service provider for encryption task need not be checked for trustworthiness.

(ii) Data transmission (as packets) use hardware based polarization encryption.

(iii) Polarized output is inserted as check bits of random size and random position. This is the reason for increased degrees of freedom available to the encryption module.

Problem 6

(i) To support multicasting with optimal set of routes and energy aware routing.

Proposed Solution

(i) To deliver multi-destination packets efficiently.

(ii) To organize the different nodes direction sensitive with respect to each node and accordingly in this research work eight directions are assigned (North, south, east, west, NE, SW, corner node and boundary node).

(iii) Branches of packets are designed to have different access output ports of routers so that contention and congestion is reduced (and also deadlocks).

(iv) Shorten the length of the transmission paths.

(v) Increase the usage of y-direction channels such that the congestion of x-direction channels can be alleviated and viceversa.

(vi) To resolve the deadlock problem, when two or more packets form a circular wait and hold loop.

Problem 7

(i) To study relevant metrics demonstrating the effectiveness of the algorithms designed, implemented and tested.
Proposed solution

To achieve this, in this work, the following metrics are studied,

(i) Contention resolving ability both at input and output.
(ii) Shortest path as the cost factor for minimization.
(iii) Computing the performance of the system by varying the available degree of freedom Vs the bits used.
(iv) Comparing the obtained metrics with similar reported works.

1.5 ISSUES OF NODE DATA AUTHENTICATION IN WIRELESS NETWORK

When a node initially joins the network, the node connects to a topology in the network and is authenticated by the central processor (also called server station) and is permitted to move, join, exit and reconnect dynamically. Figure 1.1 shows that all data transfer requests from one node to another (includes server) is initiated with an authentication acknowledgement. During authentication the central unit checks the signature pattern from respective CSCU and then initiates packet transfer using polarization encryption.

![Figure 1.1 Data Transmission with CSCU Code Pattern and Validation](image)
1.6 PERFORMANCE METRICS

The metrics include (but not limited to) are,

(i) Throughput: A measurement of the data-transfer rate.

(ii) Latency: The time delay involved in moving data traffic through a network, the sources of latency are,
   a. Propagation delay
   b. Transmission delay
   c. Processing delay

(iii) Response Time
(iv) Bandwidth
(v) Resist node data replication
(vi) Revocation: A detected misbehaving node can be dynamically removed from the system. This will be particularly useful in high cluster available networks.
(vii) Scalability: As the number of nodes in the network grows, the security characteristics may be weakened. Signature schemes function just as effectively regardless of the number of nodes in the network.

1.7 MERITS OF UNSUPERVISED IMPLEMENTATION OF $E_p$

(i) An encryption system based on unsupervised networks shall offer a modular structure w.r.t. polarization encryption.

(ii) Unsupervised network has a structure (network) composed of a number of interconnected bits and hence can be typically represented as configuration bits and by mere change of configuration bits the functionality and the structure can be altered (reconfiguration ability).

1.8 HARDWARE DESCRIPTION PROCESS

In a wireless network, node and servers are interconnected and each node is considered as a node processor that provide services to other node processors connected to a specific node. In this research work a proportion of the node that offer services need to carry out an
authentication process that makes an access request. A local memory for the processor and a remote cache for the data obtained from the memory of other node data are used. The implementation of the proposed hardware description work as CSCU that checks whether the instruction captured unit is matched with given inputs. This mechanism is possible through a trigger input button pressed sequentially and each received byte of instruction (signal) is matched for a specific pattern. The proposed hardware interprocess communication module is shown in Figure 1.2, where all the processor nodes transmit data to CSCU.

![Figure 1.2 CSCU and Interprocess Communication Module](image)

1.9 CHAPTERWISE THESIS ORGANIZATION

Chapter 2

Presents the literature survey in three broad areas namely; (i) node authentication and intrusion prevention (ii) polarization encryption (iii) Hardware implementation and link state concepts.
Chapter 3

Discusses encryption technique (polarization technique), embedded linux hardware details, signature pattern formation, contention issues, multicasting modes, etc. The relevant metrics studied in detail includes, latency and improvement in throughput and packet loss.

Chapter 4

In this chapter, analytical model of the CSCU for network security is described. The CSCU implementation with node processor in wireless network for trusted node identification is presented in this chapter. The embedded linux hardware implementation of CSCU is also presented.

Chapter 5

Polarization encryption using unsupervised network is demonstrated. Shortest path and multicasting implementation is presented.

Chapter 6

Results and discussion with comparison plots and tabulations are presented.

Chapter 7

The summary and conclusion with future scope is presented in this chapter.