Chapter 1

Introduction

Wireless network technology helps user to connect at anytime, anywhere for various mobile based real time applications by using smart phone, laptops, PDAs. By providing continuous connectivity it improves quality of life of user. It is the need of today and grows exponentially. Wired and wireless network is used for various types of data i.e. audio, video, text, mail to transmit between various locations across the world. To manage this heavy traffic on network is the big issue. Network performance is depends on various QoS parameters like – delay, jitter, bandwidth and throughput. Open nature of wireless network is vulnerable to jamming. In wireless LAN, jamming is caused by disrupting and interfering wireless communication between sender and receiver such that SNR is decreased at receiver. In Wireless LAN, jamming is different to regular network interferences as it is intensely disrupts the wireless communication and decreases the network performance. Interference in Wireless LAN is the disruption caused unintentionally. Selective jamming in wireless LAN is done by unintentional interference of wireless communications between the nodes of the same networks or other wireless devices. On the other hand, attacker is usually disrupt the wireless LAN intentionally and jam the network by interrupting and preventing communications in wireless networks and degrades network performance. To understand the behaviour of a jammer and how a jammer attacks wireless LAN and how to mitigate selective jamming to achieve better network performance, it is significant to develop powerful tools for network analysis, design and management for the performance optimization of network.

Selective jamming attacks in wireless network are under an internal threat model.Selective jamming attacks are launched by the adversary node who knows the details about the network and selectively target messages of
high importance that leads network performance degradation. To prevent selective jamming attacks, we develop anti jamming algorithm that prevents the real time packet classification at physical layer. In NS2 simulation environment, the effects of AODV and DSDV routing protocol on selective jamming attacks and mitigation of these attacks in wireless network are analyzed in terms of packet delivery ratio, packet loss ratio and end to end delay.

1.1 Motivation
Wireless network technology helps user to connect at anytime, anywhere for various mobile based real time applications by using smart phone, laptops, PDAs. By providing continuous connectivity it improves quality of life of user. The need of such a solution is relevant today and growing exponentially. Wired and wireless network is used for various types of data i.e. audio, video, text, mail to transmit between various locations across the world. To manage this heavy traffic on network is the big issue. Network performance is depends on various QoS parameters like – delay, jitter, bandwidth and throughput. Open nature of wireless network is vulnerable to jamming. Jamming is defined as the interruption in the communication by intentionally degrading the SNR through sending noise signals. As the jamming is performed intentionally to disrupt the wireless communication, it is considered different from the regular network interferences. Unintentional network interference can occur due to hardware malfunction or synchronization failure etc. On the other side jamming, the intentional interference is conducted by attacker to prevent or interrupt communication of targeted user(s) in the network. To understand how a jamming attack is done in wireless networks and how to avoid jammer to achieve efficient communication for disruption, it is progressively more significant to develop powerful tools for network analysis, design and management for the performance optimization of network.
A selective jamming attack in wireless network is under an internal threat model. Selective jamming attacks are launched by the adversary node who knows the details about the network and selectively target messages of high importance that leads network performance degradation. To mitigate these attacks, we develop algorithm that prevents the real time packet classification at physical layer. In NS2 simulation environment, the effects of AODV and DSDV routing protocol on selective jamming attacks and mitigation of these attacks in wireless network are analyzed in terms of packet delivery ratio, packet loss ratio and end to end delay.

As the technology in wireless communication has evolved in current time, the jamming attack has been a research issue. It has to be considered significantly because of execution ease and resource availability. One of the major problems in networking is the Denial of Service (DoS) attack. In this attack the attacker node tries to stop the legal communication in the network. They generate intentional interference in the network to perform such activity. So to understand the issue, we have to carry out in depth study, analyze them accurately. Also we have to study various existing attacking techniques of Jamming attack and their rescue steps. The study suggests two major aspects of jamming attacks in wireless network namely types of Jammers and placement of Jammers in wireless networks for effective jamming. To address the jamming attack, various techniques of jamming, jamming detection and countermeasure mechanisms are considered. Still one of the open issues in the field, energy efficient detection of jammer and its classification are discussed here.

Most of the existing anti-jamming techniques are available for external threat model. Our focus is applying anti-jamming techniques to internal threat model in which detection of jammer is difficult. An adversary node is a part of wireless network and acts as a random jammer is a threat to the network security and performance. It is more challenging to design a detection and
Introduction

countermeasure strategy for selective jamming attacks in wireless network for providing better security at MAC layer and improve QoS parameters for performance optimization. Our research work focuses on prevention of Selective Jamming Attack – a method that can improve security and wireless network performance.

1.2 Application areas of Wireless Networking

The Wireless LAN (WLAN) is a system which is used as an evolution of Wired LAN. In this technology the radio signals are used to send and receive the data in air medium. It is best suitable in condition where installation of wired network is not feasible. Also thus we can provide on-the-spot access to required resources. Wireless LAN supports both voice and data. (IEEE 2007).

As wireless LAN (WLAN) devices increase, different standard (see appendix) exists to connect them to the outdoors. Applications such as public Wi-Fi access, Healthcare, Video surveillance, Hospitality, Location and trekking, Education, Office automation, Retail and Inventory control all require the need for outdoor wireless access. (IEEE 2007)

1.3 Description of Research Problem

With the emergence of global connectivity and growth of usage of multimedia and real time application, Good QoS from Computer network is a challenging task. Wireless network is providing any time anywhere connectivity. Open nature of wireless network is more prone to the attacks and jamming in the network. Selective Jamming Attack from the adversary node is an internal threat to the network and cause for network performance degradation. Security in wireless network and network throughput is a big concern to both users and network designers. Design of Anti jamming algorithm include Jammer detection, Jammer localization and anti-jamming measures. Proposed anti-jamming algorithm is able to do real time packet classification at MAC Layer with strong encryption mechanism to provide security at MAC layer and improve various Quality of Service (QoS) parameters like PDR, PLR and
E2EE delay. Effect of AODV, DSDV and DSR routing protocols is taken during the QoS parameters evaluation. The Proposed algorithm for prevention of selective jamming attack in wireless network is to be developed to improve QoS parameters for wireless LAN for achieving better security in network, optimize network design and improve network performance for getting better QoS under various traffic on network.

1.4 Research Objectives and Scope

The primary objective of the research work is to build an efficient algorithm for the detection and prevention of selective jamming attacks in wireless network and optimize the network performance. The issue of selective jamming attacks in wireless network is intentional interference leads to Denial of Service (DoS) and degrade the network performance.

The proposed research work has following subsidiary objectives:

- Developing an algorithm which is able to detect adversary jammer node in the wireless network which is responsible for selective jamming at real time.
- Prevention of Selective jamming attack is done by modifying the MAC header by adding hidden layer in the MAC header.
- Applying encryption method to provide security during transmission in the wireless network.
- Perform the test that examines the effect of different routing protocols – AODV, DSDV and DSR in the wireless network for avoiding the selective jamming with different aspects such as an execution time, scalability, efficiency.
- Deriving the QoS Parameters like PDR, PLR and E2EE delay to measure network performance optimization.
1.5 Organization of the thesis

The goal of this thesis is to develop effective and efficient anti jamming algorithms that can prevent selective jamming attacks in wireless network and optimize network performance. To achieve this, I organize this thesis as follows:

Chapter 1 gives the overviews of the wireless network technology and its application in the various fields. It also includes research problem, motivation, Research Objective and scope in the designing algorithms to improve security and network performance.

Chapter 2 gives the overviews of the relevant literature work related to the Selective Jamming in the Wireless Network. It contains the different aspect of preventing selective jamming attacks in wireless network work based on the literature survey. It describes the SHCS based method, CPHS based method, AONT-HS based method, and Random Key Generation based method for internal threat model in wireless network.

Chapter 3 gives the overviews of the relevant literature work related to the field of prevention of selective jamming attack in wireless network. The chapter gives the basic need of the selection of encryption algorithm for security and selection of routing protocol for alternate path routing. It explains anti-jamming algorithm and other QoS Parameters to improve network performance.

Chapter 4 describes the experimental design and also shows the performance of the proposed anti-jamming algorithm with various scenarios in simulation tools. The chapter also describes various QoS parameters like PDR, PLR and E2EDelay for different routing protocols like AODV, DSDV and DSR for comparison.

Chapter 5 describes the conclusion of the research work with necessary procedures followed to carry out experiment
Introduction

Chapter 6 is providing a possible more future scope in the available work.