Reliability and security investigations on video streaming over satellite links

Ma, Ting

2015

Ma, T. (2015). Reliability and security investigations on video streaming over satellite links.
Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/62239>

<https://doi.org/10.32657/10356/62239>

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

**RELIABILITY AND SECURITY INVESTIGATIONS ON
VIDEO STREAMING OVER SATELLITE LINKS**

MA TING

**SCHOOL OF ELECTRICAL AND ELECTRONIC
ENGINEERING**

2015

**RELIABILITY AND SECURITY INVESTIGATIONS ON
VIDEO STREAMING OVER SATELLITE LINKS**

MA TING

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University

In partial fulfillment of the requirement for the degree of

Doctor of Philosophy

2015

Acknowledgment

Four years of Ph.D. study has been an unforgettable experience for me. The completion of this thesis would not have been possible without the help and encouragement of many people.

First of all, I would like to express my heartfelt gratitude to my principal supervisor, Dr. Lee Yee Hui, for her guidance and inspiration that I found so valuable throughout this study. It has been a great pleasure to me to be her Ph.D. student. In the past four-year research time, she spent time regularly to discuss research issues with me, and gave me valuable advice to improve my work. Her great passion for research and the style of being critical has had and will continue to have excellent effects on my academic life.

I would also like to thank my co-supervisor, Dr. Ma Maode, for his valuable suggestions and help to my studies. He has always been patient and encouraging me when I encountered difficulties. He has listened to my research problems and spared time to discuss with me frequently and gave me valuable insights. His hard working and high scientific attitude will always have a positive impact on my attitude to work and study.

In particular, I would like to sincerely thank Dr. Ong Jin Teong, for his patience in sharing his knowledge and experiences in research which benefited me a lot.

Besides, I would like to express my appreciation to my peers in the laboratory, Yeo Jun Xiang, Hu Yongxu, Mao Xiaohong and Zhou Xiaoxiao for their valuable discussions. Also, I would like to give my thanks to the technician in the Communication Laboratory III, Thung Lina.

Last but not the least, I would like to present my appreciation to my parents and all my friends from the bottom of my heart, for their always kind understanding, encouragement and supports.

Scholarship granted by Defense Science and Technology Agency is gratefully acknowledged.

To my family, friends and Hu Feng.

Table of Contents

Acknowledgment	i
Table of Contents	iv
Summary	vii
List of Acronyms.....	x
List of Figures	xiii
List of Tables.....	xvi
Chapter 1	1
Introduction.....	1
1.1. Motivation.....	1
1.2. Objectives	4
1.3. Major Contributions of the Thesis	5
1.4. Organization of the Thesis	6
Chapter 2	8
Literature Review.....	8
2.1. Video Streaming via Satellite Links	8
2.1.1. Rain Attenuation on Satellite Links	9
2.1.2. Rain Fade Mitigation Techniques	11
2.2. Satellite System Security	14
2.2.1. Threats and Vulnerabilities	14
2.2.2. Security Threats Prevention	17
2.2.3. Defense Techniques against DoS attacks.....	18
2.3. SVC Video Protection.....	21
Chapter 3	27
Rain Attenuation on Video Streaming via Satellite Links	27

3.1. Video Streaming System.....	27
3.1.1. Video Streaming.....	28
3.1.2. Video Quality Measurement	29
3.2. Modeling Rain Effects on Satellite Links	30
3.2.1. Rain Data	30
3.2.2. Rainfall Rate and Signal Level	32
3.2.3. Rainfall Rate and IP Packet Loss	36
3.3. Power Control Algorithm.....	41
3.3.1. Simulation Model.....	43
3.3.2. PID Controller Parameters	45
3.4. Evaluation and Results.....	47
3.5. Miscellaneous Consideration	50
Chapter 4	55
Preventing Satellite Network from Disassociation DoS Attacks	55
4.1. Satellite Network Model	55
4.2. Disassociation DoS Attacks	57
4.3. Rabin Function.....	58
4.4. Prevent DoS Attacks to Satellite System	60
4.5. Modeling and Verification	64
4.6. Analysis of Proposed Solution	69
Chapter 5	74
Bitstream-oriented Protection for the H.264/Scalable Video Coding.....	74
5.1. An Overview of H.264/SVC.....	74
5.2. The AES Encryption Algorithm.....	76
5.3. Bitstream-oriented Protection Scheme	78
5.3.1. Design Principle.....	78
5.3.2. Slice Weighted Protection Scheme	80
5.3.3. Format Compliance.....	83
5.4. Key Management	85
5.5. Performance Evaluation.....	87
5.5.1. Preserved Functionality	87

5.5.2. Security Analysis	88
5.5.3. Computational Cost	90
5.5.4. Comparative Analysis	95
Chapter 6	99
Conclusion and Recommendations	99
Author's Publications	102
Bibliography	104

Summary

This thesis mainly presents three parts of studies, including video streaming over satellite reliability issue, preventing satellite system from denial of service (DoS) attacks and bitstream-oriented protection for the newly H.264/scalable video coding (SVC).

The study of video streaming over satellite reliability issue is performed through video streaming experiments and simulations. A video streaming experiment over a satellite link for 24 days distributed over one year is performed to investigate the effects of rain fade. Based on the measurements, models for the relationships between rainfall rate, power level, packet loss, and video quality are proposed. Furthermore, for both uplink and downlink channel, an adaptive closed loop power control algorithm, with a proportional-integral-derivative (PID) controller is designed. This is used for the mitigation of the rain-induced attenuation in order to guarantee a certain level of quality of service (QoS) and quality of experience (QoE). Simulation results show the effectiveness of the proposed power control solution and its ability to sustain video quality levels in spite of rain fades.

The aim of preventing satellite system from DoS attacks study is to improve its DoS attack detection efficiency. The proposed Rabin function protecting sequence number of each message is able to detect disassociation DoS attacks faster, for the first step of each communication session between network control center (NCC) and return channel satellite terminals (RCST) is the sequence number verification. The modeling of satellite system with Rabin function protection against disassociation

DoS attacks is proposed. We also provide modeling verifications by employing colored petri nets (CPN) tools. And simulation results show that our proposed method is efficient and practical. Further numerical analysis demonstrates the feasibility of the proposed scheme.

The last part of study focuses on the H.264/SVC video security issue. An efficient bitstream-oriented protection scheme for the H.264/SVC bitstream is presented in a compression friendly and format compliant manner. The proposed scheme is performed based on network abstraction layer (NAL) units after video compression, so the solution is bitstream-oriented. For better computational efficiency, different computation-cost cryptographic algorithms are employed to different significant content levels of SVC to provide sufficient security. The I slice NAL units from the base layer of SVC bitstream are encrypted by the symmetric AES algorithm in cipher block chaining (CBC) mode. And the other NAL units are protected by simple CBC-mode XOR cipher. Furthermore, a robust key management (key generation and distribution) mechanism is discussed to enhance security. The security analysis and simulation results further verify that the proposed methods can effectively protect the H.264/SVC bitstream at low computational cost.

The thesis contributes to the understanding of rain attenuations to the video streaming over satellite links. The analytical models for rainfall rate, IP packet loss and received power level are derived for analysis rain attenuations on video quality. A PID controller that uses an adaptive closed loop power control approach in both uplink and downlink is proposed to overcome rain attenuation for video streaming via Ka-band satellite links. The effectiveness of our proposed scheme is also verified by using simulations. The harmful effect of DoS attacks to satellite system is presented in this thesis. Sequence number protected by Rabin function is proposed to detect the malicious DoS attacks more quickly. This thesis contributes to introducing a novel H.264/SVC protection scheme at the bitstream level. Different

complexity encryption algorithms to different important levels of the scalable video content are proposed. Sufficient protection is ensured and the computational cost is reduced. A key management scheme is developed on a layer basis to further improve the protection of the encryption keys used in AES and XOR algorithm.

List of Acronyms

AVC	Advanced Video Coding
BER	Bit Error Rate
CBC	Cipher Block Chaining
CDFs	Cumulative Distribution Functions
CGS	Coarse Grain Scalability
CPN	Colored Petri Nets
CDMA	Code Division Multiple Access
DoS	Denial of Service
DVB-RCS	Digital Video Broadcasting Return Channel by Satellite
DVB-S	Digital Video Broadcasting via Satellite
ECB	Electronic Codebook Mode
EKE	Explicit Key Exchange
FGS	Fine Grain Scalability
GEO	Geostationary Earth Orbit
GPS	Global Positioning System
GOP	Group of Picture
HDTV	High Definition Television
H.264/AVC	H.264 Advanced Video Coding
IDR	Instantaneous Decoding Refresh
IDU	Indoor Unit
IF	Intermediate Frequency

IPMs	Intra Prediction Modes
JVT	Joint Video Team
LEX	Leak Extraction
MAC	Media Access Control
MGS	Medium Grain Scalability
MIKEY	Multimedia Internet Keying
MitM	Man-in-the-Middle
MOS	Mean Opinion Score
MPA	Multiport Power Amplifier
MPQM	Moving Picture Quality Metrics
MSE	Mean Squared Error
MVD	Motion Vector Difference
NAL	Network Abstraction Layer
NCC	Network Control Center
NIST	National Institute of Standards and Technology
ODU	Outdoor Unit
PCAP	Packet Capture
PPS	Picture Parameter Set
PSNG	Pseudo-Random Pattern Generator
PSNR	Peak Signal to Noise Ratio
RBSP	Raw Byte Sequence Payload
RF	Radio Frequency
ROI	Region of Interest
RRP	Reciprocal Routing Protocol
RTP	Real-time Transport Protocol
RTT	Round Trip Time
SPS	Sequence Parameter Set

SNR	Signal to Noise Ratio
ST	Satellite Terminal
SVC	Scalable Video Coding
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TS	Transport Stream
UDP	User Datagram Protocol
VCEG	Video Coding Experts Group
VoIP	Video Conferencing and Voice over IP

List of Figures

Figure 3. 1: Video transmission via WINDS.	28
Figure 3. 2: Rain rate, IP packet loss and V-Factor for a stratiform rain event at NTU.	32
Figure 3. 3: Rain rate, IP packet loss and V-Factor for a convective rain event at NTU.	32
Figure 3. 4: Signal level vs. rainfall rate (measured data and model).	34
Figure 3.5: Comparisons of predicted rain attenuation and measured rain attenuation in CDF.	36
Figure 3. 6: IP packet loss-rainfall rate: measurements versus model.....	37
Figure 3. 7: The relationship between the received power level and IP packet loss rate.	38
Figure 3. 8: Comparisons of fitted IP packet loss and measured IP packet loss in CDF.	39
Figure 3. 9: Comparisons of fitted received power level and measured received power level in CDF.	40
Figure 3. 10: The relationship between the IP packet loss rate and V-Factor.	41
Figure 3. 11 Generalized model of rain migration in power control.	43
Figure 3. 12: Block diagram of the proposed adaptive power control system	45
Figure 3. 13: Different sampling time settings for PID controller.....	47
Figure 3. 14: Received signal level and compensated power level responding to rainfall rate fluctuations with different K_i coefficients	47

Figure 3. 15: Comparisons of received signal level and IP packet loss responding to rainfall rate fluctuations with and without power control	48
Figure 3. 16: The CDF of IP packet loss rate of 2010 one-year rainfall data with and without power control	49
Figure 3. 17: Transmission power versus bit rate	50
Figure 4. 1: Satellite network system model	56
Figure 4. 2: A disassociation DoS attack.	58
Figure 4. 3: Rabin function over sequence number.	60
Figure 4. 4: RCST sign-on authentication process with NCC.	62
Figure 4. 5: Verification process of a received message.	63
Figure 4. 6: CPN model of communications with disassociation DoS attacks.	66
Figure 4. 7: Encryption to sequence number with Rabin function model.	67
Figure 4. 8: The MAC check model.	68
Figure 4. 9: The Decryption of sequence number at NCC model	69
Figure 4. 10: Probability of Successful attacks.	71
Figure 4. 11: Probability of successful attack vs. products	72
Figure 5. 1: Hierarchical prediction structure with a GOP size of eight	75
Figure 5. 2: Spatial scalability structure with two spatial layer	75
Figure 5. 3: NAL unit structure in SVC bitstream	76
Figure 5. 4: AES encryption algorithm flow chart	78
Figure 5. 5: Proposed SVC bitstream protection method	80
Figure 5. 6: The CBC modes operations	81
Figure 5. 7: The IV generation process	82
Figure 5. 8: Normalized encoding time with different settings	92
Figure 5. 9: Normalized stream file size with different settings	92
Figure 5. 10: Encrypted file size overhead	93
Figure 5. 11: Encryption time normalized to encoding time with different	

settings	93
Figure 5. 12: Calculated entropy of the stream file before and after encryption	
(a) Foreman. (b) News	95

List of Tables

Table 3. 1: Evaluation results of the fitting models	38
Table 5. 1: Selected NAL unit type.....	84
Table 5.2: Experiments settings for FORMAN and NEWS video clips.....	91
Table 5.3: Comparative analysis of H.264/SVC encryption schemes	98

Chapter 1

Introduction

The aim of this chapter is to provide an outline of this dissertation. This includes the motivation of the study, followed by the objectives, major contributions and the organization of this dissertation.

1.1. Motivation

Satellite multicast applications now plays a significant role in our daily life. Satellite systems can reach any location on the earth and provide broadcasting services from one transmitter to many receivers. With the fast growth in applications, there is an increasing demand for satellite communication systems with higher reliability and better security. Thus the reliability and security issues of satellite system should never be ignored.

With the widespread multimedia services, such as video-on-demand and video conference, live video broadcasting is becoming ubiquitous all over the world. Due to the broadcasting characteristics and the high-speed transmission rate, satellite links allow one to access live video coverage anytime and anywhere. There is an overwhelming trend towards the use of satellite communication services for digital video delivery in recent years. The video streaming via satellite links is widely used

in broadcasting and remote communications. The lower frequencies used for commercial telecommunications, like C-band (4-8 GHz) and Ku-band (12-18 GHz), have become too congested. Therefore, higher frequency bands, such as the Ka-band (approximately 20-30 GHz), are attracting growing interest for both commercial and military satellite communication. However, the disadvantage of the Ka-band is its vulnerability to signal attenuation under certain weather conditions, in particular rain [1], [2]. Rain-induced fades can cause significant propagation loss to satellite communication systems operating at frequencies above 10 GHz. Especially, rain attenuation is more severe in the tropical region where heavy convective rain dominates [3]. The rain attenuations can reach over 20 dB at approximately 100 mm/hr rainfall rate [4]. This high rain attenuation cannot be overcome simply by system margins. The effects of rain on radio-wave propagation become more severe as the frequency increases. Along with the degradation of the received radio-wave signal, the signal to noise ratio worsens, leading to a higher packet loss rate. Therefore, video services are inevitably affected by rain attenuation.

Satellite system has a wide coverage area that extremely exceeds that of a terrestrial system. Therefore, the satellite multicast applications are gaining popularity, such as high definition television (HDTV) via satellite links, telecommunications from remote locations, radio broadcasting services and amateur communications as well [5]. However, satellite systems are vulnerable to many different kinds of threats and attacks because of its dynamic broadcast characteristic [6]. The DoS attack is one of the most common attacks to satellite systems. A DoS attack involves maliciously sending bogus messages to the server, which results in interrupting or suspending the services between a server and legitimate users. Satellite systems have energy constraints and limited computational resources. Thus, flooding satellite systems with bogus packets can highly exhaust satellite systems' limited resources. Then the server's response to legitimate users significantly slows down. Furthermore, some

vicious adversaries can intentionally send spoofed disassociation requests to the server, which causes an interruption to the communications between the server and legitimate users.

The popularity of multimedia applications is increasing with steady steps. The access to the multimedia resources is no longer only depending on wired terminals, like computers or televisions, but also via wireless devices, like laptops or cell phones. But different types of end-user environments pose different requirements of the multimedia content. To be more specifically, their demands for the display resolution, bandwidth availability, energy consumption and computational power are varied with each other. Under these circumstances, the scalable video coding extension of the H.264 advanced video coding standard (H.264/AVC) is proposed to satisfy the diverse end-user device over various network conditions.

The H.264/SVC is a latest amendment standard developed by the joint video team (JVT) of the ITU-T video coding experts group (VCEG) and the ISO/IEC moving picture experts group (MPEG) in 2007 [7]. The most outstanding characteristic of the H.264/SVC is its capability to support three scalability types: the temporal, spatial and visual quality. Generally, an SVC bitstream is comprised of a base layer and several enhancement layers. Base layer provides basic quality of the video content. Enhancement layers are responsible for enhancing the video content in one of three scalability dimensions, namely frame rate, video resolution and video quality. So it is possible to encode a raw video once and decode it at different frame rates, spatial resolutions or signal to noise ratio (SNR) video qualities according to the requirements of the application device. This feature is considered as highly suitable for up-to-date diverse equipment in multimedia applications, namely video conferencing and video-on-demand. Furthermore, SVC is also suitable for video surveillance application [8]. The base layer of lowest quality can be extracted freely from the whole bitstream. In this way, only base layer of SVC archived instead of

the whole layers reduces storage consumption for video surveillance. Moreover, SVC is much more resilient to packet loss than non-scalable video coding [9]. Thus, this capacity enables SVC fit well with the “best effort” Internet and IP networks. Because the H.264/SVC has a promising future in wide ranges of applications, the protection of multimedia data issue should be addressed.

1.2. Objectives

This thesis aims to study video transmission over satellite links reliability and security issues. The study on the reliability part is to be done by investigating the effects of rain-induced attenuation on real-time video streaming via a Ka-band satellite link. The aims of this part of the study are three folds. One is to explore the correlations between rainfall rate, video quality and power level. The second aim is to derive two numerical models, relating (a) the rainfall rate with the received power level, and (b) the rainfall rate with the IP packet loss rate, based on the correlations between these parameters. The final aim of this study is to propose an effective adaptive power control technique for rain attenuation mitigation using these models.

The study on the security problem on satellite system is with the aim of protecting it from the disassociation DoS attack. In view of the recent development of protecting satellite system from DoS attacks, proposed solution is to be achieved at low computational cost and highly effectively prevent satellite system from DoS attacks. The study on the security problem on H.264/SVC video aims at protecting it at bitstream level. In order to minimize computational cost, different layers of SVC bitstream are supposed to be protected by different computational weighted encryption algorithms.

1.3. Major Contributions of the Thesis

In this thesis, the proposed objectives have been achieved. Both reliability and security issues are studied intensively. Several important contributions have been made:

1. The statistical relationships between rain attenuation and received signal level, packet loss rate, and video quality are presented. These relationships are based on experimental results obtained from a real-time video transmission via satellite links. The analytical models for rainfall rate versus IP packet loss rate and rainfall rate versus received power level are derived. A PID controller that uses an adaptive closed loop power control approach in both uplink and downlink is proposed to overcome rain attenuation for video streaming via Ka-band satellite links. The effectiveness of our proposed scheme is verified using simulations.
2. We analyze the effects of disassociation DoS attacks to satellite systems. And we propose a Rabin function based solution to protect the sequence number of communication message to detect disassociation DoS attacks faster. Models are designed based on CPN tools to verify our solutions against Disassociation DoS attacks.
3. We propose a slice weighted protection scheme to protect H.264/SVC at the bistream level. We employ different complexity encryption algorithms to different levels of the scalable video content. We provide sufficient protection but minimize the computational cost. We implement AES with CBC mode to protect most significant I picture data. P and B slices are protected by XOR-CBC algorithm. In particular, we devise IV generation to guarantee the uniqueness of IV used in AES-CBC algorithm. We design

a key dependent mapping mechanism in allocation NAL units' types to unspecified ones to increase the difficulty for unauthorized users to crack out. We propose a key management scheme on a layer basis to further improve the protection of the encryption keys used in AES and XOR algorithm.

1.4. Organization of the Thesis

Chapter 1 provides an introduction to the thesis. It gives the motivation of the research work for the author's thesis, explains the objectives of this study, and lists the main contributions in this thesis.

Chapter 2 gives a detailed literature review on the progress in this research. The literature review consists of three parts. The first part presents the application of video streaming over satellite links and rain attenuations to satellite links. The various techniques used to mitigate the rain attenuations to satellite links are introduced and studied. The second part reports the existing vulnerabilities problem of satellite system security. And the different methods employed to protect satellite system are presented. The third part gives an overview of different solutions dedicated to video security problems.

Chapter 3 introduces the proposed power control technique to mitigate rain fades on video streaming over satellite links. The configuration of the real-time video streaming system is described. The detailed process of video streaming and video quality metrics are also presented. The numerical results obtained experimentally are analyzed and discussed, based on which models of rain effects on video streaming over satellite links are derived. It is followed by the introduction of the proposed adaptive power control algorithm with a PID controller. Simulation results to demonstrate the effectiveness of the proposed algorithm are also presented.

Chapter 4 briefly describes the satellite system model and an introduction of satellite communication. Then the effect of disassociation DoS attack to satellite system is discussed and a detailed proposed scheme to prevent such an attack to the satellite system is provided. The proposed approach is evaluated by the modeling verifications and security analysis in the last part of this chapter.

Chapter 5 firstly introduces basic theory of H.264/SVC and AES algorithm. Then the proposed method to protect the H.264/SVC is presented. Lastly the simulation results and performance evaluations of our proposed scheme are discussed and examined

The thesis is summarized in Chapter 6. Some recommendations for future work are suggested in this chapter too.

Chapter 2

Literature Review

2.1. Video Streaming via Satellite Links

Satellite communication technology has been developed for nearly 60 years. Over the past few years, the popularity of satellite system application is growing because of its wide coverage and broadcast capability. Geostationary earth orbit (GEO) satellite systems have been used for many years in long distance broadcasting [10]. Today is the age of video. Creating and distributing video content is booming explosively all over the world. There is an overwhelming trend towards the use of satellite communication services for digital video delivery in recent years. For broadcasting applications, a typical example is digital video broadcasting via satellite (DVB-S). The initial purpose of this technical standard is for digital television distribution. Now this standard is also applicable for multimedia broadcasting over satellite. Later based on the previous DVB standards, DVB return channel by satellite (DVB-RCS) standards was developed to deliver multimedia services to consumers [11]. By using satellite link connections for the return channel, DVB-RCS enables two way transmissions without the need for the physical cable connections. This feature makes DVB-RCS suitable for application in many areas where there is no terrestrial infrastructure installed. The user terminal of DVB-RCS system offers an Ethernet interface that can be used for interactive IP connectivity.

Thus, DVB-RCS systems can provide full IP connectivity. For interactive communications, two or more geographically separated local area networks can be interconnected via satellite links using the IP protocol, which supports various multimedia services such as video conferencing and voice over IP (VoIP) [12]. At the transport layer, there are two protocols available: transmission control protocol (TCP) and user datagram protocol (UDP) [13]. TCP is a connection-oriented protocol, while UDP is a connectionless protocol. Since TCP offers a guaranteed delivery, the lost packet data will be retransmitted to the client. But retransmission is not affordable in video or audio streaming, for the lost packets are too late to play them. Delay-sensitive multimedia applications, like VoIP and UPTV, usually adopt UDP as their transport protocol [14]. The real-time transport protocol (RTP) at the application layer that supports various types of codecs, is responsible for end-to-end real-time service of streaming traffic by providing timely delivery of content to the applications [15].

2.1.1. Rain Attenuation on Satellite Links

Satellite communication links are subject to atmospheric effects, such as cloud attenuation and rain fade. And rain attenuation is considered as the dominant propagation impairment affecting to satellite links. Radio waves are suffered from rain absorption and scattering [16]. Thus, rain attenuation causes the loss of radio signal and degrades the reliability and performance of satellite links. Rain-induced fades can cause significant propagation loss to satellite communication systems operating at frequencies above 10 GHz [17]. The effects of rain on radio-wave propagation become more severe as the operating frequency increases. But the lower frequency bands used for commercial telecommunications, like C-band (4-8 GHz) and Ku-band (12-18 GHz), have become extremely congested currently. Higher frequency bands, such as the Ka-band (approximately 20-30 GHz) and V-band (50-

75 GHz), are attracting growing interest for both commercial and military satellite communications. However, the disadvantage of the higher band is its vulnerability to signal attenuation under certain weather conditions, in particular rain [18], [19].

Since signal attenuation by rainfall in the satellite system is significant, various methodologies on rain-rate predication and attenuation-predication have been presented to address this issue [20]. The Bryant model investigates the impact of the typical rain cell on the satellite transmission slant path [21]. The model addresses the problem from a statistical point of view. The Bryant model uses the concept of equivalent rain cell and variable rain height to derive the calculation of rain attenuation from measured rain rates. The rain cell properties are physically related to the measured local point rainfall rate by the probability factor proposed by the model. The model is then developed by proper curve fittings based on the calculated relation between the model parameters and the measured rainfall rate. More modification coefficients are added to validate the proposed model to other areas. The SC-EXCELL model is an improved version of EXCELL model and considers the effect of convective and stratiform rain separately [22]. Crane proposed the two-component rain model based on the observations of volume cells and debris for the prediction of rain attenuation statistics [23]. The cells are referred to rain showers and debris is referred to the surrounding larger regions of lighter rain intensity in the Crane two-component model. The above three rain attenuation models are examples of physical rain attenuation prediction models. Thanks to use specific physical parameters, the physical rain attenuation prediction models perform well in rain attenuation prediction. However, physical rain attenuation predication model is not suitable for application in those sites where lack specific physical parameters. Therefore, most of widely employed models are empirical models that are based on the statistical fitting of the measured database. The ITU-R model is currently most widely accepted model for the prediction of rain attenuation. The ITU-R is proposed

as an international standard of rain prediction model based on the probability of rainfall rate in the percentage of time. Since rain attenuation is more severe in the tropical regions where heavy convective rain dominates [24]. The rain attenuations can be over 20 dB at approximately 100 mm/hr rainfall rate [25]. The existing ITU-R model might not be sufficiently accurate to be implemented. Thus, some tropical areas developed the rain attenuation predication model by collecting local rainfall data to estimate it more precisely [26, 27].

2.1.2. Rain Fade Mitigation Techniques

Along with the degradation of the received radio-wave signal, the signal to noise ratio worsens, leading to a higher packet loss rate and even an interruption of communication system. Multimedia applications are sensitive to packet losses and transmission errors. Therefore, video services via satellite links are inevitably affected by rain attenuation.

This high rain attenuation cannot be overcome simply by low-power system margins. Various rain fade mitigation techniques have been proposed in order to maintain the QoS requirements for multimedia applications. In general, there are three rain fade countermeasures for satellite broadcast systems: time diversity, site diversity, and power control. The common advantage of these three techniques is that they do not impose the burden of extra bandwidth allocation, in contrast with digital processing methods such as adaptive modulation or variable symbol rate [28].

Time diversity is the retransmission of a signal several times with an acceptable delay. The receiver selects the best quality signal out of all accumulated received ones [29]. In [30], a single satellite to earth downlink employing time diversity is presented. The time diversity gain is analyzed by the variations of the time delay

ranging from 1 to 60 minutes. It is reported that the time diversity gain is an increasing function of the time delay. The performance of time-diversity satellite communication systems has also been investigated through radar simulation in [31]. It is founded that the time diversity gain will be higher than 35% if delays is more than 10 minutes. In [32], time diversity is employed as a rain attenuation countermeasure in non-real-time satellite communications. They implement time diversity to two different locations and compare the time diversity gains. The comparison results indicate that the time diversity gain is sensitive to the frequency. However, the time diversity technique is confined to those services with time-insensitive characteristics. Besides, the receiver side must have large capacity memory and powerful enough CPUs to save the information in memory and select the desired one. Thus, time diversity method puts burden on the CPU and memory size of the receiver side.

Site diversity is based on the fact that if the signal is heavily attenuated by a rain cell in one area, there will be other ground stations spatially separated that is unaffected by the same rain cell and therefore, can be used to compensate. Site diversity requires two or more stations which are spatially far enough apart to be capable of improving overall system performance [33]. The diversity gain depends on geographical site separation, elevation angle, and other factors. A site diversity method is used in Indonesia to avoid the impact of rain attenuation [34]. They select the largest SNR ratios from the two earth stations to guarantee excellent Ka-band performance. The use of site diversity to mitigate the effects of rain attenuation is considered in [35]. The two terminals are separated by 7.5 km. Through analysis of measurements of two spatial separation terminals, there is a good indication of the rain fade mitigation by site diversity technique. In [36], two weather radar datasets collected at Spino d'Adda (Italy) and Bordeaux (France) are analyzed. And the site diversity gain is assessed for the two locations. A three-site diversity measurement has been carried

out in Malaysia [37]. And they examined the performance of site diversity systems under the rainy condition. It is observed that the link availability can be improved from 97% to 99.9% using site diversity. However, the disadvantages of this technique are the cost of setting up additional sites and the requirement for data buffering.

The last but not the least, the power control approach varying the power of the transmitter aims at maintaining a desired received signal level. This is one of the simplest, most commonly used, and most efficient rain attenuation mitigation techniques available, and will be explored in this thesis.

Several power management schemes have been proposed for wireless video service in code-division multiple-access (CDMA) systems [38-39]. In such a system, the bit error rate (BER) is adjusted by controlling the transmitter power according to the importance of each video packet. In satellite communication systems, Dennis et al. have proposed a scaling uplink power control algorithm for satellite systems working in the 30/20-GHz band [40]. The proposed algorithm makes use of 20 GHz attenuation scaled to 30 GHz to adjust the transmitted power at 30 GHz. The drawback of this scheme is that the dynamic range of power control is limited to approximately 10-12 dB. In order to mitigate multi-beam co-channel interference and rain fades, the uplink and downlink power control has been implemented to SPACEWAY ka-band satellite [41]. Another adaptive transmission power control scheme using a multi-beam satellite antenna is presented in [42]. In this scheme, the transmission power of the transmitter from the satellite towards the targeted site is controlled according to the attenuation at the reference sites. This scheme is only suitable for communication systems where the distance between sites is small. If the distance between sites is large, this scheme produces little performance improvement. A power control technique is proposed for a 16 spot-beam Ka band satellite communication system in India [43]. For multi beam systems, this power

control method utilizes the adaptive power sharing of multiple beams by using multiport power amplifier (MPA). If a fade is detected, the power of MPA will be adjusted and the power of all beams will be compensated. Although there are some other solutions for satellite transmission with power control techniques [44-45], none of them have provided insights into power control for high quality video transmission over satellite links.

2.2. Satellite System Security

2.2.1. Threats and Vulnerabilities

Because of the broadcast nature of satellites, intrusion and eavesdropping in satellite communications is much easier than that in terrestrial fixed or mobile networks. Moreover, due to its dynamic member leave-join event in satellite network, the secret keys must be constantly changed, which increases the chance of suffering malicious attacks.

Generally, there are two kinds of attacks: one is a passive attack and the other is called an active attack. A passive attack occurs when someone listens to or eavesdrops on satellite network traffic. The unauthorized users can capture network traffic for analysis just by using tools, such as network sniffer or network monitor. In broadcast networks, passive attacks are the major threats. In [46], it presents a passive threat that an intruder can monitor the MPEG-2 transmissions in DVB broadcast system. Through monitoring the traffic, the intruder can obtain some confidential information about the communication parties. But the eavesdroppers will not modify the interception messages. Passive attacks not only occur on satellite network but wireless networks as well are extremely common. Moreover, it is

difficult to predict or know such kind of attack takes place.

In contrast of passive attacks, active attacks are not merely listening on the satellite network, the active intruders will try to modify the transmission data or even maliciously inject some false data streams to the network traffic. For example, adversary could modify a packet header address for the purpose of directing it to an unintended destination or modify the user data to make the clients receive the wrong content. Among active attacks, the spoofing, message modification, man-in-the-middle (MitM) attacks, Malware and DoS are most popular.

Spoofing is the most common interference in satellite navigation system [47]. Due to the long distance of travel of the radio signal, the navigation satellite signal power becomes so weak. And thus the satellite navigation receiver is vulnerable to spoofing. Spoofing is an intentional interference that misleads a global positioning system (GPS) receiver into tracking counterfeit GPS signals [48]. The target receiver might not be able to detect the spoofing attack. As described in [49], the attacker simultaneously makes spoofing to each tracking channel of the target receiver by code-phase alignment. And then the attacker generates misleading tracking information to make the receiver to track the counterfeit signals.

Message modification attack involves altering a packet header address or the user data. Then the modified message would be forwarded to its unintended destination [50]. Message modification attacks exist in the 802.11 networks. In [51], the message modification attack is considered as a security flaws in the 802.11 protocol. The attacker is able to make arbitrary modifications to the encrypted message without being detected. The message modification attack damages the data integrity.

As the name indicates, a man-in-the-middle attack occurs when two legitimate users unknowingly connect to a third device instead of connecting with each other [52]. The third device can monitor and capture the communication information between

the two devices transparently. For example, the Man-in-the-middle attack actively manipulates Bluetooth secure simple pairing [53]. The two legitimate users exchange the information during their phase of the Bluetooth secure simple pairing. Because Bluetooth is a wireless communication system, there is a possibility that the transmission could be tampered by MitM attacks. After a successful attack, the MitM attacker can intercept and modify all the data exchanged between the two victim users.

Malware represents a major security threat to computer systems. This kind of threat is performed by using malicious software to disrupt and damage the computer system [54]. Common types of malware include Trojan horse, worms, viruses, spyware, and botnets.

The last but not the least, the DoS attacks maliciously make the system resources unavailable to the authorized clients [55]. Generally, DoS attacks are divided into two types, the vulnerability attacks and flooding attacks [56]. In the vulnerability DoS attack, attacker accomplishes crashing the operating system by the execution of malware. The DoS attack targets at injecting some false packets into the network traffic to prevent communications from being forwarded properly. The malformed attack packets interact with victims (system resource exhaustion) and cause excessive memory consumption and extra CPU processing. Typical examples of vulnerability DoS attacks are the land attack and the ping of death. In the second type, flooding DoS attackers focus on disrupting legitimate users' connectivity by continuously sending the victim a large amount of network traffic or service requests to the target system. As a result, the victim responds slowly or even crashes completely, and the legitimate users are not able to communication with the victim due to congestion of workloads. A flooding DoS attack can be launched in a number of ways. There are five basic types of such attacks: the consumption of limited resources, such as bandwidth; the disruption of configuration information; the

alteration of state information; the destruction of physical network components and obstructing the communication media between the intended user and the victim. There are many examples of flooding DoS attacks, such as SYN flooding, UDP flooding and ICMP (echo requests and timestamp requests) flooding. The attacker sends out a large number of attack packets directly toward a victim and then the victim's network resource is consumed. Attack packets types can be TCP, ICMP and UDP. DoS attacks have already become a very serious threat to network security because of its simple implementation and terrible damage effects [57]. Thus, DoS attack is also our concern here in this thesis.

2.2.2. Security Threats Prevention

To prevent aforementioned security attacks, some studies have been carried out in literature. For passive attacks to satellite systems, the existing methods are mainly about prevention area. Message encryption is normally used to achieve data confidentiality. And the critical role of message encryption method is key management. Key management issue for satellite system has been studied by many researchers over the last few years. A multicast key management for satellite communication is proposed in [58]. The proposed solutions are based on the multilayer Internet protocol security and logical key. The end-user is located in one branch of the LKH tree and the satellite terminals are located in another branch. The root key in the LKH tree and a branch key secure the data content for the users. A new multicast security key management for DVB-S is proposed in [59]. This key management solution consists of two independent LKH layer architectures: a satellite layer and a terrestrial layer. Besides, all the keys of both layers are produced by chaotic generators.

Spoofing attack can be resisted by enhancing message source authentication mechanisms. The receiver side would properly authenticate the source of every message and communicate only with those messages passed authentication correctly. G. Zheng et al. propose a two-way access authentication scheme in [60]. The authentication scheme consists of four phases: mobile user registration, mobile user management, mobile authentication and authentication update. The Syverson-van Oorschot logic is employed to strengthen the authentication process to resist spoofing attacks.

Message modification attacks damage the integrity of message, so the prevention of message modification attacks relies on message-integrity check mechanisms. In [61], a message authentication and integrity protection scheme based on optically generated chaos is introduced. The proposed protocol enforces authentication at the physical layer and prevents message modification attack.

To examine and prevent MitM attacks, the security of mutual authentication needs to be guaranteed. A modification of logical reasoning model is used to improve the security of the mutual authentication protocols in [62]. The model can detect MitM attack and defend a mutual authentication protocol against MitM. In [63], an efficient three-pass authenticated key establishment protocol that provides secure mutual authentication is proposed to prevent MitM. The proposed protocol is based on elliptic curve cryptography. To detect malicious software, anti-malware and anti-virus software are like safeguard against malware attacks to prevent further spread of malware.

2.2.3. Defense Techniques against DoS attacks

The DoS attacks can be launched in many networks, either wired or wireless networks. Wireless ad hoc networks and wireless sensor networks are inevitably

susceptible to DoS attacks. Many researchers have been developing solutions to defense DoS attacks. Due to the features of DoS attacks, if the victim suffers from DoS attacks, there is nothing can be done except to disconnect the victim from the network. Therefore, the most significant requirement of defense mechanisms must be capable of detecting the DoS attacks as soon as possible. The goal of detection approaches is to distinguish malicious packet traffic from legitimate packet traffic. Several DoS attacks detection approaches to particular network environments have been proposed in the literature [64-68].

Reciprocal routing protocol (RRP) proposed by Yi Xu *et al.* is a countermeasure to detect IP layer DoS attacks in wireless networks [64]. Each node needs to undertake packet forwarding responsibility if it sends large amount of packets through other nodes. And the responsibility is proportionate to the amount of packets. Since a legitimate node is willing to take its responsibility while a malicious one would not, the normal nodes can be differentiated from the malicious ones. If a malicious node drops the packets that are supposed to be forwarded, its neighbor nodes are able to detect it and the isolate the malicious node.

A central manager solution is designed to detect the DoS attacks for wireless LANs in [65]. The central manager is a back-end server to track clients in the authentication process to detect DoS attacks. The central manager generates and manages three tables to avoid DoS attacks. The three tables record the number of login and logout requests from clients to the central manager. Moreover, a timer is defined to limit the client's response time that is no more than 30 seconds.

D. Mansouri *et al.* presents an energy-preserving solution to detect DoS in Wireless sensor networks [66]. They introduce the concept of hierarchical clustering technique. Inside each cluster, there is a controlled node analyzing the traffic. Whenever an abnormal behavior is detected, controlled nodes will send warnings to

the cluster-head.

Ping Du *et al.* describe a new IP packet size entropy-based solution for DoS attacks detection [67]. The DoS attacks are detected by identifying abrupt changes in packet size distribution. And the entropy is used as a metric for packet size distribution. By observing the time series of the entropy of packet size, a spike indicates that a possible DoS attack occurs.

In [68], a dynamic approach is developed to detect DoS attacks in wireless sensor networks. They choose some special nodes called cNodes to observe and report DoS attacks to the cluster head. The choice of cNodes in each cluster is made by using a random number generator. Besides, cNodes are changed dynamically. Thus, the proposed dynamic solution can improve security by avoiding the cNodes prediction by an attacker.

A satellite multicast system is also a wireless network. Therefore, satellite multicast communication is inevitably susceptible to DoS attacks. In order to prevent DoS attacks, a round-trip time (RTT) based prevention technique to secure satellite network is proposed in [69]. Firstly, it would make an approximate estimate of flows RTTs and their legitimate sending rates of the satellite networks. If network bandwidth consumption increases and it exceeds pre-defined threshold, the monitor will consider it as a possible DoS attack, for a high variation in bandwidth consumption indicates that a DoS attacker injected a significant amount of traffic into the satellite network system. Then the monitor sends them a test feedback requiring them to decrease their sending rates to a particular value. If a flow does not react in a single RTT, then it is considered as an unresponsive node and its packets are discarded. Although this scheme does not require high cost of computational resources, it cannot perfectly defend against DoS attack. Because this RTT based technique relies on the comparison between bandwidth consumption and pre-defined

threshold value, if the intruders launch DoS attacks and the bandwidth consumption does not exceed the threshold value, in this case, the satellite system would not consider it as a potential DoS attack. So no measurements are taken to protect satellite network. However, the satellite system is in great danger of suffering the DoS attack in the aforementioned situation.

Another solution is to design a protocol protecting DoS attacks in [70]. It uses a two-step verification method to detect the DoS attacks. Firstly, the sequence number of message is checked whether it is equivalent to the nonce value. And then monitor will make a comparison between the computed MAC value by using his private key and the one retrieved from received message header. And the last step is that NCC needs to further verify the integrity of the message. In fact, our method is based on this idea but implement Rabin function over the first step of verifying the sequence number. Due to strong protection on sequence number, then we can more quickly discard the bogus packets.

2.3. SVC Video Protection

Scalable Video Coding, an extension of H.264/AVC standard, is newly standardized by JVT of ISO/ICE MPEG and ITU-T for video data coding with various scalabilities. To ensure that content of H264/SVC being transmitted cannot be viewed by unauthorized individuals, it is necessary to secure any scalable bitstreams against possible attacks.

Encryption is a conventional technology to secure delivering the video content. Currently, various encryption schemes for the non-scalable video such as H.264/AVC and MPEG-2 have been studied a lot. These proposed encryption algorithms can be mainly classified into two categories: full encryption and selective

encryption. The first type is to employ cipher to encrypt all the video data, which generates heavy computation. The second one is to only encrypt some selected content in the video content, which achieves less computational complexity. Thus, selective video encryption methods are preferred to implement to protect video content in applications. A content-based selective encryption scheme for H.264/AVC is proposed in [71]. The video with different content features are encrypted adaptively in the unit of group of picture (GOP). For partially H.264/AVC encryption, the codewords of intra-prediction mode, the sign bit of the codewords of DCT coefficient and the info_suffix of the codewords of MVD are encrypted in [72].

Although various encryption approaches for multimedia information exist, these approaches are mainly presented for non-scalable video coding feature. For scalable video coding encryption, it is necessary to preserve the scalable feature of SVC after encryption. Different layers with specific resolutions can still be extracted from the encrypted bitstream. Since the H.264/SVC is a newly proposed standard, the security study on it is not as extensively as other previous proposed video codec. In literature, encryption schemes for SVC can be classified into two categories: the compression-integrated encryption and the bitstream-oriented encryption [73]. The compression-integrated encryption scheme can be performed during different stages of the compression process of H.264/SVC, while the bitstream-oriented encryption method is conducted after video compression.

The approaches of compression-integrated encryptions to H.264/SVC have been presented in [74], [75], [76], and [77]. H264/SVC contains one base-layer and several enhancement-layers. Suwan Park and Sang-Uk proposed a selective encryption scheme which is performed at all layers and each layer being encrypted with mutually different keys [74]. For the base layer, three domains (temporality, spatiality and quality) of the intra prediction modes (IPMs) of 4×4 luma block, the motion vector difference (MVD) and the sign bits of the texture data are chosen to

be encrypted. The proposed scheme encrypts with three domains in hierarchical layers using independently different keys. For the enhancement layers, only important domain of aforementioned three domains would be applied encryption according to its specific scalability type. But they did not discuss the key generation and distribution in further detail. In [75], encryptions of the sign of texture, motion vector and FGS data are carried out. A layered encryption scheme is introduced to protect the SVC by leak extraction (LEX) cipher algorithm in [76]. The proposed scheme encrypts different layers of H264/SVC. From the structure of H264/SVC, the base layer of H264/SVC bitstream is more important than the enhancement layers, for base layer is the basis of the enhancement layers. For the base layer, they conduct the intra-prediction mode and residual sign encryption. While the enhancement layers are classified into temporal scalability layer and spatial/SNR scalability layer. For enhancement layers, only light-weighted encryption is applied. The LEX algorithm that is based on AES is adopted as stream cipher in their proposed method. For these three proposed methods, only protection on the sign bit of texture data cannot guarantee the full reliability of encryption. Y. Kim et al. propose to protect the region of interest (ROI) of H.264/SVC in [77]. Their method mainly aims at securing the ROI, which is regarded as an important and valued area of video content. In H264/SVC, encoded bitstream is composed of NAL units which contain NAL header and their data payload. And hence, the ROI is distinguished from a picture by identifying the slice group id in the NAL header. After selecting the ROI units, the XOR-operation is performed to encrypt sign data of selected units. All the texture, motion vectors and the fine grain scalability (FGS) belonging to ROI are considered to be encrypted. But the ROI is difficult to be defined and represented for different video security requirements.

The main disadvantage of compression-integrated is its lack of flexibility in applications. The compression-integrated scheme is only for online scenarios, for

once compression needs to be done, and the encryption has to be performed to videos as well. But the bit-stream-oriented method can be applied for both online and off-line scenarios [78]. Besides, the main drawback of compression-integrated method is highly computational cost of compression for both encryption and decryption process. Since the H.264/SVC bitstream consists of NAL units, the bitstream-oriented schemes for SVC encryption are performed at NAL unit level. The bitstream-oriented schemes of protecting the SVC bitstream have been proposed in [79], [80] and [81]. According to Li Chunhua et al.'s solution [79], the NAL unit whose type is instantaneous decoding refresh (IDR) picture, sequence parameter set (SPS), or picture parameter set (PPS) are ciphered by LEX algorithm. But this kind of selective encryption cannot ensure completely security as some NAL units unencrypted. A format-compliant encryption of SVC is proposed in [80], [81]. To achieve format compliance, the encrypted NAL units' types are replaced with unspecified NALU types. Then these NAL unit payloads are encrypted by the AES block cipher in electronic codebook mode (ECB). But it is not safe for encrypting more than one block with one identical key. And it is also inefficient to implement AES to all the NAL units, which requires long computation time and resources.

Mokhtarian and Hefeeda propose a secure authentication scheme of transmission H264/SVC [82]. First of all, during the generating the authentication information stage, the authentication information is attached to specific network NAL units of the stream in a video format-compliant manner. To prevent the authentication information from loss, it makes copies of the authentication information. And then the rewritten SVC video streams undergo the verification process. The result of verification operations should achieve all possible sub-streams that can be extracted from the original stream can be effectively and successfully be verified. In case of any mismatch data occurs, such data is marked as unauthentic and is discarded at last. The remaining part of the stream is recognized as authentic one. Given that the

hierarchical structure of H.264/SVC video stream, whose levels consist of GoPs, temporal layers, frames, spatial/CGS layers, MGS quality layers, and finally, video frames, so the authentication process should be a bottom-up manner and secure all layers of H264/SVC. The hash function and digital signature are used to secure on the streams to prevent any changes in the contents of any video frame, frame insertion, frame reordering, frame removal or any other type of tampering.

Tomas et al. presents a novel architecture for the secure delivery of encrypted H.264/SVC bitstreams [83]. The architecture called SVC-sec that exploits the structure of an SVC bitstream in order to efficiently deliver the bitstream while providing end-to-end security for content providers. This architecture relies on a block cipher and stream cipher in CBC mode of operation. In the encryption order of their proposed mechanism, the packets from base layer enjoy highest priority, followed by medium grain scalability (MGS) and FGS, the coarse grain scalability (CGS) packets would be ordered to the end of the bitstream.

The key management is a critical issue to enhance the security of any cipher algorithm. To our best knowledge, the existing H.264/SVC authentication schemes are quite limited, only in [84-85].

A hierarchical key management is designed for H.264/SVC in [84]. The different layers in the bitstream will be assigned a class identity. And a key server will generate the root key and all the layer keys. The layer key will be sent to user by the key server. Each layer will be encrypted by a layer key corresponding to its privilege. Besides, the user can use his layer key to derive his successor layer keys.

A standard key management protocol called multimedia Internet keying protocol (MIKEY) is used to solve key generation and distribution problems for H.264/SVC in [85]. In MIKEY system, there are TGK master keys, TEK traffic encryption keys, master encryption keys, authentication keys and salt keys. TGK master keys are

generated by Diffie-Hellman algorithm and it generates the TEK traffic encryption keys. And TEK further generates the master encryption key, authentication key and salt keys.

Chapter 3

Rain Attenuation on Video Streaming via Satellite Links

3.1. Video Streaming System

The video streaming system is demonstrated in Fig. 3.1. The video streaming system is composed of a video server and a video receiver, both of which communicate via the wideband inter-networking engineering test and demonstration satellite (WINDS) using ultra-small aperture terminals (USAT). WINDS was launched by the Japan aerospace exploration agency (JAXA) and the national institute of information and communications technology (NICT) in February 2008. WINDS aims to develop technologies for ultra-high data rate satellite communications in the Ka-band [86]. The USAT with a two reflector antenna is an earth station developed for easy deployment and installation in inaccessible areas for communication purposes. A significant characteristic of the USAT is its ability to provide high-speed communication at a downlink rate of 155Mbps using an ultra-small reflector antenna with a diameter of only 45cm [87]. The indoor unit (IDU) in our system provides

time division multiple access (TDMA) synchronization, data modulation and demodulation. In transmission mode, the IDU implements code modulation for the data on the Ethernet interface from the user equipment and outputs it to the outdoor unit (ODU) which is responsible of converting the intermediate frequency (IF) signals to radio frequency (RF) signals and vice versa (Fig. 3.1). Video streaming can be performed in either unicast or multicast transmission mode over the WINDS platform.

Figure 3. 1: Video transmission via WINDS.

3.1.1. Video Streaming

A loopback transmission mode is adopted in our experiment to investigate the characteristics of video communication via satellite. The content is transmitted from our site via the uplink to the WINDS and received back at the same site via the downlink. WINDS acts as a bent pipe, receiving and then re-transmitting back to the same site. If the transmission suffers rain fades, both the uplink and the downlink are

affected. In this thesis, the measured two-way loss rate is referred to as IP packet loss rate.

For satellite transmissions, a video codec with high compression efficiency is required. The H.264/AVC is chosen as the video codec for the video streaming experiments [88]. Considering the maximum raw data rate of approximately 4.96 Mbps on the loopback link, the video is compressed to 3.5 Mbps to allow for sufficient room for packetization and other overheads. After encoding, the video elementary stream is multiplexed into an MPEG2 transport stream (TS) using the tsMuxer software [89]. The IP packets of a streaming session with a direct PC-to-PC link are recorded using tcpdump [90] into a packet capture (PCAP) file for consistent repeatable playback and post-processing.

In our real-time video streaming experiments, tcpreplay [90] is adopted to play back the PCAP files at the video server over the WINDS links in a continuous loop. The client side runs tcpdump to log the network traffic and capture the arriving video packets in PCAP format. Post-processing and analysis is then performed on the PCAP files in order to extract various quantifiable parameters from the captured files, such as the packet loss rate and the V-Factor.

3.1.2. Video Quality Measurement

Losses of the satellite signal due to rain attenuation will directly affect the transmitted bit stream. The resulting errors will be observed as packet loss at the receiver end. Thus, packet loss will be taken into consideration throughout the following analysis.

Based on the decoded video after reception, both objective and subjective techniques can be adopted for quality assessment. Subjective video quality evaluation is

concerned with how video is perceived by a viewer and his or her opinion of a particular video sequence [91]. The mean opinion score (MOS) is usually adopted to assess perceived quality in the subjective video evaluation. Time-consuming and cumbersome are the main drawbacks of subjective video quality assessment, especially when it involves hundreds of hours of continuous video monitoring as in our experiments. Objective video evaluation techniques on the other hand use mathematical models to estimate the quality of a video as perceived by the human eye. Most image processing studies only implement basic objective quality measurements such as the peak signal to noise ratio (PSNR) and the mean squared error (MSE). However those are not only unreliable but also impractical for measuring the quality of streaming video [92].

The hybrid V-Factor metric based on moving picture quality metrics (MPQM) is applied to measure video quality [93]. The V-Factor metric is based on deep packet inspection of the video stream. The overall V-Factor value is computed by a codec-specific curve fit equation using the inputs from a bandwidth model, the video coding layer (VCL) complexity model and the loss model. So the V-Factor can indicate the influence of the delay and the bandwidth to the video quality. It takes into account not only the impact of network impairments, like jitter, delay and packet loss, but also the impact of video impairments due to the contents characteristics, the compression mechanism and bandwidth constraints. The value of V-Factor ranges from 1 (bad) to 5 (excellent) in accordance with MOS.

3.2. Modeling Rain Effects on Satellite Links

3.2.1. Rain Data

Data was collected in video streaming experiments conducted over two days each month for an entire year. Two common types of rain events, namely convective rain and stratiform rain, have been observed during our experiments. Stratiform rain has a relatively low rainfall rate of less than 25 mm/hr, and generally lasts for a longer period of time. The rainfall rates of convective rain on the other hand exceed 25 mm/hr, but these events typically last for a short period of time. Fig. 3.2 depicts the data collected from May 20th to 21st, 2010 as an example. A stratiform rain event with up to 6 mm/hr of rainfall rate at around 17 hours into the experiment was recorded. This stratiform rain event lasted for a period of over 4 hours. This rain event resulted in a power level drop of up to 5 dB and an IP packet loss rate of up to 4%. The V-Factor occasionally drops to 1 throughout the rain event. Fig. 3.3 shows another data set collected from June 21st to 22nd, 2010. An obvious convective rain event with up to 60 mm/hr occurred at the 9th hour of the experiment, which caused signal levels to drop by approximately 17 dB. Unlike the stratiform rain event, this convective rain event lasted for only 40 minutes. Accordingly, this convective rain event leads to nearly 100% IP packet loss and unacceptable video quality (V-Factor of 1) for the entire duration of the rain event.

Figure 3. 2: Rain rate, IP packet loss and V-Factor for a stratiform rain event at NTU.

Figure 3. 3: Rain rate, IP packet loss and V-Factor for a convective rain event at NTU.

From the measurements, it can be seen that the rainfall leads to a decline in the signal level and an increase in the IP packet loss. To quantify the impact of rain fades on both received signal level and IP packet loss rate, the measurement results were used to model the relationships by means of least mean squared curve-fitting.

3.2.2. Rainfall Rate and Signal Level

An exponential function (3.1) can closely fit the experimental data:

$$P = 16.57 * e^{-0.04363 * r} - 33.57 \quad (3.1)$$

where r represents the rainfall rate, and P is the received signal level. Fig. 3.4 shows a plot of the signal level versus the rainfall rate. From the depicted model behavior, the received signal level decreases exponentially with the increase of rainfall rate. The signal level initially drops fast while its deterioration saturates after the rainfall rate reaches 24 mm/hr. The proposed generalized rain attenuation prediction model is developed by using the curve fitting of measured rain fall rate and received power level. The more generalized model of the rain attenuation can considered as:

$$A_p = A_o - \eta e^{-\alpha R_p} \quad (3.2)$$

where A_p is the rain attenuation at exceeding time $p\%$ and R_p is the corresponding rainfall rate. Other parameters A_o, α , and η are correcting coefficients for the curve fitting. The exponential function is used to correct the inaccurate prediction of the ITU model at large rainfall rate. Our proposed model is based on the measured data. Some parameters may be varied for different regions. The difference between the proposed model and measured statistic is small. As a result, the curve fitting method can best predict the rain attenuation in the local area with better accuracy.

Figure 3. 4: Signal level vs. rainfall rate (measured data and model).

The existing ITU-R P.618-10 prediction models have been developed to calculate the rain attenuation [94]. This model can estimate long-term statistics of the slant-path rain attenuation at a given location for frequencies up to 55 GHz. Therefore, a comparison between the proposed model and the ITU-R model will be performed here.

The ground station USAT is located at Singapore (1.34°N, 103.68°E) with an elevation angle of 45°. The specific attenuation γ_R can be obtained using the frequency-dependent coefficients given in Recommendation ITU-R P.838 [95] and the rainfall rate exceeded at 0.01% of time, $R_{0.01}$:

$$\gamma_R = k(R_{0.01})^\alpha [dB / km] \quad (3.3)$$

Besides, the effective slant path length L_E is calculated using the elevation angle, latitude, and the rain height which is the mean rain height above mean sea level (refer to [94] for details). The attenuation exceeding 0.01% of the year $A_{0.01}$ is calculated as follows.

$$A_{0.01} = \gamma_R L_E [dB] \quad (3.4)$$

Finally, the estimated attenuation to be exceeded for other percentages of an average year, in the range 0.001% to 5%, can be derived from $A_{0.01}$ by:

$$A_p = A_{0.01} \left(\frac{p}{0.01} \right)^{-(0.655+0.033 \ln(p)-0.045 \ln(A_{0.01})-\beta(1-p) \sin \theta)} \quad (3.5)$$

where $\beta=0$ when $p \geq 1\%$ in our case.

Since the ITU-R model is a widely accepted rain attenuation prediction model, a comparison between the ITU-R model and our proposed model is made. Fig. 3.5 depicts the cumulative distribution functions (CDFs) of rain attenuation based on both models in comparison with our measurements. It can be observed that the predicted rain attenuation is within close range for both models and is consistent with the measured attenuation. Besides, general attenuation CDF trends for both models are similar and resemble the real situation. In conclusion, the comparison indicates that the proposed model fits the measured data well and is also consistent with ITU-R model. The proposed model is not complex but a simplified exponential function whereas the ITU-R model involves the solving of a series of complex equations. Therefore, our model has the advantage of wide prediction range and simplicity.

Figure 3.5: Comparisons of predicted rain attenuation and measured rain attenuation in CDF.

3.2.3. Rainfall Rate and IP Packet Loss

Next, the relationship between rainfall rate and IP packet loss is derived from the measured data. A hyperbolic tangent function (3.6) is used to model the relationship between the rainfall rate and the IP packet loss. The measured data shown in Fig. 3.6 are used for the curve fitting calculations.

$$L = 49.83 * \tanh\left(\frac{r - 38.7}{16.981}\right) + 48.7961 \quad (3.6)$$

where L is the IP packet loss rate, and r represents the rainfall rate. The other numeric values are generated from the curve fitting calculations. The function of all the numeric values is to shape the curve to best fit the measured data. The value 16.981 is to adjust the smoothing level of the hyperbolic tangent function curve. The value 38.7 is to shift the hyperbolic tangent function curve in the X-axis. The value 49.83 is to adjust the curve in the Y-axis and 48.7961 is to shift the hyperbolic tangent function curve in the Y axis. The plot in Fig. 3.6 illustrates the effectiveness of this

fit.

Furthermore, the mathematical relationship between the received power level and IP packet loss rate can be derived from (3.1) and (3.6).

First of all, the rainfall rate can be expressed in terms of the received power level P in (3.7).

Figure 3. 6: IP packet loss-rainfall rate: measurements versus model.

$$r = \frac{\ln \frac{P + 33.57}{16.57}}{-0.04363} \quad (3.7)$$

given the mathematical property of (3.8)

$$\tanh = \frac{e^x - e^{-x}}{e^x + e^{-x}} \quad (3.8)$$

we can obtain the direct correlation between received power level and IP packet loss as (3.9).

$$L = 49.83 * \frac{20.5529 * (P + 33.57)^{-2.6996} - 1}{20.5529 * (P + 33.57)^{-2.6996} + 1} + 48.7961 \quad (3.9)$$

The measured data and the modeled relationship in (3.9) between the received power

level and the IP packet loss is depicted in Fig. 3.7. As seen, the proposed model closely fits the measurements. The IP packet loss rate increases with declining received signal level.

Table 3.1 shows the numerical quality of the model fits in terms of root mean squared error (RMSE) of the residuals and R-square. The RMSE measures the difference between predicted value and actual value. The R-square indicates the quality of fit of the model, where a value of 1 indicates perfect agreement between predicted and observed values.

Figure 3. 7: The relationship between the received power level and IP packet loss rate.

Table 3. 1: Evaluation results of the fitting models

Evaluation metric	Model of received power versus rainfall rate (Eq.1)	Model of IP loss versus rainfall rate (Eq.5)	Model of IP loss versus received power (Eq.8)
RMSE	0.51 dBm	0.90 %	1.22 %
R-square	0.9908	0.9995	0.9990

The RMSE for our proposed fitted models is low and R-square values are very close

to one, therefore all three models provide excellent fits to the measured data.

In order to verify the fitting results, CDFs of the received power and IP packet loss rate over one-year experimental days are calculated by applying the fitting models to the full one year rainfall data. Comparisons between the model predictions and the measured data are shown in Fig. 3.8 and Fig. 3.9. In general, there is a very good agreement between the model predictions and the measured data. The major advantage of the demonstrated correlation is that, based on a given rainfall rate, predictions of the received signal level and IP packet loss rate can be obtained. This allows us to effectively implement a power control scheme using the proposed models.

Figure 3. 8: Comparisons of fitted received power level and measured received power level in CDF.

Figure 3. 9: Comparisons of fitted IP packet loss and measured IP packet loss in CDF.

Since there is a direct relationship between IP packet loss rate and video quality, we need to determine the maximum acceptable IP packet loss rate that will produce a video quality that is still acceptable to viewers. In order to better demonstrate the relationship between IP packet loss rate and V-Factor, we have compiled all the experimental data together. The V-Factor is shown as a function of IP packet loss rate in Fig. 3.10. V-Factor shows a sharp step function, which shows that a V-Factor of 3 or above (indicating acceptable or better video quality) can be achieved when the IP packet loss is below 1%. The V-Factor drops below 1.5 (indicating unacceptable video quality) when the IP packet loss goes above 1.05%. Consequently, 1.05% IP packet loss rate has to be maintained to guarantee acceptable video quality. For the purpose of our experiments, the IP packet loss rate is therefore the major parameter that will be analyzed for our proposed power control scheme.

Figure 3. 10: The relationship between the IP packet loss rate and V-Factor.

3.3. Power Control Algorithm

As shown in the previous section, video quality is directly dependent on IP packet loss, which in turn is determined by received signal strength. Therefore, in order to guarantee an acceptable video quality under different rainfall rate conditions, a certain level of transmit power has to be compensated. Conventional schemes like uplink power control or downlink power control are based on adjusting either the earth station transmitting power or satellite transponder gain. Those methods working alone suffer from latency caused by long round trip delay. Furthermore, the required compensation power or gain becomes a serious burden when either the satellite transponder or earth station is working alone under power control process. This will easily push them to their power limits.

An adaptive closed loop power control algorithm with PID controller is proposed with combination of the uplink power control and the downlink power control schemes. The PID controller has been widely adopted in systems with feedback to

efficiently achieve stabilized state [96-97]. As weather conditions are always changing, a closed loop feedback power control system is needed to achieve the aforementioned compensation of the transmitting power. The benefit of a closed-loop power control approach is that it is able to adjust the transmission power adaptively according to current weather conditions in real time. In addition, a PID controller can help to smooth the feedback process, especially under drastic changes in rainfall rates. The proposed adaptive power control mechanism is designed to adjust both the satellite and earth station transmitting power in accordance to the commands generated by comparing the target and measured received signal level. Due to the contributions from both the satellite side and earth station side, the loop is expected to react more quickly to the adjusting command. This will shorten the system stabilization time. Moreover, both satellite transponder and earth station share the responsibility to supply the required power compensation. Therefore, problems due to power limitation will be alleviated as well.

The more generalized model of rain mitigation in our proposed power control is shown in the following Fig. 3.11. P_{rec} is defined as the received power level. P_{tar} is predefined target received power level. P_{mcp} is defined as maximum compensated power. P_{tr} is defined as the transmission power. At earth station, it takes a target received power as a reference level and compares the received power level with the reference level. If the received power level is not less than the target received power level, then it is no need to compensate the transmission power. If the received power level is less than the target received power level, then the compensated power level is calculated. Besides, PID controller is employed to facilitate the speed of system stability. The next step is to compare the calculated compensated power level with the allowed maximum compensated power level. If the calculated compensated power level is bigger than the maximum compensated power level, then the maximum compensated power level is chosen as the system compensation power.

Otherwise, the calculated compensated power level is still treated as output system compensation power. The total required compensation power consists of two parts; one is to control the Earth Station transmitting power; and another is to control the Satellite transponder gain. The adjusted transmitting power for Earth Station is instantly generated; while the command for Satellite is encoded and then sent to the Satellite via the transmission channel.

Figure 3. 11 Generalized model of rain migration in power control.

3.3.1. Simulation Model

To verify the effectiveness of the proposed adaptive power control scheme, simulations are carried out using MATLAB. Fig. 3.12 shows the simulation model in the form of a block diagram for the proposed scheme. There are five main model components in the simulation system: the Earth Station, the Uplink Channel, Satellite Transponder, Down-Link Channel and Rain Generator.

The Earth Station block receives signal from the satellite. After proper calculation, it generates an adjusted transmit signal and power control command for the satellite.

This calculation process is the major compensation controller inside the Earth Station. It takes a target received signal power as a reference level and computes the current difference between the actual received signal power level and the reference level. This difference is considered as the instantaneous compensation power. However, directly injecting this difference as compensation power into the power control system can easily cause the system to become unstable. Therefore, a properly designed PID controller is added. The output of the PID controller is then taken as the total required compensation power. With proper weights, the total required compensation power is split into two parts; one is to control the Earth Station transmitting power; and another is to control the Satellite Transponder gain. The command for Earth Station is instantly carried out and the adjusted transmitting power is generated; while the command for Satellite is then coded and sent to the Satellite via the transmission channel.

The channel block, both uplink and downlink, are properly modeled to include propagation loss and rain attenuation loss. The round trip delay is split equally into the uplink channel block and the downlink channel block.

According to the power control command, Satellite transponder tunes its transponder gain to amplify the received attenuated signal to be sent back to the Earth Station.

The Rain Generator block generates different real-time rainfall rates to the up/down link channels to simulate rain effects on the satellite links.

Figure 3. 12: Block diagram of the proposed adaptive power control system

3.3.2. PID Controller Parameters

Due to time delays in the loop, the outdated feedback information results in a dynamic behavior. This can lead to oscillations at the response side. A properly tuned PID controller should reach stability in the shortest settling time. A generalized representation for the PID controller can be written as:

$$C(t) = K_p * e(t) + K_i \int_0^t e(t) dt + K_d \frac{de(t)}{dt} \quad (3.10)$$

where $e(t)$ represents the error signals, and K_p , K_i and K_d are proportional gain, integral gain and derivative gain, respectively. The proportional term of the PID controller is responsible for the output that is proportional to the current error. The proportional gain cannot be too high, otherwise the system will become unstable. At the same time, the proportional gain cannot be too low, or the control action will become too small when responding to the system disturbance. The typical function of the integral action is to eliminate offsets of the steady state and to guarantee that

the output agrees with the target value in a steady state. The derivative term is a prediction of future errors, based on the current rate of change. The derivative term is highly sensitive to noise in the error term and may cause the PID controller to go into an unsteady state if the noise and K_d are sufficiently large.

In our power control system, K_d is set to be zero to ensure the stability and K_p is initialized to be a moderate value of 0.5. According to simulations, the proportional gain and the derivative gain contribute little to the speed of convergence.

Furthermore, the intrinsic round trip delay determines that the effect of the power control command will be postponed. For example, the command for the satellite in this case will lag around 125 ms, which is half of the round trip delay. Taking into account this feature, the PID controller is set to work with a 125 ms sampling time. This setting will filter out unnecessary fluctuations before the command takes effect and thus help to improve the settling time for the whole system. A comparison is shown in Fig. 3.13 with different sampling time settings for the PID controller. We assume that there is a sudden onset of a heavy rain (rainfall rate of 96 mm/hr) event at 1000 ms to simulate the step response of the whole loop. As can be concluded, a sampling time of 125 ms will help to shorten the settling time by around 2 round trip delays.

Loop response with different K_i settings is illustrated in Fig. 3.14. Clearly, the Earth Station compensating power first increases sharply when confronted with a convective rain event of 96 mm/hr rainfall rate. With the implemented power compensation approach, the received power level climbs towards the pre-defined target level (of -18 dBm). In addition, it is observed that the time used to reach a steady convergence varies among different integral gains. More specifically, when the integral gain K_i is increased, the response curve moves quickly towards the target received signal level, which implies a shorter convergence time. On the contrary,

there is more oscillation when the integral gain becomes too large. In this case a K_i of 0.003 can properly shorten the settling time without introducing overshoot fluctuations.

Figure 3.13: Different sampling time settings for PID controller

Figure 3.14: Received signal level and compensated power level responding to rainfall rate fluctuations with different K_i coefficients

3.4. Evaluation and Results

In order to further evaluate the proposed scheme, the comparison of the system responses with and without power control implementation is presented in Fig. 3.15. The rainfall rate is designed to increase gradually from 0 to 96 mm/hr, which is the largest rainfall rate observed in our experiment records. The probability of rainfall rate exceeding 96 mm/hr is approximately 0.01% in one year, so 96 mm/hr effectively represents very heavy convective rain. The normal received signal level declines due to the rain attenuation. It is also demonstrated that the received signal level reduces as the rainfall rate continues to increase. Accordingly, the IP packet loss rate simultaneously goes up as a reaction to the decrease in received signal level. On the other hand, the received signal level with PID power control as a countermeasure shows that these effects can be well compensated, regardless of rainfall rate variations. The IP packet loss rate can be reduced to near zero, ensuring high video quality. The comparison demonstrates that the proposed PID power control technique can effectively improve the quality of the video transmission under rain attenuation.

Figure 3. 15: Comparisons of received signal level and IP packet loss responding to rainfall rate fluctuations with and without power control

In addition, the performance of the proposed approach has also been assessed using the full one year rainfall rate collected with the weather station in 2010. In order to alleviate the non-linearity issue, the maximum total compensating power that the Earth Station and the Satellite transponder can provide together is assumed to be 10 dB. Fig. 3.16 shows the CDF of IP packet loss rates for one year with and without the proposed power control. It can be observed that the link reliability has been significantly enhanced. The probability of IP packet loss rates below 1% is increased from 98.97% to around 99.65% with the implementation of the power control technique. To demonstrate this improvement in terms of duration over a whole year, the total amount of time with higher than 1% IP packet loss rate is reduced from 90.23 hours to 30.66 hours with the implementation of the proposed power control method. This means that the proposed power control scheme reduces the amount of video communication with unacceptable quality by a factor of 3. Therefore, it can be concluded that our power control scheme significantly improves the overall performance of the satellite link.

Figure 3. 16: The CDF of IP packet loss rate of 2010 one-year rainfall data with and without power control

The efficiency of the system can be explored on the curve fitting process. The nonlinear curve fitting problem is solved in the least-squares sense. It is equivalent to find the coefficients of x that best fit the equation

$$\min_x \frac{1}{2} \|F(x, xdata) - ydata\|_2^2 = \min_x \sum_i (F(x, xdata_i) - ydata_i)^2 \quad (3.11)$$

where $xdata$ is the input data and output data is $ydata$. It is implemented with the Trust-Region Reflective algorithm. The computational complexity of the Trust-Region Reflective algorithm is $O(n)$ with a single repetition loop. On the other hand, the computation complexity of the proposed power control model is $O(c)$.

3.5. Miscellaneous Consideration

According to the previous simulation and analysis, a total compensation power of 16 dBm is needed in the case of maximum rain (96 mm/hr). There may exist such a scenario that this amount of extra power is not affordable from the base station or satellite transponder. However, this problem can be alleviated by modifying the transmission data rate.

Figure 3. 17: Transmission power versus bit rate

As has been shown in Fig. 3.17, the power of the transmitted signal is decreasing

when the video bit rate increases. Generally, when the bit rate doubles, the transmitted power shrinks half, or decreases 3 dB. This property makes it possible to trade off channel capacity for power level. It means that the compensation for the uplink and downlink power gain should not be too high when heavy rain occurs. Because lowering the bit rate of the video transmission can provide extra power level improvement.

Besides, video transmission requires stringent delay constraints guarantees for user satisfaction. When the delay of a video packet exceeds the corresponding maximum delay, this video packet is dropped. Then the perceived video quality will be influenced. Therefore, it is a challenge to guarantee delay bound for bandwidth-consuming video streaming applications in bandwidth-limited networks.

During each experiment period, the satellite is solely assigned for the usage for the mentioned purpose. No other users exist and the available uplink bandwidth can be fully taken by the abovementioned usage. The end-to-end packet delay can then be considered as

$$D_{E2E} = D_{RTT} + D_{SAT} + D_{TRAN} \quad (3.12)$$

Where the transmission delay D_{TRAN} is the time taken to transmit a single data packet at the data transmission rate:

$$D_{TRAN} = \frac{Packet_Size}{Data_Rate} \quad (3.13)$$

and D_{RTT} is the roundtrip propagation delay of the satellite channel and D_{SAT} is the delay caused by the satellite transponder. D_{SAT} can be further divided into the buffer (if any) queuing time $D_{SAT,QUE}$ and the delay caused by internal processing $D_{SAT,INT}$. In general, the roundtrip propagation delay D_{RTT} dominates the entire delay physically because the satellite operates at the geostationary orbit. As a result, the minimum delay can be considered as D_{RTT} . From the application point of view, the

experiment carried out in this thesis can be categorized as non-interactive voice or video application and its delay requirement is relatively loose compared to the interactive voice or video services.

However, if the system serves more than one user, the time-division duplex protocol can be used. And the delay of the buffer $D_{\text{SAT,BUF}}$ will be taken into account. Different protocols can be used for the delay bound estimation purpose. A typical example is described in [98]. The evaluation of the bounded delay can be achieved by observing the pause frame pattern. Alternatively, the transmission delay D_{TRAN} can be considered with the inclusion of the queueing delays in the IP backbone. As illustrated in [99], the bounded effective bit rate can be estimated. In addition, the system in this thesis can be treated as a packet satellite system with contention-free reservations. The data channel is time slotted with a time unit equal to the transmission time of one packet and two types of slots are designed. One is the transmission time slot for the transmission of packets while the other one is the reserved time slots for the reservation of packets. With a very large number of users, the bounded delay condition can be deduced in a similarly way presented in [100].

Due to the delay bounds, typical data rate bound can be supported by the multi-user satellite network. As a result, the data transmission rate should be adaptive to the specific delay requirements. In [101], a delay guaranteed method is proposed to solve the problem of resource allocation and rate adaptation for maximizing the sum video quality. Resource allocation and rate adaptation adapt the channel resources and the video source rate of each user. The authors of [102] developed an optimal adaptive transmissions scheme to ensure statistical QoS provisioning, in terms of bandwidth and delay bound, for multi-layer video transmissions over wireless channels. A separate queue is maintained for each video layer and the statistical QoS requirement needs to be satisfied by all video layers. This can be also accomplished with the scalable nature of the H264/SVC codec used in this thesis. Variable bit rate stream

can be provided by the codec to fit into the throughput limitations of the whole satellite system.

It is a major concern for the resource allocations to meet a set of QoS requirements. Generally, there are two different policies of resource allocation for multiple users, which are the static resource allocation and the dynamic resource allocation among users. By the static resource allocation scheme, each user is allocated a fixed amount of channel bandwidth. By the dynamic resource allocation scheme, multiple users share the channel bandwidth and the resources are dynamically allocated among users. The dynamic resource allocation can improve the utilization of communication resources.

In our satellite transmission system, the satellite can be regarded as the base station (BS) and multiple subscriber stations (SSs) can exist simultaneously. The BS serves as the interconnection hop for all the SSs and the SSs cannot establish a direct connection with each other. The network will be working in the time division duplex (TDD) mode in which time slots will be assigned to each of the SSs upon their registrations. As a result, the system resources can be scheduled by the BS based on the request from each of the SSs. A simple way to deal with this situation is to allocate a fixed amount of resource including the buffers and channel bandwidth to each SS. However, it may not be efficient because the traffic of different applications may differ among those SSs. For example, each of two SSs may be holding an interactive video meeting. And there is another traffic stream downloading a movie. Consequently, adaptive resource allocation should be performed to meet the need from each SS to the maximum extent. There are some excellent works like [103] and [104] that have presented interesting adaptation protocols for such a purpose. A scheme is developed to guarantee QoS for video streaming in resource scarcity network [105]. This scheme analyses the characteristics of video packets and prioritize the video packets that are more crucial to decode the video frame sequence.

Then the video packets with priority will be allocated separate network resources. Variations of these algorithms may be adopted for the system resources allocation in our system. However, this is currently not of the major focus in this work and we will work on them in the future.

Chapter 4

Preventing Satellite Network from Disassociation DoS Attacks

We present our proposal of protecting satellite network system from disassociation DoS attacks in this chapter. We firstly introduce satellite network system architecture and some necessary background of DoS attacks. Then we give a brief introduction of Rabin function using in our solution. Based on that, we propose our scheme that takes advantage of Rabin function for securing the sequence number of message. Lastly, we provide primary results to validate the applicability of our method.

4.1. Satellite Network Model

Standard digital video broadcasting-interaction channel for satellite distribution systems (DVB-ICS DS) [106] provides an overall satellite system model architecture as shown in Fig. 4.1. Generally, a typical satellite network system consists of a NCC and a number of RCSTs.

- NCC: a NCC is mainly in charge of the monitoring and controlling duties. It manages the authentication, connection and association of authorized users

by appropriate generating control signals in the satellite multicast interactive network.

- RCST: RCSTs can transmit data through a return channel via satellite. RCSTs send their resource connection requests to the NCC. These messages are transmitted via satellite by using data transfer protocols.

Figure 4. 1: Satellite network system model.

In a satellite network system scenario, each RCST and NCC is appointed with a unique media access control (MAC) address. And the pre-computed session key is a shared secret between the NCC and the RCST. According to the public-key protocol, even though the attacker can intercept the messages, he is not able to derive the session key value. In addition, the NCC divides the time into fixed intervals T_i . In each interval period, the NCC dependably sends a different nonce N_i for the purpose of replay detection. When a RCST logs on the satellite network, it will perform an initial negotiation handshake with the NCC to establish authentication

and the security mechanism policy, in particular the cryptographic algorithms and key sizes to be used subsequently. Once the negotiation step has completed, the NCC will proceed with the next key exchange step. Explicit key exchange (EKE) protocol is employed to achieve mutual key exchange.

The RCST responds to each EKE request message with an EKE response message, the NCC can authenticate the terminal based on response message. Only after successful authentication, the NCC and RCST are able to decrypt the payload stream data. Otherwise, the fake RCST cannot recover and access the encrypted payload stream data.

If some RCSTs want to disassociate with the NCC or some new terminals want to associate with the NCC, then NCC need to update the session keys used in the satellite network. To assign a new key, the NCC will send EKE request message to each RCST. The RCST will then extract the secret session key from the received EKE request message and respond with a proper EKE response message. However, this process is usually subjected to malicious attacks, especially, the DoS attack.

4.2. Disassociation DoS Attacks

In this thesis, the disassociation DoS attack to satellite system is our major threat concern. The Fig. 4.2 depicts a disassociation DoS attack operation diagram. The NCC and RCST has established connectivity. When the NCC and RCST communicate with each other, the communication traffic flows generate and aggregate. But adversaries who are listening to the traffic flows can gain access to the data messages. The attackers can exploit these intercepted messages to produce a bogus disassociation request message. This disassociation request message may either be sent from the RCST to the NCC or from the NCC to the RCST. When the NCC receives a disassociation request from the RCST, it will abort its

communication with this RCST and delete all the stored information relevant to the RCST from its memory. If an attacker sends a spurious disassociation request to the NCC, the NCC will mistakenly cease its connection with the victim RCST. If the victim RCST demands to obtain an access to the service, it needs to undergo the authentication process once again. The additional authentication process not only involves the cancellation of existing regular data communication, but requires more time and efforts to re-establish the verification as well. In consequence, the fake disassociation DoS request has successfully consumed the system resources and also disrupted the authorized users' communication with the satellite system.

Figure 4. 2: A disassociation DoS attack.

4.3. Rabin Function

The basic idea of our proposed scheme is to employ the Rabin function [107] over the sequence number instead of a plain sequence number. The Rabin function is a trapdoor one-way function as depicted in Fig. 4.3. Because of its one way characteristic, like if when $y = R(x)$, the value of x cannot be determined if only given the value of y .

For the encryption, let $p = \{0, \dots, n-1\}$ be the plain text. The encrypted text c is then given in (4.1) by

$$c = m^2 \bmod n \quad (4.1)$$

Where $n = p \cdot q$, p and q are prime numbers. For simplified computation of square roots modulo, p and q are usually chosen as $p \equiv q \equiv 3 \bmod 4$.

For the decryption, the p and q are needed in order to get the value of m_p and m_q in (4.2).

$$\begin{cases} m_p = \sqrt{c} \bmod p \\ m_q = \sqrt{c} \bmod q \end{cases} \quad (4.2)$$

By applying the extended Euclidean algorithm, y_p and y_q , with $y_p \cdot p + y_q \cdot q = 1$, the values of y_p and y_q can be obtained. Next, by the invocation of the Chinese remainder theorem, the four square roots: $+r$, $-r$, $+s$ and $-s$ can be obtained in the set $\{0, \dots, n-1\}$.

$$\begin{cases} r = (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n \\ -r = n - r \\ s = (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n \\ -s = n - s \end{cases} \quad (4.3)$$

Lastly, with one of these square roots mod n , the original plain text value, m , can be derived.

Based on the feature of Rabin function, a lightweight method for verifying the incoming packet by executing protection over its sequence number is developed.

Figure 4. 3: Rabin function over sequence number.

4.4. Prevent DoS Attacks to Satellite System

Every message sent by a RCST has a unique sequence number [108]. The sequence number is used to detect whether there are any packet loss in the communication process. The sequence number of message is usually linearly distributed as $m_{i+1} = m_i + 1$. However, if an attacker observes the sequence number, he can easily figure out the next packet's sequence number by easily adding one to the current sequence number value. Besides, the attacker can deceive the source's MAC address by using available tools such as Spoof-MAC [109], MAC Changer [110], and Aircsnarf [111]. Then the malicious attacker is able to send a bogus disassociation request to the NCC. As a result, the NCC may terminate its service with the victim RCST and the victim RCST is forced to disconnect with the NCC. Furthermore, if the MAC address of the NCC is deceived by some malicious attackers, then the attackers can dispatch forged disassociation requests to every RCST in the system. As a consequence, normal communications of the whole satellite multicast network system will be suspended and suffer destructive disassociation DoS attacks.

Since the first verification step is to check the sequence number of the received message [70], security and reliability of the sequence number issue needs to be enhanced to accelerate the disassociation DoS attacks detection. If a disassociation DoS attack can be discovered at the first step by simply examining the sequence number of the received message, then the cost of computational resources can be greatly cut down by avoiding the subsequent steps of MAC value and payload verifications.

During the process of each RCST connection, the RCST will make handshakes with the NCC for authentication and session key generation based on DVB-RCS standard security specification as shown in Fig. 4.4. The RCST side initially sends its requests to log on. This log-on message contains the RCST's MAC address. After receiving the request from RCST, the NCC side will respond to RCST with a sign-on request message authentication code (MAC) message to negotiate of cryptographic algorithms and parameters. The function of MAC message is to provide both the authenticity of a message and its integrity. The sign-on MAC message structure includes public key algorithm choice, hash algorithm choice, encryption algorithm choice and nonce size choice. Upon receiving the request, the RCST will send a sign-on response MAC message to agree on security algorithms and parameters. After successful authentication, the NCC will proceed to send the main key exchange (MKE)/quick key exchange (QKE)/EKE key exchange request messages to RCST for delivering a pre-determined secret session key, integer k and prime numbers p and q . MKE uses the Diffie-Hellman algorithm to protect the secret key. QKE uses the cookie to derive the session key and EKE uses AES to encrypt the session key. For example, if the values of p , q and k are transmitted by the EKE MAC message, then the p , q and k can be protected by the counter (CTR) mode of the AES cipher algorithm according to DVB-RCS standard. At last, the RCST extracts session key, integer k and prime numbers p and q . And it reply with MKE/QKE/EKE key

exchange response messages to complete the shared session key establishment.

Figure 4. 4: RCST log-on authentication process with NCC.

The primary verification process of a received message is demonstrated in Fig. 4.5. At first, after receiving the secret value p , q and k from NCC, the RCST transmits a message with the encrypted sequence number by using Rabin function. The two secret prime numbers, p and q , are employed to perform encryption to sequence number by Rabin function. And the value of two prime numbers p and q is related to the value of k . With p fixed, if the current sequence number is odd, q would be the k -th prime number after the original q ; whereas, when the current sequence number is even, the q value would not be changed. We assume that NCC and RCST mutually understand the effect of value k . The process involves multiple modulus n for the Rabin cryptosystem. And thus the computational cost for the eavesdropper will dramatically increase. Once the message from the RCST is received, the NCC will decrypt the sequence number based on its p and q values. Due to the characteristics of the Rabin function, there are four candidates of plain sequence number m . Therefore, the NCC needs to look up its sequence number table to find the exact

sequence number. If the decrypted sequence number matches the nonce N_i , then the NCC would continue to compute the value $MAC(K_{ST_i}Seq | h(M))$ using the shared key K_{ST_i} that can be computed by K_{NCC} . Then, the NCC further verifies the value of the payload to make sure that it is identical to the value retrieved from the received message. All above procedures have to be verified before the received message is accepted. Otherwise, the NCC will discard the received message.

Figure 4. 5: Verification process of a received message.

Our scheme is aimed to enhance the security protection of the sequence number of message. It is achieved by encrypting the sequence number with the Rabin function. By use of one-way Rabin function to protect the sequence number, even if the attacker is able to obtain the current sequence number, he cannot work out the next exact sequence number.

4.5. Modeling and Verification

CPN has been adopted as the principal modeling tool for analyzing and verifying our scheme. CPN is a graphically-oriented modelling language combining with the functional programming language standard meta-language (ML). CPN is capable of offering design, specification, simulation and verification of systems. CPN tools have been widely adopted in the academic area. It fully supports the expression of a long range of interactions. Besides, CPN has an intuitive graphical representation and relatively simple implementation, which is suitable for establishing model of concurrency [112]. Thus, CPN is well known for their graphical and analytical capabilities for the specification and verification of different systems. Furthermore, CPN, which is a comprehensive tool for editing, simulating and analyzing, can offer simulations of information flows dynamically and construct graphs automatically. CPN tools have strong explicit definition for both its syntax and semantics, which ensures a solid specification of the model generation, checking and simulation [113]. CPN are convenient for methodology of modular security representation and verification because of the features of CPN including its graphical nature, the simplicity of the model and the firm mathematical foundation. Therefore, CPN can provide a formal security analysis of our proposed security solution.

Two models are designed based on CPN tools to verify our solution against disassociation DoS attack. In order to better evaluate our proposed scheme, we compare two different situations where the system suffer disassociation DoS attacks with proposed solution and without in our CPN model.

In a CPN model, data is represented by tokens. And each token belongs to a special data type called the color set of a token. Generally, the color set can be variable, constant or function. If the color set is a new one, then it has to be declared firstly before use. The token color is the actual assignment of value to this token.

To model the messages, two color sets SN and DIS are declared to be the sets of integers. Color set SN is declared for representing the sequence number of the transmission message. And color set DIS is defined for modeling the state of sending dissociation requests.

For the sake of intuitive demonstration importance of protection on sequence number, we simplify the packet structure. In our CPN model, the packet consists of two parts, in particular, the disassociation request state and sequence number. When NCC receives a packet from RCST, first step is to check *dis* value with *stateyes* which is a constant defined as one. In this designed model, if the value of variable *dis* is zero, it indicates that the packet contains a disassociation request. In this situation, NCC will accept its request and terminate communication with RCST. But if NCC hasn't received RCST's request for disassociation, NCC will continue to check the sequence number of received packet with its next sequence number list. If sequence number matches the one in NCC's *NextSn* list, then NCC side will consider the terminal as an authorized user. The model of communication between the NCC and RCST without attacks is like aforementioned description. The models with disassociation DoS attacks and our scheme will then be presented as follows.

1) Model of the disassociation DoS attacks

When an attacker wants to interrupt the connection between authorized user and NCC side, the attacker will keep eavesdropping on the traffic. In the scenario, the attacker may figure out the sequence number of current message sent from the RCST to NCC. Since normal sequence number is linearly increased, it is so effortless for the attacker to create bogus sequence number simply by adding one to current value of sequence number. In consequence, the attacker would generate a fake dissociation request with its cracked sequence number. In order to demonstrate the necessity of protection on sequence number, we assume that attacker can successfully pass verifications of its MAC address and payload during subsequent authentication

steps. In this sense, if the attacker is able to obtain correct sequence number, he can launch a disassociation DoS attacks which breaks the connection between the NCC and the legitimate terminals.

In addition, the process of disassociation DoS attacks is developed in CPN as depicted in Fig. 4.6. In this model, the RCST side is sending packets to the NCC side. In the meanwhile, the attacker also sniffs on the communication traffic and launches flooding disassociation DoS attacks to the NCC side. When the malicious intruder makes *dis* to zero and transmits it to the NCC with exact next sequence number, the NCC will believe it as the disassociation request from authorized clients. As a result, the RCST side is compelled to lose communication with the NCC side due to the intentional interruption by the DoS attackers.

Figure 4. 6: CPN model of communications with disassociation DoS attacks.

2) Prevent disassociation DoS attacks scheme

As aforementioned introduction of our proposed scheme, the CPN model is employed to examine our method. Except the normal transmission model, we further

develop the encryption model, attacker side model, MAC check model and the decryption model in CPN. Thus, the whole communication process in which the DoS attacker breaks the communication and our proposed scheme detects the attacker will be demonstrated in our simulation CPN model.

The sequence number encryption model is depicted in Fig. 4.7. The communication message is represented as product of three color sets of *SN*, *DIS* and *MAC*. Initially, the RCST sends message to the transition *GenratESN*. Upon receiving the message, the transition *GenratESN* employs Rabin function to encrypt the sequence number of received message.

Figure 4. 7: Encryption to Sequence Number with Rabin function Model.

The attacker listens on the traffic model is the same as aforementioned model in Fig. 4.6. In order to detect the attacker, MAC address check model is developed as shown in Fig. 4.8. Thus, the NCC side will take the first step to examine the MAC address of every received message before decryption stage. Besides, if the sequence number of received packet is not the same as the one stored in NCC's list, then the NCC will systematically consider it as a malicious intruder and store its MAC address to its *BlackMac* place. If the attacker intends to launch bogus disassociation requests next time, it will be detected immediately by the MAC check procedure in our method. Hence, the proposed approach can effectively detect and prevent the disassociation

DoS attack.

Figure 4. 8: The MAC Check Model.

At the final stage, after the MAC address verification, the place NCC will continue to perform decryption part model as shown in Fig. 4.9. Due to decryption algorithms of Rabin function, there are four candidates of the decrypted sequence number. The function of *SelectSN* transition is to compare the decrypted sequence numbers with *NextSn* stored in NCC's list place. If one of four decrypted sequence numbers exactly matches *NextSn* value, then the NCC will update its *NextSn* place and send an *ACK* to the RCST side. On the other hand, if none of decrypted sequence numbers corresponds to *NextSn*, then the NCC will regard current sender as an attacker and save its MAC address on the *BlackMac* place to prevent it from generating fake request next time.

Figure 4. 9: The decryption of sequence number at NCC model.

4.6. Analysis of Proposed Solution

The proposed scheme not only successfully prevents disassociation DoS attacks but enhances the efficiency of the disassociation DoS attacks detection as well. Normally, the intruder obtains messages from the RCST and generates a fake disassociation message using a linearly increased sequence number. According to our proposed method, the sequence number is protected by the Rabin function. Thus, the NCC is capable of easily distinguishing regular packets from the fake packets. In this sense, the NCC avoids examining its MAC and payload values, which greatly reduces the computational cost.

1) Consecutive Sequence Number Prediction

For the sake of the probability of successful disassociation DoS attack estimate, a simulation has been implemented by using MATLAB. It is assumed that an attacker completely eavesdrops a message transmitted from the RCST to the NCC, including the sequence number, the RCST's MAC address and other confidential information. The malicious intruder pretends to be RCST to send a fake disassociation request message to the NCC using the bogus sequence number. According to the proposed method, the accomplishment of such a disassociation DoS attack firstly depends on the successful sequence number verification.

According to the algorithm, a successful attack will occur if and only if there exist two consecutive encrypted sequence numbers by the Rabin function corresponding to the two normal consecutive plain sequence numbers (consecutive sequence number prediction). In our simulation, the prime number values used in the Rabin function is set as $p = 7$, $q = 11$ and the size of the plain text of the sequence number varies from 100 to 40960. Note that these p and q set are used for simple simulation purpose to reveal the relation between the insecure probability and the size of plaintext space. In this scenario, the probability of a successful disassociation DoS attack is demonstrated in Fig. 4.10. In this figure, it can be seen that the probability of a successful attack approaches a limit of 0.9% along with the increase in size of the sequence number, which indicates that the risk of proposed method is not high and can be controlled.

Figure 4. 10: Probability of successful attacks.

In addition, according to the Rabin function, the products of the two prime numbers can affect the performance of the proposed scheme. Thus, another simulation has been conducted to investigate the influence of the product of two prime numbers. The simulation results are demonstrated in Fig. 4.11. It can be clearly observed that the probability of a successful disassociation DoS attack tends to reach zero with the increase of the two prime numbers' product. Therefore, it can be concluded that the larger the product of the two prime numbers, the lower the probability of a successful DoS attack. This observation also indicates that the performance of the proposed scheme can be improved by increasing the product of the two prime numbers p and q used in the Rabin function. At last, all the simulation results demonstrate that the proposed scheme can achieve a great performance for the detection and prevention of disassociation DoS attacks to the satellite system.

It is also noted that the computational complexity of factorizing a number smaller than 10000 is relatively easy. However, the trend shown in Fig. 11 is still valid for a consecutive sequence number prediction attack. With a proper algorithm to mapping the original sequence number to a larger value, exponential extension, for example, can help to alleviate this problem. And thus a large modular can be used for the

encryption. This scheme can be simple, such as adding and certain large number to all the sequence numbers. This works as shifting all the sequence number with a fixed amount into the larger integer region. Other mapping scheme like product each of the sequence number with a large integer may also work. And this algorithm will be discussed in the future work.

Figure 4. 11: Probability of successful attack vs. products.

2) Factorization for Rabin Modulus

Another method to break the Rabin cryptosystem is to find out the solution of

$$x^2 = y \pmod{N} \quad (4.4)$$

This is equivalent to compute the square roots modulo N , and it has been proven that it is equivalent to a factorization problem. The typical factoring process for N is $O(\log(N))$ iterations and thus the overall reduction is polynomial-time.

However, the previous analysis is based on the situation where the intruders cannot obtain the values of p and q to decrypt the encrypted plain sequence number m by Rabin function. But if the intruder is able to figure out the values of p and q , then the intruder would be able to decrypt the ciphered sequence number C and

get the plain sequence number m . However, even if the intruder can gather all the above important data, due to the feature of the Rabin function, the decrypted sequence numbers unfortunately have four candidate values. Thus, the chance for the intruder to obtain the right candidate value is still low without the look-up table stored in the NCC. At the NCC side, the irrelevant decrypted sequence numbers can be excluded by comparing them with the latest received sequence number stored its sequence number list. For instance, if there are four decrypted sequence numbers according to the Rabin function, the NCC can select the one which is slightly greater than the latest received sequence number. In this way, the probability of the attacker obtaining the correct sequence number and launching a malicious attack to the satellite system will be greatly decreased. Therefore, the proposed scheme can effectively detect and prevent the disassociation DoS attacks.

Chapter 5

Bitstream-oriented Protection for the H.264/Scalable Video Coding

5.1. An Overview of H.264/SVC

The SVC is proposed as a scalable extension of H.264/AVC, which indicates the rest of bitstream can be still decodable even if some parts of the bitstream are removed. H.264/SVC supports three types of scalabilities: temporal, spatial and quality scalability. Temporal scalability refers to the capability to provide video bitstream with different frame rates by extracting the bitstream subsets. Temporal scalability with different temporal enhancement layers can be achieved by the concept of hierarchical B-pictures. A typical hierarchical prediction structure with a GOP size of eight and four temporal layers is demonstrated in Fig. 5.1. The T_0 to T_3 identify the corresponding temporal layer. A GOP in H.264/SVC is composed of a key picture and all pictures located between the key picture and the previous key picture. In a GOP, frames of higher temporal layers can only be predicted from frames of lower temporal layers. In spatial scalability, inter-layer prediction is utilized to provide resolution variety as shown in Fig. 5.2. The base layer is identified as D_0 and D_1 represents the first enhancement layer in spatial scalability. A frame from

D_1 spatial layer can be not only predicted from other frames at the same spatial layer, but the frames from lower spatial layers D_0 as well. Quality scalability in H.264/SVC is to produce videos with different quality levels. There are two different quality modes of SVC, namely CGS, and MGS respectively. The CGS can be considered as a special case of spatial scalability with the same resolution but different quantization parameters to layers. In MGS, prediction structure is more flexible where both base and enhancement layers can be referenced. Key picture concept is applied in MGS to solve the problem of drifting effect between the encoder and the decoder.

Figure 5. 1: Hierarchical prediction structure with a GOP size of eight

Figure 5. 2: Spatial scalability structure with two spatial layers

Similar to H.264/AVC, the SVC bitstream consists of a sequence of NAL units. The NAL unit is defined as the smallest unit in the SVC bitstream. As shown in Fig. 5.3, the NAL unit is composed of the NAL header and raw byte sequence payload (RBSP). The header of NAL unit specifies the type and scalability information of NAL unit. The RBSP represents integer number of bytes of data. There are two types of NAL unit, namely the VCL NAL unit and non-VCL NAL unit. The VCL unit represents the content of the video data, while non-VCL NAL unit is responsible for providing sequence parameter information for decoding and displaying video data. Although SVC and AVC both are composed of NAL units, the structure of NAL unit is not the same. The header of AVC NAL unit is only one byte, whereas the header of SVC NAL unit has an additional three bytes of data associated to scalability information of NAL unit. As the scalability characteristic of SVC bitstream, sub-bitstream with specific temporal, spatial or quality requirement can be extracted at NAL unit level with reference to its header information.

Figure 5. 3: NAL unit structure in SVC bitstream

5.2. The AES Encryption Algorithm

The AES algorithm, based on Rijndael algorithm, is a symmetric block cipher adopted by the national institute of standards and technology (NIST) in 2001 [114].

The basic structure of 128-bit AES consists of an input block with the size of 128 bits, a secret user key of 128 bits and a 128-bit ciphered output. The number of AES cipher rounds depends on the size of the key. There are three supportable key lengths: 128-bit, 192-bit and 256-bit, whose iteration rounds N is 10, 12 and 14 respectively. The AES algorithm mainly employs four operations: *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey*. The AES encryption process is shown in Fig. 5.4. At first round, the input block data merely undergoes the *AddRoundKey* which is a simple XOR operation between the input matrix and the key of the current round. The *RoundKey* is derived from the expansion of secret user key by attaching recursively four bytes to the user key. From the second to the last but one round, the data will be through all four operations. *SubBytes* is a non-linear byte substitution and each byte is replaced with the Rijindael S-box. *ShiftRows* is a linear operation where each row of the matrix is shifted cyclically a certain number of steps. *MixColumns* is a linear operation where each column of the matrix is multiplied by the known matrix for the key. In the final round, *SubBytes*, *ShiftRows* and *AddRoundKey* (except *MixColumns*) will be performed to encrypt the data block. Similarly, the AES decryption algorithm implements the inverse of all aforementioned transformations in reverse order.

Figure 5. 4: AES encryption algorithm flow chart

5.3. Bitstream-oriented Protection Scheme

5.3.1. Design Principle

Based on the characteristic of SVC mentioned above, several considerations need to be taken into account. Firstly, the main feature of SVC is its capability of supporting bitstream extractions in application. So preserving functionality after encryption should be satisfied, e.g. bitstream of encrypted SVC file should be scalable as well. Since bitstream extraction is performed in NAL unit level, the bitstream oriented encryption employed after compression is preferred. Besides, non-VCL NAL units that carry video parameter data can assist particular bitstream operations, these parameter NAL units will be left unencrypted. Secondly, due to the scalable access manner of SVC, all layers of bitstream are needed to be protected in case of leakage of content. Thirdly, low computational cost of encryption algorithm is suggested. This requirement is to avoid extra burden of complexity in considerations of complex

encoding and decoding process of SVC. Lastly, the encrypted bitstream is compliant with the standard decoder, which means the standard SVC decoder is able to decode the encrypted bitstream without decryption.

According to the requirements described above, the proposed H.264/SVC bitstream protection scheme works as shown in Fig. 5.5. Firstly, SVC bitstream is obtained by the JSVM encoder. Then NAL units are extracted from the encoded bitstream. Since the base layer is the basis of enhancement layers in SVC bitstream, more security concerns should be given to the base layer than enhancement layers. The NAL units of base layer are distinguished from others of enhancement layers by verifying *dependency_id*, *temporal_id* and *quality_id* in each NAL unit header. However, according to the SVC standard, pictures data encoded in base layer can be further divided into I picture data and P picture data. As has been investigated in [115], I picture data plays a dominant role in reconstructing the original video from the bitstream. Therefore, the NAL units from base layer continue to be parsed by examining their *slice_type*. The NAL units containing I picture information from the base layer should be encrypted by advanced encryption scheme and the NAL units carrying P picture data from the base layers should be performed light-weighted XOR operations in the proposed method. In this way, the confidentiality of video can be achieved and the computational cost is correspondingly reduced by limiting AES to selected partitions of base layers. The NAL units from the enhancement layers would be performed light-weighted XOR operations. At last, all encrypted NAL units' types are reassigned with an unspecified NAL unit type. In this way, the confidentiality of video can be achieved and the computational cost is correspondingly reduced by limiting AES to selected partitions of base layers.

Figure 5. 5: Proposed SVC bitstream protection method

In order to better comprehend our proposed method, we elaborate the four main works in the following section. We first present our scheme for I slice protection, and then introduce lightly encryption on P slice and enhancement layers. Furthermore, we demonstrate our implementations to make our scheme in format compliancy manner. Lastly, we devise a key management mechanism for our SVC protection method.

5.3.2. Slice Weighted Protection Scheme

5.3.2.1. I Slice Protection with AES

For the I slice encryption, the AES is chosen as our cipher. AES is a block cipher, it splits the plain text into blocks to execute encryption. And CBC mode is applied to assist AES block encryption in our proposed scheme, which uses the results of the last block encryption to encrypt the next block [116]. It is noted that the header of VCL NAL units indicates the type of its payload data and presents the layer identification. Header information of NAL units is necessary for decoding and extraction process. Therefore, the NAL unit headers are not encrypted and only the

payloads are encrypted. In Fig. 5.6, it can be seen that plaintext P is partitioned into small blocks as $P_1, P_2, \dots, P_m$. The first plain text block P_1 is XORed with the IV to generate the correspondent cipher block C_1 . For the following plain text blocks, the i th cipher block is determined by the i th plain block and the previous $(i-1)$ th cipher block. Then two identical blocks of plaintext never encrypt to the same ciphertext. Therefore, the security is strengthened as the current encrypted block depends on the previous ciphered one.

Figure 5. 6: The CBC modes operations

To maintain security, a unique IV must be used for each NAL unit. Otherwise, the same plain text might be encrypted to the same cipher text, and then it would leak information to the adversary. In our proposed encryption algorithm, each NAL unit containing I picture data is assigned with an unpredictable IV. The IV generation example is shown in Fig. 5.7. Since the header of each NAL unit is unencrypted, the 128-bit IV is constructed from the payload of NAL unit as a 4×4 array of bytes. In order to guarantee the uniqueness of IV, a counter is needed as it increments every time. However, if a counter is directly used in the IV, it is easy for the attacker to find this sequential manner. So we suggest to XOR the extracted 128-bit block with a counter block whose first column is the counter and the rest are zeros. The purpose

of setting the counter in one column is to enhance the difficulty for attacker to solve the value of IV. In this way, the uniqueness and unpredictability of IV is guaranteed.

Figure 5. 7: The IV generation process

5.3.2.2. B and P Slices Protection with CBC-Mode XOR

In H.264/SVC, the base layer is independently decoded and enhancement layers depend on the base layer to improve the video quality. Similarly inside base layer, I slice can be decoded without the reference to other slices by use of intra-picture coding, but P slice depends on I slice or other P slices to be decoded. Therefore, the NAL units from enhancement layers and containing P slices are less significant contents with comparison to I slice NAL units. Considering the security and computational cost, those NAL units will be protected by a light-weighted XOR algorithm. For the enhancement layers and P slices, the NAL units' headers are in the same way left unencrypted and the payloads are under XOR operations. The payload of NAL units are divided into separate blocks. Similarly to the AES encryption described in Fig. 5.6, the XOR algorithm is also performed in CBC mode. Except that the IV is replaced with a pre-assigned secret key IV_{xor} and the encryption key is another pre-assigned secret key Key_{xor} . The purpose is to defend against known-plaintext attack.

5.3.3. Format Compliance

Format compliance indicates that the encrypted bitstream should be compliant with the compression coder. Any standard decoder should be able to decode the encrypted bitstream without decryption. In [80], it is still considered as format compliant if a decoder ignores the encrypted NAL units data by signaling the NAL units to unspecified types. So we develop the transparent encryption based on this idea, but strengthen security on NAL units type reassignments, rather than one to one mapping in [80].

Table 5.1 shows the selected NAL units type categories. The NAL units with their types equal to 1, 5 or 20 are VCL NAL units. The NAL units type equal to the range of 16 to 18 are determined as reserved data. And NAL units having their types equal to 0, in the range of 24 to 31 are defined as unspecified data. According to the SVC standard declaration, the unspecified NAL units are used as determined by the application. And the standard decoder will ignore these unspecified NAL units without affecting the decoding process.

Table 5. 1: Selected NAL unit type

NUT	Description	SVC Class
0	Unspecified	Non-VCL
1	Non-IDR slice	VCL
5	IDR slice	VCL
6	SEI	Non-VCL
12	Filler data	Non-VCL
14	Prefix NAL	Variable
16...18	Reserved	Non-VCL
20	SVC slice	VCL
21...23	Reserved	Non-VCL
24...31	Unspecified	Non-VCL

The mapping table from encrypted NALU to unspecified NALU can be further protected with the base layer key which is shared by all authorized users. There are 4 types of NALU need to be operated, namely 1, 5, 14 and 20. Totally 9 types of unspecified NALU can be used for rearrangements, which means the mapping table can be of 3024 variants. One of the 3024 mapping tables can be selected by extracting the first 2 bytes of Key_{map} by following equation

$$Key_{map} = IV_{xor} \oplus Key_{xor} \quad (5.1)$$

$$Map_Table_ID = dec(K_0(0:15)) \bmod 3024 \quad (5.2)$$

In this way, NAL units type reassignments can be protected by increasing the diversity of mapping manners. And only the users with privilege are aware of the mapping table and thus the original NAL units types.

5.4. Key Management

The asymmetric RSA algorithm is employed to distribute the secret symmetric keys used in AES and CBC-mode XOR encryption: K_i , IV_{xor} and Key_{xor} . In order to improve the overall security, an additional private key ADD is generated and distributed to clients.

In our case, an N-layer SVC bitstream would need N encryption keys, namely K_0 to K_N . However, due to the scalability of SVC bitstream, the user at layer L_i with K_i is not able to enjoy the whole quality of video sequence unless he gets all the higher layers' secret keys from K_{i+1} to K_N . For the highest level users, they have access to all the layers of SVC bitstream. If each layer is assigned with a different key, then the highest level users would need a database to store all the keys. It would be uneconomical to store all the keys, in particular, there are a number of enhancement layers. So a cryptographic hash function based key distribution is used to mitigate the storage of the key and maintain the security.

Firstly, K_N is generated with initial salt by following equation

$$K_N = H(salt) \quad (5.3)$$

Where $H()$ is denoted as a cryptographic hash function. And salt is a random string generated by pseudo-random pattern generator (PSNG). The salt will be changing during each time session, which usually lasts 12 hours. The rest keys for lower level layers are then derived from the following equation

$$K_{i-1} = H(K_i, ADD, KeyID_{i-1}) \quad (5.4)$$

Here, we denote the $KeyID_n$ as the summation of the *temporal_id*, *dependency_id* and *quality_id*. Furthermore, *ADD* denotes the aforementioned additional private key protected by RSA.

When a user at the i ($KeyID_i = i$) layer request to obtain the K_i from the server, K_i and protected *ADD* is sent to him after his privilege is authenticated.

The asymmetric RSA algorithm is employed to distribute the secret information *ADD*. Firstly, the server obtains the recipient's public key (n, e) and computes the ciphertext by using the public key.

$$c = m^e \bmod n \quad (5.5)$$

At the receiving end, the plaintext is recovered by using receiver's own private key (n, d).

$$m = c^d \bmod n \quad (5.6)$$

Here in our case, the secret *ADD* is equal to plaintext m to be encrypted by RSA algorithm. After owning the secret K_i and *ADD*, the user can derive the rest keys by using (5.4).

To increase security, repetitions can be applied to (5.4) to derive the K_i . If the length of derived key $kLen$ is less than the hash function output length $hLen$, the first $kLen$ bytes of hash function output are taken as derived key. Instead of store all the lower layers' keys, we can independently derive predecessors' keys by use of current layer'

key. In addition, K_{i-1} is determined by the K_i , ADD and $KeyID_{i-1}$ by using the hash function. Due to the one-way characteristic of hash function, the users at higher level can obtain the keys of lower levels. But the keys with lower $KeyID$ cannot derive the key implemented at higher layers. This feature is in accordance with the SVC applications where the paid user can get the full quality of the video and unpaid users cannot see the high quality of the video.

5.5. Performance Evaluation

In this section, we will discuss and evaluate the performance of our proposed scheme in terms of functionality, scalability, computational cost and comparative analysis with existing approaches.

5.5.1. Preserved Functionality

5.5.1.1. Format Compliance

In our scheme, the NAL unit types of ciphered bitstream are appointed to new unspecified labels. But the altered bitstream satisfies the syntax and semantics' requirements of the H.264/SVC standard. And the H.264/SVC standard decoder can decode the encrypted bitstream successfully without any coder disobedience, which is in accordance with the definition of format compliance. So the protected bitstream can be denoted as format compliant.

5.5.1.2. Scalability

The proposed encryption algorithm is performed directly to NAL units, so it won't violate bitstream extraction applications. In addition, all the encryption operations are applied to the NAL unit payload, both the structure of NAL unit and header of NAL unit are preserved. Since the scalability information is contained in the NAL

unit headers, scalability is still kept in the ciphered bitstream. Therefore, the presented scheme preserves the scalability function of encrypted SVC bitstream.

5.5.2. Security Analysis

To evaluate the feasibility of our proposed protection method, security of bitstream encryption and key management will be discussed. Moreover, two attack models are applied to test the strength of the protection scheme and key management.

The bitstream are under sufficient protection by our proposed scheme. Firstly, due to the scalability feature of SVC bitstream, all the layers of SVC video data are under protection. Not only is the base layer implemented with encryption, but also the enhancement layers. Secondly, we pay more attention to protect the most significant I picture video content by using AES-CBC algorithm. AES in itself is safe against any brute force attacks and has never been cracked yet. It would take 149 trillion years to crack the 128-bit AES using a brute force attack at 255 keys per second [85]. As to AES-CBC, the key factor to ensure the robustness of encryption algorithm is the uniqueness of IV. In our proposed work, the IV is XORed with a counter to guarantee its uniqueness. Hence, the ciphered I picture data are infeasible for attacker to break. Without being decrypted I picture data, the video is still unintelligible to unauthorized users, even P picture and enhancement layers data successfully broken. Thirdly, unspecified NAL unit type reassignments are implemented by our aforementioned table mapping. This operation is to further improve the security of encrypted NAL units.

Furthermore, the proposed key management mechanism increases the strength of bitstream protection method. The critical key generation process is protected by one-way hash function. And lower layer's key is determined by the higher layer's key,

ADD and $KeyID_{i-1}$ by using the hash function. Due to the one-way characteristic of hash function, the users at lower layer are not able to recover the key implemented at higher layers. Moreover, RSA is employed to distribute the secret information ADD as mentioned above, because RSA algorithm can provide enough security with large key like 2048 bits.

The robustness of the aforementioned key management and protection scheme against various security attacks are evaluated by the following tests.

1) Brute-Force attacks

The brute-force attack is aimed to enumerate all possible keys until the correct key is found. Since the key length of AES is 128 bits, this means the attackers' trying-space is as large as 2^{128} . It is too large for attackers to break our cryptographic key. Assuming the attacker can identify whether the decrypted results are the correct plaintext, attackers are on average required to decrypt half of the total number of possible keys as 2^{n-1} . However, the assumption that the attackers can judge the correctness of tried key is false. This is because the encrypted information is part of a specific NAL unit and the decrypted results cannot be verified because the verification would need a more sophisticated decoding process. Furthermore, the salt to generate K_N will be renewed after every 12 hours, so the keys will be changed too. It is more difficult for attacker to find the correct key within 12 hours. So our proposed scheme can be considered resistant to brute-force attacks.

2) Known-Plaintext attacks

In this attack model, both plaintext and its corresponding ciphertext are known to the attacker for key recovery. The AES will be invulnerable to known-plaintext attacks, because the cipher and its inverse process with different components can effectively eliminate the chances of weak and semi-weak keys. Furthermore, the non-linearity of the key expansion procedure also helps to reduce the possibility of equivalent

keys. As a matter of fact, a slight change in the plaintext will result in a large amount of difference for the ciphertext. This avalanche phenomenon makes the direct break of the cipher key practically impossible. On the other hand, the attacker can simply try all possible keys to decrypt the ciphertext, and see whether it matches the plaintext. This situation is equivalent to the brute-force attack case. Secondly, for XOR encryption of the dependent NALUs, the known-plaintext attack may consumes less resource to recover the key than that for AES. However, those NALUs lead less harm to the whole video bitstream because the decryption of them will need the AES encrypted NALUs. Finally, the derivation of the keys from layer to layer requires additional information (ADD) and ADD is also properly protected. It makes the recovery process even harder for the attackers. To sum up, the proposed security scheme can be considered to be immune to the known-plaintext attacks.

5.5.3. Computational Cost

The computational cost of proposed scheme is simulated in MATLAB environment. Two raw YUV videos sequences, namely “Foreman” and “News”, are taken into account in the simulations. The resolutions of test sequences are CIF (352×288 pixels) and QCIF (176×144 pixels). The H.264/SVC reference software, called JSVM 9.19, encodes the two sequences. As has been discussed in the previous sections, the encoding parameter *GOPSIZE* and *INTR* can be changed to vary the I and P picture numbers in the resulting H.264 bitstream file. Except for the case that *INTR*=-1, which means only one frame will be encoded as I picture, otherwise the I and P picture numbers can be calculated respectively.

$$I_NUM = \text{floor}(\text{Num_Frame} / \text{INTR}) \quad (5.7)$$

$$P_NUM = \text{floor}(\text{Num_Frame} / \text{GoP}) - I_NUM \quad (5.8)$$

The detailed settings for each video experiment are listed in Table 5.2.

Table 5.2: Experiments settings for FORMAN and NEWS video clips

EXPERIMENT NUMBER	GOP	INTR	I_NUM	P_NUM	B_NUM
1	4	4	75	2	223
2	4	8	38	39	223
3	4	32	19	58	223
4	4	32	10	67	223
5	4	-1	1	76	223
6	8	8	38	2	260
7	8	16	19	21	260
8	8	32	10	30	260
9	8	64	5	35	260
10	8	-1	1	39	260
11	16	32	10	12	278
12	16	64	5	17	278
13	16	128	3	19	278
14	16	-1	1	21	278

The encoding time for two sequences with different parameter settings are shown in Fig. 5.8. The computational time is normalized to the average encoding time of the experiments respectively. It can be seen that the overall computing time varies slightly among different video encoding parameter settings. Less computational cost is generally observed with fewer B picture. This is understandable because B pictures require more computational resources in encoding process.

Figure 5. 8: Normalized encoding time with different settings

The resulting SVC stream file size is also shown in Fig. 5.9. The size is normalized to the original raw file size respectively. According to the results, smaller encoded file size is generally corresponding to more B pictures. As a result, Fig. 5.8 and Fig. 5.9 show a tradeoff between encoding time and encoded file size.

Figure 5. 9: Normalized stream file size with different settings

The file size overhead of the encrypted stream file is depicted in Fig. 5.10. It can be observed that, for experiments with the same GOP size, more P pictures generally result in higher file size overhead. Generally, the overhead of the proposed method is achieved below 1.6%, which is acceptable and comparatively lower than that in [117].

Figure 5. 10: Encrypted file size overhead

The encryption time for the 14 experiments is depicted in Fig. 5.11. Within the same GOP size, encryption time cost is decreased as the increase of intra period value. The larger the *INTR* value is, the fewer the number of I picture is. As expected, due to the more complicating algorithm for AES, stream with more I pictures consumes more encryption time than those with less I pictures.

Figure 5. 11: Encryption time normalized to encoding time with different settings

Hence, if sophisticated encryption algorithm, in this case AES, is employed to all the layers, the computational resource and time cost would be too high to accept. Selective encryption is considered to reduce the amount of data to be encrypted while ensuring the required security level. In literature, selective encryption is always

implemented to important parts of bitstream or packets. In our proposed method, selective encryption is denoted as different levels of protection. More complicate cipher algorithm would be adopted for important plaintext; while light-weighted cipher would be employed to less significant instead of leaving uncovered. As encryption efficiency can be evaluated by the ratio of encryption time to encoding time, Fig. 5.11 can also be regarded as the encryption efficiency with different GOP and *INTR* settings. The minimum efficiency corresponds to the maximum I picture frames. The highest overhead time consuming is simulated as around 0.002% for both videos, which can be considered as neglectable to the encoding time. Therefore, our selective level protection scheme is not computational expensive.

The entropy of the stream file before and after encryption is also investigated to evaluate the effect of the encryption algorithms. The entropy is firstly calculated within NAL unit level on a byte basis. Then the entropies of all the NAL units are added up as the final stream file entropy. Fig. 5.12 depicts the results for both Foreman and News. It can be seen that the total entropy after encryption is higher than that before encryption. This means the proposed encryption algorithms introduce no negative effect to the encoding efficiency.

Figure 5. 12: Calculated entropy of the stream file before and after encryption (a) Foreman.
(b) News

5.5.4. Comparative Analysis

To compare with current state-of-the-art SVC encryption solutions, we select six critical kinds of methods and carry out the comparative analysis with our proposed scheme. Table 5.3 demonstrates the brief comparative results of different existing SVC protection schemes with ours. In the table, the first row shows the main comparison aspects and properties. CF denotes schemes that preserve compression efficiency and is so called compression friendliness. FC represents format compliant scheme for the H.264/SVC standard. BO denotes bitstream-oriented solution. Other

chosen comparisons aspects are in terms of add offline complexity, bit-rate overhead, encryption algorithms, key generation (K-G) and distribution (K-D).

Generally, all the encrypted contents are different among the following discussed seven schemes. Some implemented schemes are considered to provide low level perception security by choosing weak encryption content. The only residual data or sign bits encryption in [76] cannot ensure the security because encrypted video can be decoded by malicious brute force attack on sign bits. For the compression friendliness property, the schemes with IPM encryption and DC value alterations cause video statistics change, so that lead to compression efficiency degradation. As the format compliance, all the methods follow and preserve H.264/SVC standard format. Among those schemes, only our proposed method and [80] are bitstream-oriented encryption schemes, while the others are compression-integrated schemes. For the offline application scenario, the video data is already in the status of compressed bitstream. Therefore, compression-integrated schemes have to require more computational complexity denoted as “+H” to perform compression or decompression. However, the bitstream-oriented would not increase additional computational cost for the offline scenario. Bit-rate overhead indicates the change of video data size after encryption. This bit-rate overhead issue may be due to residual data encryption, DC value alteration or block cipher padding. The employed encryption algorithms of existing approach can be categorized into two types: simple XOR stream cipher or complicated AES (LEX) cipher. The former algorithm achieves small computational cost but lack of sufficient security. The latter is able to secure the content but suffers high computational cost. One common inadequacy of existing methods is key generation and distribution issue.

In short, our proposed scheme protects NAL units after compression, so it has no effect on the compression efficiency and format compliancy of the bit-stream. The method is a bitstream-oriented, and hence would not introduce additional complexity

for offline situation. The encryption algorithm incorporates AES and XOR to protect different important levels of video content. At last, we implement a complete secure key generation and distribution on layer basis for the SVC bitstream protection.

Table 5.3: Comparative analysis of H.264/SVC encryption schemes

Schemes	Encrypted Content	CF	FC	BO	Add Complexity (offline)	Bit-rate Overhead	Encryption Algorithm	K-G	K-D
ROI encryption	Sign of texture MVD and FGS in ROI	Yes	Yes	No	+H	No	XOR	No	No
NAL level encryption	IDR ,SPS and PPS	No	Yes	No	+H	Yes	LEX	Yes	No
Format compliant encryption[80]	NAL unit	Yes	Yes	Yes	0	Yes	AES-ECB	No	No
Selective encryption	IPM, sign of residual and MVD	No	Yes	No	+H	Yes	Not specified	Yes	No
Scalable protection	Sign of texture MVD and FGS	Yes	Yes	No	+H	No	XOR	Yes	Yes
Scalable encryption	Sign of texture and MVD, DC alteration	No	Yes	No	+H	Yes	XOR	No	No
Our scheme	NAL unit payload	Yes	Yes	Yes	0	Yes	AES-CBC, XOR	Yes	Yes

Chapter 6

Conclusion and Recommendations

In this thesis, rain attenuations on video streaming, DoS attacks to satellite system and H.264/SVC video content protection issues have been studied and presented schemes to cope with these problems.

Video streaming over satellite links suffers severe signal degradations due to rain attenuation. A number of experiments of video streaming via satellite links have been conducted to investigate the relationships between four major factors: rainfall rate, received power level, IP packet loss, and video quality. Statistical analysis has been performed to extract these relationships. Three models for power level versus rainfall rate, IP packet loss versus rainfall rate and IP packet loss versus power level have been proposed and verified respectively. Based on these works, a closed-loop adaptive power control scheme has been proposed as a countermeasure to overcome the degradation of video quality caused by rain fades. A PID controller was used to mitigate the settling time of the received signal strength towards the desired level. Simulation results have shown the feasibility of the proposed power control scheme and its ability to maintain good video quality in spite of rain fades. The proposed power control scheme is able to improve the reliability of the satellite link by approximately 3 times based on the data for the year 2010.

In defense against DoS attacks, a Rabin function employed solution has been successfully proposed to improve the security of the sequence number. Through the analysis of the simulation results, the proposed method has been found to be able to efficiently prevent DoS attacks and have low consumption of computation resources by avoiding further verification.

In H.264/SVC video protection, an efficient bitstream-oriented scheme has been presented and examined. Owing to the scalability of SVC bitstream, I picture data from the base layer are protected by highly secured AES algorithm in CBC mode, whereas the P picture data and enhancement layers NAL units are under the protection of XOR cipher. Besides, the uniqueness of IV, key generation and key distribution issues have also been developed in this thesis. To be format compliant, the original types of NAL units are replaced by the unspecified types in a secure way of mapping without influencing the decoding process. At last, the experimental results have demonstrated that the proposed scheme can protect the H.264/SVC with preservation of its full functionalities and has low computational cost.

Some of the studies presented in this thesis are still at their initial stages of research. They have great potential for further development. The following are the suggestions for the near future research.

- The power control method to mitigate rain attenuation is worth being extended to combine with site diversity technique. The maximum compensation power level is 10 dB. When the rain attenuation exceeds the maximum compensation power, it is useful to employ site diversity to supplement the power control method on improving the link performance.
- The research on DoS attacks prevention is at its initial stage. Future work would focus on the evaluation of the effectiveness of the proposed solution in more details. More studies should be done to demonstrate the time efficiency and computational cost of proposed method. Comparisons of its performance with

other methods will also be carried out.

- The protection of H.264/SVC video is a potential and challenging research area. In this thesis, the H.264/SVC encryption has been studied. It is believed that the authentication of H.264/SVC would be another field which is worth investigating.

Author's Publications

Journal Papers

1. Ting Ma, Yee Hui Lee, Maode Ma, Stefan Winkler, "The Rain Attenuation on Real-Time Video Streaming via Satellite Links," *Journal of Computer Theory and Engineering*, Vol. 4, No. 4, August 2012, pp. 595-598.
2. Ting Ma, Yee Hui Lee, Maode Ma, "Protecting Satellite Systems from Disassociation DoS Attacks," *Wireless Personal Communications*, Vol. 69, No. 2, 2013, pp. 623-638.
3. Ting Ma, Yee Hui Lee, Stefan Winkler and Maode Ma, "QoS Provisioning by Power Control for Video Communication via Satellite Links," *International Journal of Satellite Communications and Networking*, Published Online, 2014.

Manuscript under Review

1. Ting Ma, Maode Ma and Yee Hui Lee, "Bitstream-oriented Protection for the H.264/Scalable Video Coding (SVC)," has been submitted to Springer Multimedia Systems.

Conference Papers

1. Ting Ma, Yee Hui Lee, Maode Ma, "Protecting Satellite Networks from Disassociation DoS attacks," *Proceeding of IEEE International Conference Communication Systems*, Nov. 2010, pp. 662-666.

Bibliography

- [1] J. P. Choi and V. W. S. Chan, "Predicting and Adapting Satellite Channels with Weather-induced Impairments," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 38, No. 3, 2002, pp. 779-790.
- [2] F. Gargione, T. Iida, F. Valdoni and F. Vatalaro, "Services, Technologies, and Systems at Ka Band and Beyond – a Survey," *IEEE Journal on Selected Areas in Communications*, Vol. 17, No. 2, 1999, pp. 133-144.
- [3] A.F. Ismail, M.R. Islam, J. Din, A.R. Tharek and N.L.I. Jamaludin, "Investigation of Rain Fading on a 26 GHz Link in Tropical Climate," *Proceeding 6th International Conference Telecommunication Systems, Services and Application*, 2011, pp. 126-129.
- [4] R.A. Farrugia and C.J. Debono, "Accurate Modeling of Ka-band Videoconferencing Systems Based on the Quality of Experience," *IET Communications*, Vol. 3, No. 1, 2009, pp. 67-74.
- [5] Richharia, M., & Westbrook, L. D., *Satellite Systems for Personal Applications: Concepts and Technology*, 1st ed. Wiley, London, 2010.
- [6] Beaumont, J.-F., & Doucet, G., (2007), "Threats and Vulnerabilities of Next Generation Satellite Personal Communications Systems: A defense Perspective," *Proceeding of IEEE Globecom Workshops*, Nov. 2007, pp. 1–5.
- [7] H. Schwarz, D. Marpe and T. Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard," *IEEE Transactions on Circuits Systems for Video Technology*, Vol. 17, No. 9, Sep. 2007, pp. 1103-1120.
- [8] H. Sohn, E. T. AnzaKu, W. De Neve, Y. M. Ro and K. N. Plataniotis, "Privacy

- Protection in Video Surveillance Systems using Scalable Video Coding,” *Proceeding 6th IEEE International Conference Advanced Video and Signal Based Surveillance*, Sep. 2009, pp. 424-429.
- [9] Y. Liu, S. Zhang, S. Xu and Y. Zhang, “Research on H.264/SVC Compressed Video Communication in 3G,” *Proceeding 4th International Conference Computer Science and Education*, 2009, pp. 327-332.
- [10] F. De Rango, M. Tropea, P. Fazio and S. Marano, “Call Admission Control for Aggregate MPEG-2 Traffic over Multimedia Geo-satellite Networks,” *IEEE Transactions Broadcasting*, Vol. 4, No. 3, 2008, pp. 612-622.
- [11] *Digital Video Broadcasting (DVB): Interaction Channel for Satellite Distribution Systems*, ETSI EN 301 790 v1.5.1, May 2009.
- [12] F. Filali, G. Aniba and W. Dabbous, “Efficient Support of IP Multicast in the Next Generation of GEO Satellites,” *IEEE Journal on Selected Areas in Communications*, Vol. 22, No. 2, 2004, pp. 413-425.
- [13] M. Dulik, “TCP and UDP Deployment in Environment with High Delay and High Bit Error Rate,” *Proceeding 4th IEEE International Symposium on Logistics and Industrial Informatics*, Sep. 2012, pp. 131-134.
- [14] H. Zheng and J. Boyce, “An Improved UDP Protocol for Video Transmission over Internet-to-wireless Networks,” *IEEE Transactions on Multimedia*, Vol. 3, No. 3, 2001, pp. 356-365.
- [15] G. Cunningham, P. Perry, J. Murphy and L. Murphy, “Seamless Handover of IPTV Streams in a Wireless LAN network,” *IEEE Transactions on Broadcasting*, Vol. 55, No. 4, 2009, pp. 796-801.
- [16] F. F. Amrullah, E. Setijadi and G. Hendrantoro, “Computation of Rain Attenuation in Tropical Region with Multiple Scattering and Multiple Absorption Effects using Exponential Drop Size Distribution,” *General Assembly and Scientific Symposium*, 2011, pp. 1-4.
- [17] B. Mohapatra, P. K. Sahu and A. Patra, “16 Spot Beam Ka-band Satellite Communication in India for Rain Fade Mitigation,” *Proceeding Student Conference on Engineering and Systems*, 2012, pp. 1-4.
- [18] J. P. Choi and V. W. S. Chan, “Predicting and Adapting Satellite Channels with Weather-induced Impairments,” *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 38, No. 3, 2002, pp. 779-790.

- [19] F. Gargione, T. Iida, F. Valdoni and F. Vatalaro, "Services, Technologies, and Systems at Ka Band and Beyond – a Survey," *IEEE Journal on Selected Areas in Communications*, Vol. 17, No. 2, 1999, pp. 133-144.
- [20] K. Charilaos, F. Laurent, F. Vincent, J. Nicolas and L. Joel, "Use of the HYCELL Model for Predicting Rain Attenuation on UAS Low Elevation Datalinks," *Proceeding the 4th European Conference on Antennas and Propagation*, Apr. 2010, pp. 1-5.
- [21] G. F. Bryant, I. Adimula, C. Riva, and G. Brussaard, "Rain Attenuation Statistics from Rain Cell Diameters and Heights," *International Journal of Satellite Communications*, Vol. 19, 2001, pp. 263-283.
- [22] C. Capsoni, L. Luini, A. Paraboni, C. Riva, and A. Martellucci, 2009, "A New Prediction Model of Rain Attenuation that Separately Accounts for Stratiform and Convective Rain," *IEEE Transactions on Antennas and Propagation*, Vol. 57, No. 1, Jan. 2009, pp. 196-204.
- [23] R. K. Crane, "A Two-component Rain Model for the Prediction of Attenuation Statistics," *Radio Science*, Vol. 17, No. 6, 1982, pp. 1371-1387.
- [24] A.F. Ismail, M.R. Islam, J. Din, A.R. Tharek and N.L.I. Jamaludin, "Investigation of Rain Fading on a 26 GHz Link in Tropical Climate," *Proceeding 6th International Conference Telecommunication Systems, Services and Application*, 2011, pp. 126-129.
- [25] R.A. Farrugia and C.J. Debono, "Accurate Modeling of Ka-band Videoconferencing Systems based on the Quality of Experience," *IET Communications*, Vol. 3, No. 1, 2009, pp. 67-74.
- [26] K. Ulaganathen, T. A. Rahman, S. K. A. Rahim and R. M. Islam, "Review of Rain Attenuation Studies in Tropical and Equatorial Regions in Malaysia: an Overview," *IEEE Antennas and Propagation Magazine*, Vol. 55, No. 1, Feb. 2013, pp. 103-113.
- [27] K.O.S. Sudarshana and A.T.L.K. Samarasinghe, "Rain Rate and Rain Attenuation Estimation for Ku Band Satellite Communication over Sri Lanka," *Proceeding of 6th International Conference on Industrial and Information Systems*, Aug. 2011, pp. 16-19.
- [28] Q. W. Pan, J.E. Allnutt and C. Tsui, "Evaluation of Diversity and Power Control Techniques for Satellite Communication Systems in Tropical and Equatorial Rain Climates," *IEEE Transactions Antennas Propagation*, Vol. 56,

- No. 10, 2008, pp. 3293-3301.
- [29] C. Capsoni, M. D'Amico, R. Nebuloni and C. Riva, "Performance of Site Diversity Technique Estimated from Time Diversity," *Proceeding 5th European Conference Antennas and Propagation*, 2011, pp. 1463-1466.
- [30] K. M. Udofia and I. E. Otung, "Evaluating Time Diversity Performance on an on-board Processing Satellite to Earth Station Downlink," *Proceeding 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies*, 2008, pp. 325-330.
- [31] C. Capsoni, M. D'Amico and R. Nebuloni, "Performance of Time-diversity Satellite Communication Systems Investigated through Radar Simulation," *Proceeding 2nd European Conference on Antennas and Propagation*, Nov. 2007, pp. 1-4.
- [32] E. Matricciani, "Time Diversity in Satellite Links Affected by Rain: Prediction of the Gain at Different Localities," *Proceeding 2nd European Conference Antennas and Propagation*, Nov. 2007, pp. 1-5.
- [33] J. X. Yeo, Y. H. Lee and J. T. Ong, "Performance of Site Diversity Investigated through Radar Derived Results," *IEEE Transactions Antennas Propagation*, Vol. 59, No. 10, 2011, pp. 3890-3898.
- [34] Oxy Riza P, K. Tanjung, G. Hendrantoro and A. Mauludiyanto. "Implementation Site Diversity Method on Ka-band Satellite to Reduce the Impact of Rain Attenuation in the Tropics Area," *Proceeding International Conference ICT for Smart Society*, Jun. 2013, pp. 1-6.
- [35] D. D. Hodges and R. J. Watson, "An Analysis of Conditional Site Diversity: a Study at Ka-band," *IEEE Transactions on Antennas and Propagation*, Vol. 57, No. 3, Mar. 2009, pp. 721-727.
- [36] L. Luini and N. Jeanin, "Use of Weather Radar Data for Site Diversity Predictions and Impact of Rain Field Advection," *Proceeding 4th Advanced Satellite Mobile Systems*, 2008, pp. 122-127.
- [37] A. G. Nabi, J. Din, "Link Availability Improvement using Site Diversity for High Altitude Platform Station in Malaysia," *Proceeding IEEE International Conference RF and Microwave*, Dec. 2008, pp. 395-398.
- [38] R. Mathar and A. Schmeink, "Proportional QoS Adjustment for Achieving Feasible Power Allocation in CDMA Systems," *IEEE Transactions on*

- Communications*, Vol. 56, No. 2, 2008, pp. 254-259.
- [39] I.M. Kim and H.M. Kim, "Efficient Power-management Schemes for Video Service in CDMA Systems," *IET Electronics Letters*, Vol. 36, No. 13, 2000, pp. 1149-1150.
- [40] D. G. Sweeney and C. W. Bostian, "Implementing Adaptive Power Control as a 30/20-GHz Fade Countermeasure," *IEEE Transactions Antennas Propagation*, Vol. 47, No. 1, 1999, pp. 40-46.
- [41] Russell J. F. Fang, "Broadband IP Transmission over SPACEWAY Satellite with On-board Processing and Switching," *Proceeding IEEE Global Telecommunications Conference*, Dec. 2011, pp. 1-5.
- [42] H. Fukuchi and T. Saito, "Novel Mitigation Technologies for Rain Attenuation in Broadband Satellite Communication System using from Ka-to W-band," *Proceeding 6th International Conference on Information, Communications and Signal Processing*, 2007, pp. 1-5.
- [43] B. Mohapatra, P. K. Sahu and A. patra, "16 Spot Beam Ka-band Satellite Communication in India for Rain Fade Mitigation," *Proceeding Student Conference on Engineering and Systems*, Mar. 2012, pp.1-4.
- [44] Y. Wang, J. Kang, Q. Chen, Qiang and M. Liu, "Rain Attenuation Compensation Scheme of the Ka Band Multi-beam Satellite Communication System," *Proceeding IET International Conference Wireless, Mobile and Multimedia Networks*, 2006, pp. 1-3.
- [45] Q. W. Pan, J. E. Allnutt and C. Tsui, "Satellite-to-earth 12 GHz Fade Slope Analysis at a Tropical Location," *Proceeding IEEE Antennas and Propagation Society International Symposium*, Vol. 4A, 2005, pp. 51-54.
- [46] K. Ahmad, B. Bakhache and S. E. Assad, "Secure and Efficient Support of Internet Multicast Transmission over Satellite DVB," *Proceeding Symposium on Broadband Networks and Fast Internet*, May 2012, pp. 65-71.
- [47] J.-C. Juang, "Analysis of Global Navigation Satellite System Position Deviation under Spoofing," *IET Radar, Sonar and Navigation*, Vol. 3, No. 1, 2009, pp. 1-7.
- [48] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela and A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," *IEEE Transactions on power systems*, Vol. 28, No. 3, Aug. 2013, pp. 3253-3262.

- [49] A. Cavaleri, b. Motella, M. Pini and M. Fantino, "Detection of Spoofed GPS Signal at Code and Carrier Tracking Level," *Proceeding 5th Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, Dec. 2010, pp. 1-6.
- [50] S. Glass and V. Muthukkumarasamy, "A Study of the TKIP Cryptographic DoS Attack," *Proceeding 15th IEEE International Conference on Networks*, Nov. 2007, pp. 59-65.
- [51] N. Borisov, I. Goldberg and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11," *Proceeding 7th International Conference on Mobile Computing and Networking*, 2001, pp. 180-189.
- [52] S. Sandhya and Sumithra Devi K.A., "Contention for Man-in-the-Middle Attacks in Blue Tooth Networks," *Proceeding 4th International Conference on Computational Intelligence and Communication Networks*, 2012, pp.700-703.
- [53] K. Hypponen and K. M.J. Haataja, "Nino Man-in-the-middle Attack on Bluetooth Secure Simple Pairing," *Proceeding 3rd IEEE International Conference on Internet*, Sept. 2007, pp. 1-5.
- [54] M. Apel, C. Bockermann and M. Meier, "Measuring Similarity of Malware Behavior," in *Proceeding 5th LCN Workshop on Security in Communications Networks*, Oct. 2009, pp. 891-898.
- [55] J. Mirkovic, J. Martin and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review*, Vol. 34, No. 2, 2004, pp. 39-53.
- [56] G. Carl, G. Kesidis, R. R. Brooks and S. Rai, "Denial-of-service Attack Detection Techniques," *IEEE Internet Computing*, 2006, pp. 82-89.
- [57] Rocky K. C. Chang, "Defending against Flooding-based Distributed Denial-of-service Attacks: a Tutorial," *IEEE Communication Magazine*, Oct. 2002, pp. 42-51.
- [58] M. P. Howarth, S. Iyengar, Z. Sun and H. Cruickshank, "Dynamics of Key Management in Secure Satellite Multicast," *IEEE Journal on Selected Areas in Communications*, Vol. 22, No. 2, Feb. 2004, pp. 308-319.
- [59] K. Ahmad, B. Bakhache, S. E. Assad, D. Caragata and M. Chetto, "Multicast Security Protocol over Satellite DVC based on Chaotic Sequences," *Proceeding International Conference Internet Technology and Secured*

Transactions, 2011, pp. 97-102.

- [60] G. Zheng, H.T. Ma, C. Cheng and Y.C. Tu, "Design and Logical Analysis on the Access Authentication Scheme for Satellite Mobile Communication Networks Message Modification Attacks," *IET Information Security*, Vol. 6, No. 1, 2012, pp: 6-13.
- [61] P. Rizomiliotis, A. Bogris and D. Syvridis, "Message Origin Authentication and Integrity Protection in Chaos-Based Optical Communication," *IEEE Journal of Quantum Electronics*, Vol. 46, No. 3, March 2010, pp: 377-383.
- [62] Z. Chen, S. Guo, R. Duan and S. Wang, "Security Analysis on Mutual Authentication against Man-in-the-Middle Attack," *Proceeding International Conference on Information Science and Engineering*, 2009, pp: 1855-1858.
- [63] P. E. ABI-CHAR, A. Mhamed and B. EL-Hassan, "A Secure Authenticated Key Agreement Protocol based on Elliptic Curve Cryptography," *Proceeding International Symposium on Information Assurance and Security*, 2007, pp: 89-94.
- [64] Y. Xu and W. Wang, "Detecting and Mitigating DoS Attacks in Wireless Networks without Affecting the Normal Behaving Nodes," *Proceeding Military Communication Conference*, 2007, pp. 1-7.
- [65] P. Ding, "Central Manager: a Solution to Avoid Denial of Service Attacks for Wireless LANs," *International Journal of Network Security*, Vol. 4, No. 1, Jan. 2007, pp. 35-44.
- [66] Mansouri D., Mokdad L., Ben-othman J. and Ioualalen M., "Detecting DoS Attacks in WSN based on Clustering Technique," *Proceeding Wireless Communications and Networking Conference*, 2013, pp. 2214-2219.
- [67] P. Du and S. Abe, "Detecting DoS Attacks using Packet Size Distribution," *Proceeding 2nd Bio-Inspired Models of Networks, Information and Computing Systems*, Dec. 2007, pp. 93-96.
- [68] M. Guechari, L. Mokdad and S. Tan, "Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks," *Proceeding IEEE ICC Ad Hoc and Sensor Networking Symposium*, 2012, pp. 173-177.
- [69] Taleb, T., Kato N., & Nemoto, Y., "A Round-trip Time-based Prevention Technique to Secure LEO Satellite Networks from Denial-of-service Attacks," *Proceeding IEEE 60th Vehicular Technology Conference*, Vol. 6, Sept. 2004, pp.

4012-4016.

- [70] Onen, M., & Molva, R., "Denial of Service Prevention in Satellite Network," *Proceeding IEEE International Conference on Communications*, Vol. 7, Jun. 2004, pp. 4387-4391.
- [71] Y. Zhao and L. Zhuo, "A Content-based Encryption Scheme for Wireless H.264 Compressed Videos," *Proceeding International Conference on Wireless Communication and Signal Processing*, Oct. 2012, pp. 1-6.
- [72] N. Mao, L. Zhuo, J. Zhang and X. Li, "Fast Compression Domain Video Encryption Scheme for H.264/AVC Streaming," *Proceeding 14th International Conference on Advanced Communication Technology*, Feb. 2012, pp. 425-429.
- [73] T. Stutz and A. Uhl, "A Survey of H.264 AVC/SVC Encryption," *IEEE Transactions on Circuits Systems for Video Technology*, Vol. 22, No. 3, Mar. 2012, pp. 325-339.
- [74] Su-Wan P., Sang-Uk S., "Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding (SVC)," *Proceeding IEEE 4th International Conference Network Computing and Advanced Information Management*, 2008, pp. 371-376.
- [75] Y.G. Won, T.M. Bae and Y. M. Ro, "Scalable Protection and Access Control in Full Scalable Video Coding," *Proceeding 5th International Workshop Digital Watermarking*, Vol. 4283 of Lecture notes in computer science, Springer, Korea, Nov. 2006, pp. 407-421.
- [76] C. Li, C. Yuan and Y. Zhong, "Layered Encryption for Scalable Video Coding," *Proceeding 2nd International Conference Image and Signal Processing*, 2009, pp. 1-4.
- [77] Y. Kim, S. H. Jin, T. M. Bae and Y. M. Ro, "A Selective Video Encryption for the Region of Interest in Scalable Video Coding," *Proceeding TENCON 2007-IEEE Region 10 Conference*, Taipei, Taiwan, Oct. 2007, pp. 1-4.
- [78] C. Li, "Multimedia Forensics and Security," *IGI Publishing Hershey, PA, USA*, 2008, pp. 351-352.
- [79] C. Li, X. Zhou, and Y. Zhong, "NAL Level Encryption for Scalable Video Coding," *Proceeding 9th Pacific Rim Conference Multimedia: Advances in Multimedia Information Processing*, Berlin, Heidelberg, 2008, pp. 496-505.
- [80] Thomas St., Andreas Uhl, "Format-compliant Encryption of H.264/AVC and

- SVC,” *Proceeding 10th IEEE International Symposium Multimedia*, 2008, pp. 446-451.
- [81] H. Kodikara Arachchi, X. Perramon, S. Dogan and A.M. Kondo, “Adaptation-aware Encryption of Scalable H.264/AVC Video for Content Security,” *Signal Process.: Image Communication*, 2009, pp. 468-483.
- [82] K. Mokhtarian and M. Hefeeda, “Authentication of Scalable Video Streams with Low Communication Overhead,” *IEEE Transactions on Multimedia*, Vol. 12, No. 7, Nov. 2010, pp. 730-742.
- [83] N. Thomas, D. Bull and D. Redmill, “A Novel H.264 SVC Encryption Scheme for Secure Bit-rate Transcoding,” *Proceeding Picture Coding Symposium*, 2009, pp. 1-4.
- [84] M. Fan, C. Yuan and Y. Zhang, “An Efficient Hierarchical Key Management of H.264/Scalable Video Coding,” *Proceeding IEEE International Conference Intelligent Computing and Intelligent Systems*, Oct. 2010, pp. 757-760.
- [85] M. N. Asghar and M. Ghanbari, “MIKEY for Key Management of H.264 Scalable Video Coded Layers,” *Journal of King Saud University-Computer and Information Science*, 2012, pp. 1-10.
- [86] M. Umehira, K. Kobayashi, Y. Yasui, M. Tanaka, R. Suzuki, H. Shinonaga and N. Kawai, “Recent Japanese R&D in Satellite Communications,” *IEICE Transactions on Communications*, Vol. E92-B, No. 11, 2009, pp. 3290-3299.
- [87] Y. H. Lee, S. Winkler, “Effects of Rain Attenuation on Satellite Video Transmission,” *Proceeding IEEE 73rd Conference Vehicle Technology*, 2011, pp. 1-5.
- [88] ITU-T, Coding of Audio-Visual Objects – Part 10: Advanced Video Coding, ITU-T Rec. H.264/ISO/IEC 14496-10:2012.
- [89] A. de Lattre, J. Bilien, A. Daoud, C. Stenac, A. Cellerier and J.-P. Saman. VideoLAN Streaming Howto. 2002-2005 the VideoLAN project. [Online]. Available: <http://images1.videolan.org/doc/streaming-howto/en/streaming-howto-en.pdf>
- [90] Tcpreplay. [Online]. Available: <http://tcpreplay.synfin.net/trac/>
- [91] M. Vranjes, S. Rimac-Drlje and D. Zagar, “Subjective and Objective Quality Evaluation of the H.264/AVC Coded Video,” *Proceeding 15th International Conference System, Signals and Image Processing*, pp. 287-290, 2008.

- [92] A. K. Moorthy, K. Seshadrinathan, R. Soundararajan and A. C. Bovik, "Wireless Video Quality Assessment: a Study of Subjective Scores and Objective Algorithms," *IEEE Transactions on Circuits Systems for Video Technology*, Vol. 20, No. 4, 2010, pp. 587-599.
- [93] S. Winkler and P. Mohandas, "The Evolution of Video Quality Measurement: From PSNR to Hybrid Metrics," *IEEE Transactions on Broadcasting*, Vol. 54, No. 3, 2008, pp. 660-668.
- [94] ITU-R, *Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems*, ITU-R Rec. P.618-9, 2009.
- [95] ITU-R, *Specific Attenuation Model for Rain for Use in Prediction Methods*, ITU-R Rec. P.838-3, 2005.
- [96] A. Sharifi, K. Sabahi, M. A. Shoorehdeli, M. A. Nekoui and M. Teshnehlab, "Load Frequency Control in Interconnected Power System using Multi-objective PID Controller," *Proceeding IEEE Conference Soft Computing in Industrial Applications*, June 2008, pp. 217-221.
- [97] J. Sun and X. Liu, "The Application Prospects of Intelligent PID Controller in Power Plant Process Control," *Proceeding International Conference Modeling, Identification and Control*, June 2012, pp. 399-403.
- [98] C. Jackson, J. Sun, J. Wysocarski and M. Wang, "Achieving Bounded Delay on a Time-varying Satellite Uplink," *Proceedings of IEEE Military Communications Conference*, 2009, pp: 1-7.
- [99] J. Janssen, D. D. Vleeschauwer, R. Windey, G. H. Petit and J. Leroy, "Delay Bounds for Voice over IP Calls Transported over Satellite Access Networks," *Mobile Networks and Applications, Special Issue on Satellite-Based Information Services*, Vol. 7, No. 1, 2002, pp: 79-89.
- [100] E. W. M. Wong and T. S. Yum, "Delay Bounds for Packet Satellite Protocols," *Proceedings of Global Telecommunications Conference and Exhibition*, Vol. 3, 1989, pp: 1409-1415.
- [101] A.A. Khalek, C. Caramanis and R. W. Heath Jr., "Delay-Constrained Video Transmission: Quality-driven Resource Allocation and Scheduling," *IEEE Journal of Selected Topics in Signal Processing*, Jun. 2014, pp: 1-16.
- [102] Q. Du and X. Zhang, "Statistical QoS Provisionings for Wireless Unicast/Multicast of Multi-Layer Video Streams," *IEEE Journal on Selected*

- Areas in Communications*, Vol. 28, No. 3, Apr. 2010, pp: 420-433.
- [103] G. Su and Min Wu, "Efficient Bandwidth Resource Allocation for Low-delay Multiuser Video Streaming," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 15, No. 9, 2005, pp: 1124-1137.
- [104] J. Xu, Y. Andreopoulos, Y. Xiao and M. van der Schaar, "Non-stationary Resource Allocation Policies for Delay-constrained Video Streaming: Application to Video over Internet-of-Things-Enabled Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 32, No. 4, 2014, pp: 782-794.
- [105] M. Sarkar and R. Goel, "An Algorithm to Enhance QoS for Streaming Video over WLANs," *Proceeding World Congress on Engineering and Computer Science Advances in Electrical and Electronics Engineering*, 2008, pp: 76-85.
- [106] European Standard: EN 301 790 V1.5.1. *Digital Video Broadcasting; Interaction Channel for Satellite Distribution Systems*, May 2009, pp. 135-151.
- [107] Buchmann, J., & Kaiser, M., "Computer Proven Correctness of the Rabin Public-key Scheme," *Proceeding of World Academy of Science, Engineering and Technology*, Vol. 27, May 2007, pp. 212-217.
- [108] Aslam, B., Islam, M. H., & Khan, S. A., "Pseudo Randomized Sequence Number based Solution to 802.11 Disassociation Denial of Service Attack," *Proceeding International Conference 1st Mobile Computing and Wireless Communication*, 2006, pp. 215-220.
- [109] SpoofMAC. www.klcconsulting.net/smac/.
- [110] MAC Changer. www.alobbs.com/macchanger/.
- [111] Airsnarf. www.airsnarf.shmoo.com.
- [112] Ratzer, A., Wells, L., Lassen, H., Laursen, M., Qvortrup, J., Stissing, M., *CPN Tools for Editing, Simulating and Analyzing Coloured Petri Nets, Applications and Theory of Petri Nets*, 2003, pp. 450-462.
- [113] CPN Tools. Homepage: <http://wiki.daimi.au.dk/cptools/cpntools.wiki>.
- [114] FIPS PUB 197, *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, U.S. Department of Commerce, Nov. 2001. [Online]. Available: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

- [115] Z. Shahid, M. Chaumont and W. Puech, "Fast Protection of H.264/AVC by Delective Encryption of CAVLC and CABAC for I and P Frames," *IEEE Transactions on Circuits Systems for Video Technology*, Vol. 21, No.5, May 2011, pp. 565-576.
- [116] J. Wang, *Computer Network Security: Theory and Practice*, Higher Education Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2009, pp. 71-72.
- [117] Z. Wei, Y. Wu, X. Ding and R. Deng, "A Scalable and Format-compliant Encryption Scheme for H.264/SVC Bitstreams," *Signal Process.: Image Communication*, Vol. 27, No.9, Oct. 2012, pp. 1011-1024.