MOBILE MULTIHOP RELAY WIMAX NETWORKS

SECURITY PERSPECTIVES

ADNAN SHAHID KHAN
ABEDA MUHAMMAD IQBAL

MOBILE MULTIHOP RELAY WIMAX NETWORKS

A SECURITY PERSPECTIVE

MOBILE MULTIHOP RELAY WIMAX NETWORKS

A SECURITY PERSPECTIVE

Adnan Shahid Khan

Abeda Muhammad Iqbal

Universiti Malaysia Sarawak

Kota Samarahan

First Publication 2018

Published in Malaysia by

UNIMAS Publisher,
Universiti Malaysia Sarawak,
94300 Kota Samarahan,
Sarawak, Malaysia.

Printed in Malaysia by

PPKS Production Sdn. Bhd.(623666-M)
Jalan Canna Off, Jalan Alwi, Tabuan Jaya
93350 Kuching, Sarawak, Malaysia

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Adnan Shahid Khan
MOBILE MULTIHOP RELAY WIMAX NETWORKS : SECURITY PERSPECTIVES
/Adnan Shahid Khan, Abeda Muhammad Iqbal.
Includes index.
ISBN 978-967-2008-59-0
1. IEEE 802.16 (Standard).
2. Wireless LANs.
3. Wireless communication systems.
4. Mobile communication systems.
5. Government publications--Malaysia.
I. Abeda Muhammad Iqbal.
II. Title.621.384

Contents

Preface

This book comprises in depth view of Mobile multihop relay (MMR) Worldwide Interoperability for Microwave Access (WiMAX) networks support multihop communication to increase wireless coverage and provide lower backhaul deployment cost with high throughput. It is believed that due to lack of physical infrastructure, MMR WiMAX is vulnerable to several medium access control (MAC) layer attacks especially denial of service, replay attack, man in the middle attack and interleaving attack. The objective of this book is to discuss the current security measure in MMR WiMAX networks that provides secure end to end data transmission and secure multicast and broadcast service (MBS). The discussed MMR WiMAX security protocols are incorporated at two different security phases, one for authentication and key management and the other for ensuring forward and backward secrecy in MBS. In the first phase, self-organized efficient authentication and key management scheme (SEAKS) is discussed to counter the various attacks. In the second phase, secure and efficient distributed relay-based rekeying algorithm (SEDRRA) is illustrated to tackle forward and backward secrecy. The performance of SEAKS has been evaluated using BAN LOGIC, National Chiao Tung University network simulator (NCTUns 6.0) and mathematical derivations. SEDRRA has been validated by formal method using rank theorem and mathematical derivation. Most importantly, the discussed security protocols have significantly enhanced network performance by providing efficient counter measures for security vulnerabilities. The proposed SEAKS protocols are backward and forward compatible and can also be applied to mobile WiMAX networks. SEDRRA can be applied to secure MBS for pay per view, TV broadcasting, and video conferencing applications.

Acknowledgement

My deepest gratitude to Allah SWT, the most gracious, most merciful for giving me the strength and wisdom in His abundance.

I would like to express my appreciation to Professor Dr Norsheila binti Fisal, Professor Dr Mazlan Abbas, Professor Dr Narayanan Kulathuramaiyar, Associate Prof. Dr Sharifah Hafizah Syed Ariffin, Associate Prof. Dr Johari Bin Abdullah and Dr Halikul Bin Lenando for their review and feedback; my key aspirations to complete this book. I wish to extend my gratitude to D. Nauman Shahid, Dr Shazia Parveen, Dr Madeeha Atta, Dr Attaullah Shah Bukhari, Sabiha Umar, Umar Ali Parvaiz Butt, Dr Maliha Waseem and Dr Waseem Zia for generously sharing their time, knowledge, experience, love and prayers. I would also like to say special thanks to my daughter Ayesha binti Adnan Ali Khan for sincerely offering me her inspiring smile, day in, day out.

Finally, I wish to express my appreciation to my parents Shahid Ali Khan (Father) and Nadra Parveen (Mother) whose financial support, love and persistent confidence in me, has taken the load off my shoulder. This work would not have been completed without their moral support, patience, encouragement, understanding and unwavering love and care. The continued encouragement and support have held up my spirit to make this piece possible.

List of Abbreviations

AES - Advanced Encryption Standard

AKID - Authorization Key Identifier

API - Application Programming Interface

AUTH-INFO - Authentication Information

AUTH - Authentication

AK - Authorization Key

AAA - Authentication, Authorization, and Accounting

BSAddr - Base Station Mac Address

BCID - Basic Connection Identifier

BS - Base Station

BS - Backward Secrecy

BWA - Broadband Wireless Access

CPS - Common Part Sub-layer

CS - Convergence Sub-layer

CERT - Certificate

CCM - Counter with CBC-MAC

CBC - Cipher Block Chaining

DSL - Digital Subscriber Line

DoS - Denial of Service

EAP	-	Extensible Authentication Protocol
ECB	-	Electronic Codebook
FS	-	Forward Secrecy
GUI	-	Graphical User Interface
GTEK	-	Group Traffic Encryption Key
GKEK	-	Group Key Encryption Key
GKUC	-	Group Key Update Command
HMAC	-	Hash-based Message Authentication Code
KEK	-	Key Encryption Key
KST	-	Knowledge Shared Table
LOS	-	Line of Sight
MAC	-	Media Access Control
MMR	-	Mobile Multihop Relay
MBRA	-	Multicast and Broadcast rekeying algorithm
MS	-	Mobile Station
MR-BS	-	Multihop Relay Base station
M-I-T-M	-	Man-in-the-Middle
MD-SHA	-	Message Digest Secure Hash Algorithm
N-RS	-	Non-Transparent Relay Station
NLOS	-	Non-line of Sight Authority
OD-2009	-	Official Draft-2009
O	-	Big O

PO	-	Packet Overhead
PDR	-	Packet Delivery Ratio
PR	-	Packet Received
PS	-	Packet Send
PDU	-	Protocol Data Unit
Pre-PAK	-	Pre-Primary Authorization Key
PKM	-	Privacy Key Management
PHY	-	PHYsical Layer
PKMv1	-	Privacy Key Management version 1
PKMv2	-	Privacy Key Management version 2
QoS	-	Quality of Service
RS	-	Relay Station
RSA	-	Ron Rivest, Adi Shamir and Leonard Adleman
RMRA	-	Relay Multicast Rekeying Algorithm
RNG-REQ	-	Ranging Request
RNG-RSP	-	Ranging Response
REQ	-	Request
RAR	-	Relay Authentication Request
MTRMs	-	Monthly Technology Review Meetings
RSP	-	Response
SEAKS	-	Self Organized Efficient Authentication and Key Management Scheme

SEDRRA	-	Secure and Efficient Distributed Relay-Based Rekeying Algorithm
SS	-	Subscriber Station
SIG	-	Signature
SZK	-	Security Zone Key
SZKEK	-	Security Zone Key Encryption Key
SBC	-	SS Basic Capability
SAID	-	Security Association Identifier
SA	-	Security Association
SHP	-	Small Hydro Power
TEK	-	Traffic Encryption Key
TLS	-	Transport Layer Security
WIMAX	-	Worldwide Interoperability for Microwave Access

1

Introduction

The IEEE 802.16 standard intends to provide broadband wireless access (BWA) for metropolitan area network (MAN), and is to design for the delivery of last mile BWA is substitute to the cable and DSL [1]. After adopting nomadic mobility i.e. IEEE 802.16e, the standard moves towards the mobile multihop relay (MMR) functions in IEEE 802.16j for coverage extension and throughput enhancement that is done simply by adding relays in between MR-BS and the SS [2,3]. However, insertion of new relays demand strict authentication and key management schemes between MR-BS, RS and SS to secure the traffic from different adversaries especially when the multihop RS initially joins the network [4]. Thus, security is essential in wireless technologies to allow rapid adoption and enhance their maturity, while designing the standard, the IEEE 802.16 working group has taken into consideration the security aspects to avoid mistakes of IEEE 802.11. Standard security specifications can mainly be found within the MAC layer which is called security sublayer.

The separate security sublayer provides authentication, secure key exchange and encryption. IEEE 802.16 employs a concept of security association (SA) which defines security parameters keys and encryption algorithms [5, 6]. First, the authorization consists of an X.509 certificate, an authorization key (AK), a key encryption key (KEK) and a hash message authentication code (HMAC) key, which will be used for authentication and key management. Second, the data for transport connections consists of a SA identifier (SAID), a cipher; traffic encryption keys (TEKs) and initialization

vectors for TEKs, which will be used for secure data transmission. This chapter will present the security requirements, challenges and different schemes of MMR WiMAX network. It also discussed and analyzed the existing PKM authentication protocols, multicast and broadcast rekeying algorithms and related work to the proposed WiMAX security model.

1.1 Evolution of IEEE 802.16 Standards

Around 1999, Working Group on Broadband Wireless Access Standards was set up to design the standards with their recommendations to support the enhancement and deployment of broadband wireless access standard. During 2001, IEEE 802.16-2001 standard was approved. Its frequency range and data transmission rates were 10-66GHZ and 70Mbps respectively and support LOS fixed point to point and point to multipoint communication [7, 8]. Due to absence of unlicensed spectrum and LOS demand, deployment of IEEE 802.16-2001 standard was restricted. Thus, for these reasons, during 2004, three more amendments, IEEE 802.16a-b-c were released [9]. The purpose for these enhancements is to improve interpretability, QoS, data performance, mesh networking and to support NLOS communication. Later, all these amendments combine together under a single standard: IEEE 802.16-2004 [10-12].

In 2005, IEEE 802.16e-2005 or simply IEEE 802.16e was approved and in 2006 it was released [13]. It is basically the enhancement of IEEE 802.16-2004 by adding mobility features and it's also known as mobile WiMAX. In 2006, IEEE802.16j was launched, the amendment to IEEE 802.16e by inserting relay stations in between BS and SS to enhance the coverage area. In 2009, IEEE merged all previous IEEE 802.16 standards together to form the latest standard i.e. IEEE 802.16-2009. During the same year, IEEE 802.16j-2009 specifying the multihop relays were released [14-16]. This amendment provides a more enhanced and systematic security and communications architecture than was previously defined in older versions of this standard.

1.2 MMR WiMAX Networks

In IEEE 802.16j-2009, multihop relays are an elective deployment to support performance and converge area in WiMAX networks [17-29]. In multihop relays network, BS can be modified to multihop relay base station (MR-BS). Communication within SS and MR-BS are relayed through RS, thus enhancing the coverage area and efficiency of the network.

Multihop relays [30-39] are partially or fully under the supervision of MR-BS. Thus leads towards two different modes viz. centralized and distributed scheduling modes. Relays with full MR-BS supervision is functioned under centralized scheduling mode where MR-BS is full responsible for all the decisions. Relays with partial MR-BS supervision functioned under distributed scheduling mode where all the decisions are taken by RS with the collaboration of MR-BS [40].

Relays are categories into two, non-transparent and transparent relays. Non-transparent relays function in both centralized as well as distributed scheduling mode. But for transparent relays, it only can function in centralized scheduling mode. These relays can operate in three separate schemes depending on the processing of received signals. These schemes includes amplify and forward, decode and forward and estimate and forward. Decode and forward and amplify and forward relays are also termed as non-transparent relays and transparent relays respectively [41]. These relays may be fixed in location like mounting on the top of the building or mobile travelling on vehicles [42]. As far as security matters are concerns, these relays worked in two different security modes i.e. centralized security mode and distributed security mode [43,44] that are well discussed later in this chapter. The complete diagram for multihop relays with transparent and non-transparent features is shown in Figure 1.1.

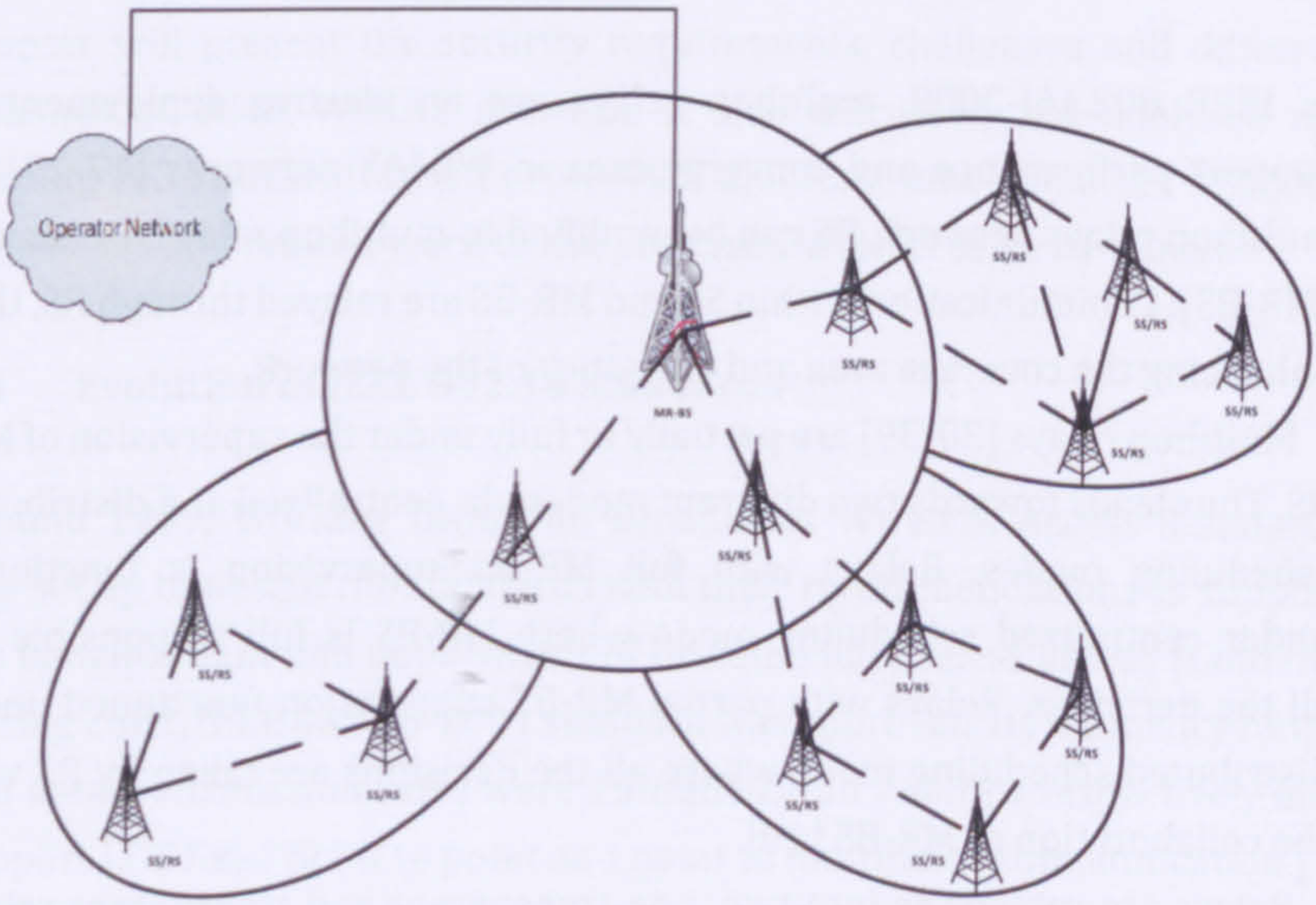

Figure 1.1: Multihop Topology

In MMR WiMAX network, two different relay station operational mode are defined; transparent mode RS(T-RS) and non-transparent mode RS (N-RS) [45]. The key difference between these two relay modes of operation is the ability to generate and send control information to its sub-ordinate stations which are included in the frame header. The RS operating in transparent mode do not generate and transmit control information, but in non-transparent mode, the relays do generate and transmit its own control information to its sub-ordinate stations [46]. The frame header contains essential scheduling information which the nodes use to determine when they are allowed transmit and receive information.

The Transparent mode Relay Station (T-RS) [47]: This type of RSs only forward control information generated by the MR-BS, and hence they do not extend the coverage area of the BS. However, T-RS can be used to enhance the system capacity in term of throughput within the BS coverage area. T-RS has less complexity and cheaper as compared with the N-RS. So, the T-RS only can operate in a centralised scheduling mode and for topology up to two hops only [48,49]. Figure 1.2 illustrate the transparent relay mode.

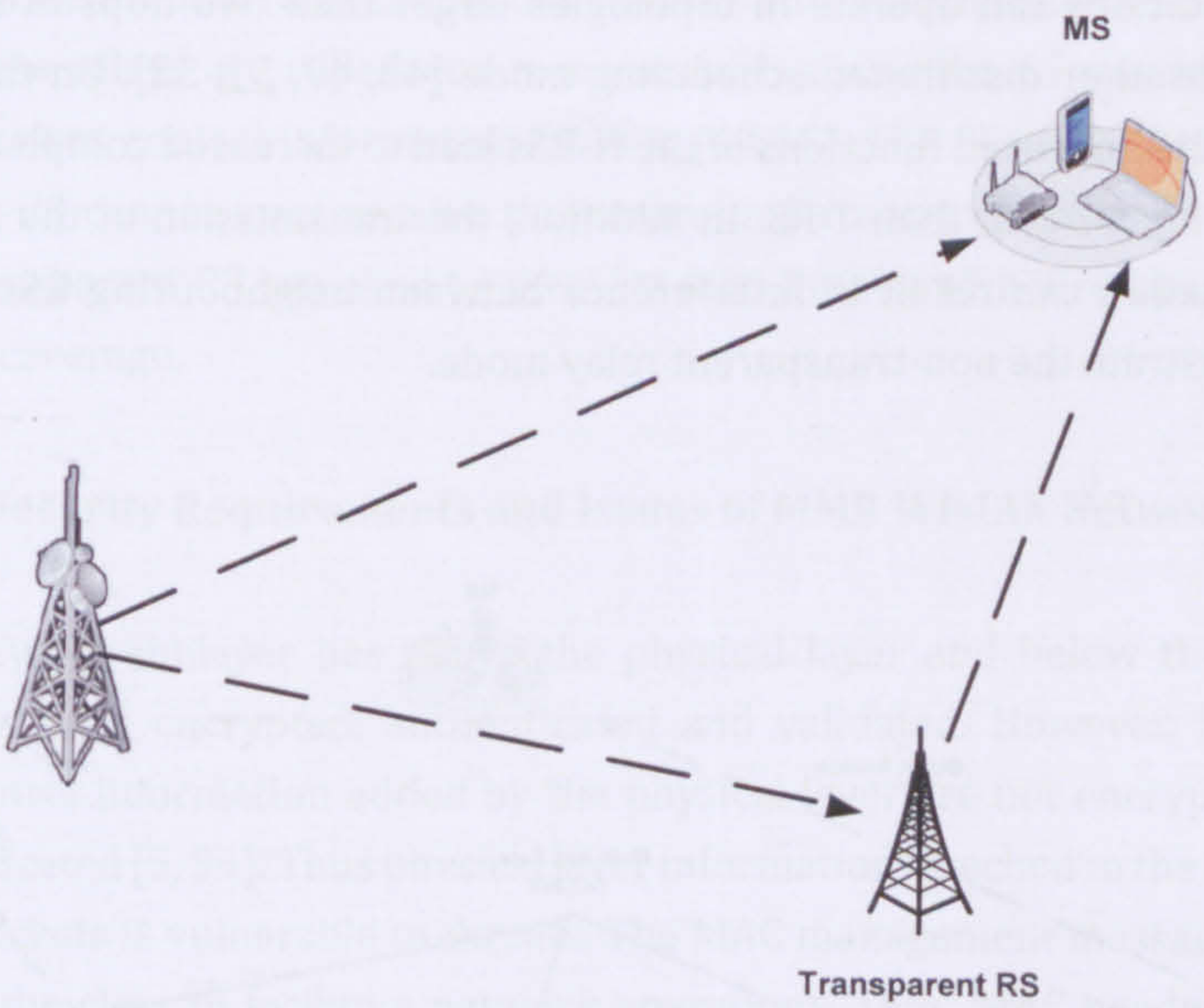

Figure 1.2: Transparent Relay Mode

In transparent relaying, the SSs communicating with relays can receive and decode the control information from the MR-BS. So, the RSs serving those SSs are not required to transmit control information themselves. These SSs are in range of the MR-BS but by using multiple hops with the aid of RSs can achieve higher throughput [50]. So, the goal of this type relaying is to enhance network capacity in term of throughput. This scheme of relaying

is called *transparent relaying*; because the SS is not aware the RS exists. In the transparent relaying all control information originates from the MR-BS.

The Non-Transparent mode Relay Station (N-RS) [10,49]. The N-RSs can operate on both centralized and distributed scheduling. When NT-RSs operate in distributed scheduling, they generate their own control information. However, when they are operating in a centralized scheduling, they only forward those provided by the BS. N-RSs can be used to provide cell coverage extension as well as capacity enhancement. Non-transparent relay stations can operate in topologies larger than two hops in either a centralised or distributed scheduling mode [43, 47, 51, 52]. On the other hand, the improved functions of the N-RSs lead to increased complexity and hence higher cost than T-RS. In addition, the transmission of the framing information can result in interference between neighbouring RSs. Figure 1.3 illustrate the non-transparent relay mode.

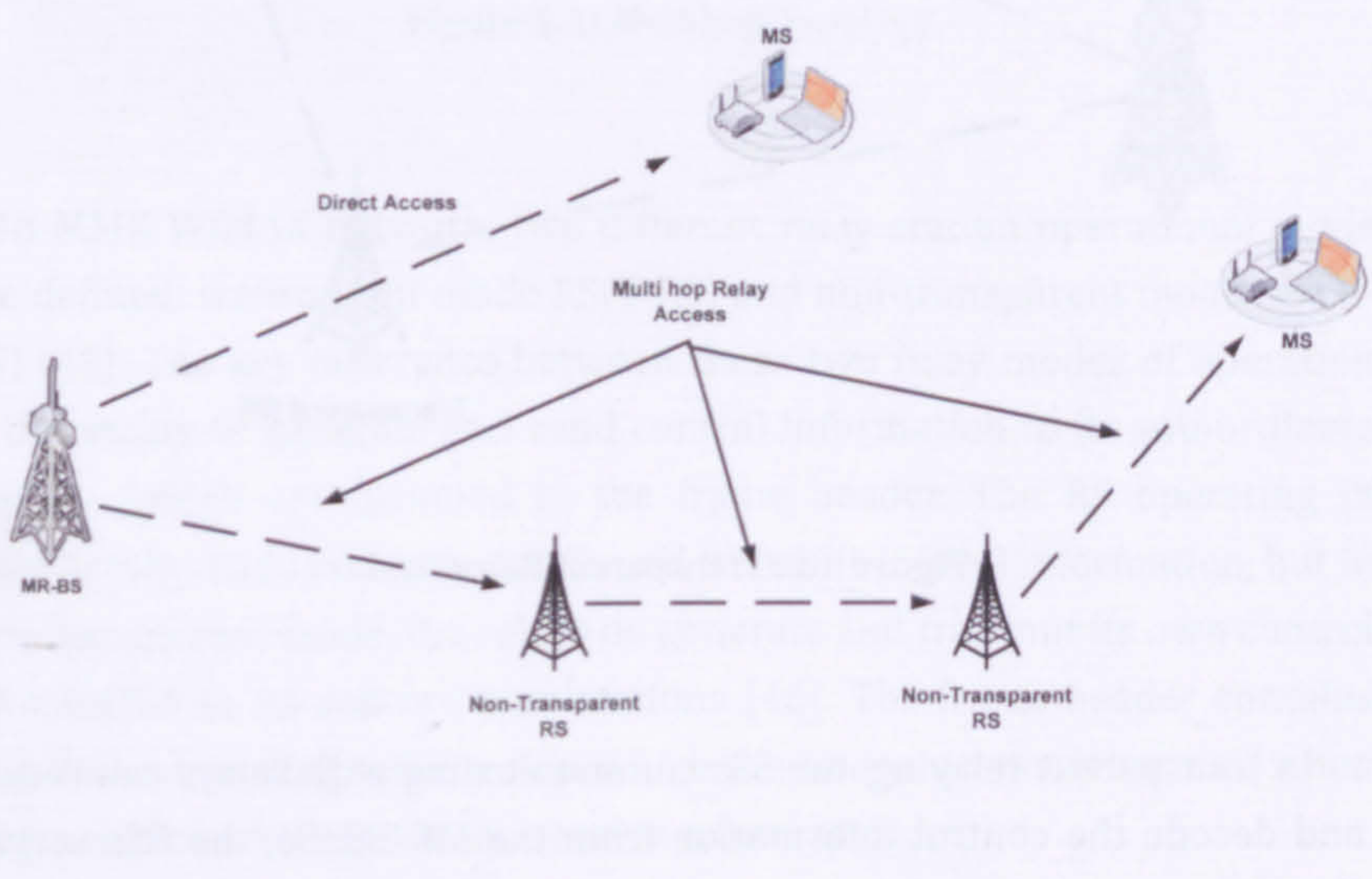

Figure 1.3: Non-Transparent Relay Mode

Furthermore, the N-RS can operate on amplify and forward scheme or decode and forward scheme. In amplify and forward, the N-RS acts as an analogue repeater that only amplify the received signal and forward it to the next node [52,53].

In non-transparent relaying, the SSs served with RSs and cannot receive or decode the control information from the MR-BS [49,53]. So, the relays serving these SSs must generate and transmit its own frame containing control information at the beginning of it. The end SS considers the serving RS as its base station and cannot deal with control information sent by MR-BS. These relays are called *non-transparent* because the SS synchronizes and receives control information from it [43,46]. The SSs out of range of the MR-BS cannot even receive the control information sent by it, so the non-transparent RS can send to them its own frame and hence extend the MR-BS coverage.

1.3 Security Requirements and Issues of MMR WiMAX Networks

The security sublayer lies above the physical layer and below the MAC CPS, which is encrypted, authenticated and validated. However, header and control information added by the physical layer are not encrypted or authenticated [5, 54]. Thus physical layer information attached to the higher layer packets is vulnerable to threats. The MAC management messages are sent in the clear to facilitate network operations. Thus, MAC header, MAC management messages like DCD, DL-MAP, UCD, UL-MAP, RNG-REQ, RNG-RSP, PKM-REQ, PKM-RSP, SBC-REQ and SBC-RSP are sent unencrypted, give wide field for the attacker to play [55-57]. Especially for the attacks mentioned later in this chapter.

DoS attack on the BS may possibly ensue during the PKMv2 authentication because of the intense public key computational load, an attacker might simply flood the BS with messages and the BS could use up its computational resources, evaluating signatures and decrypting messages[54,58]. BS authentication process in PKMv2 is vulnerable to an interleaving attack. In this attack, the attacker impersonates a valid RS, exchange the first two

messages of PKMv2 sequences with a valid BS, and then it replays these to the original, valid RS to gain the final PKMv2 messages. The attacker then uses the final message from the original RS to complete the original PKMv2 sequence with the BS resulting in unauthorized access to the network [59]. As the number of Hops increases in the distributed and non-transparent environment, unreliability increases thus more powerful and complex attacks can occur [54,60]. In the case, when the attacks involves the BS, it's a little bit tricky for the adversary to get successful as BS is much more intelligent device, however, if the case when RS is involved as RS is not too intelligent than BS, thus the chances of different attacks for RS is higher then BS.

MMR WiMAX network may need the following security function, which have not widely studied by others until now. Localized and hop-by-hop authentication is required. In MMR WiMAX network RS is introduced for coverage extension and throughput enhancement, for this purpose, localized and hop-by-hop authentication between RS, MS and MR-BS should be supported [4,61]. All the participating devices must be validated and authenticated by AAA server through MR-BS [62], because digital certificates of participating devices are only registered in AAA server database [63]. However, on the other hand, N-RS should authenticate other N-RS/MS on behalf of MR-BS [61,62]. Conventional MS should be used in MMR WiMAX network without any functional modification.

1.4 Security Scheme for MMR WiMAX Networks

In multihop relay WiMAX networks, two different security schemes has been proposed viz. centralized security scheme and distributed security scheme. Both schemes are discussed briefly in the following section.

Centralized security scheme normally resides in MR-BS in the multihop relay system where security association (SA) is established within RS and MR-BS without the participation of intermediate RS [5]. The intermediate RS does not decrypt the user data payload or do any kind of authentication to the SS or other RS; it just relays what MR-BS transmits to it [64]. MR-BS