ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

New System Security Model for a Mobile Operator's Meshed Access Network

Sharad Kumar Verma[1], Dr. D.B. Ojha[2]

Research Scholar, Department of CSE, Mewar University, Chittorgarh, Rajasthan, India[1]

Professor, Department of Engineering & Technology, Mewar University, Chittorgarh, Rajasthan, India[2]

ABSTRACT: A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e., routing functionality will be incorporated into mobile nodes. Such networks are more vulnerable to security attacks than conventional wireless networks. The main objective of this paper is to presents a description of the new security model for the 3rd generation mobile network architectures for the case of wireless mesh backhauls.

Keywords: 3rd generation mobile, wireless mess backhauls, security model

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Such networks are more vulnerable to security attacks than conventional wireless networks [5].

Radio sinks are used to provide back haul connectivity for base stations of mobile networks, in cases in which cable-based alternatives are not available and cannot be deployed in an economic or timely manner. To ensure high availability, such wireless back hauls have been predominantly used in redundant tree and ring topologies. Yet following the success of WiFi-based wireless mesh networks in recent years mobile network operators have become increasingly interested in meshed topologies for carrier-grade wireless back hauls as well. Mesh topologies may provide availability levels comparable to redundant trees and rings, while being more flexible and using capacity more efficiently [1]. However, radio links are also more exposed, and thus easier to tap and to interfere with, than their wired counter parts. This makes wireless back hauls, and in particular multi-hop ones like in wireless meshes, potentially more susceptible to security vulnerabilities. For carrier-grade wireless mesh backhaul solutions security therefore becomes a high priority non-functional requirement. Mobile network operators have high security demands in order to protect their business assets. Assets not only include the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

mobile network infrastructure and services, which must be protected from unauthorized use and from attacks on their availability or quality ,but an important asset requiring protection is furthermore an operator's reputation with current and potential customers. They thus need to ensure that their customers' data that is transported via their networks is protected against misappropriation. In some legislation, this is even an obligation of carriers as part of their due diligence. Architectural design issues can quickly compromise these security goals. A prominent example is GSM's security architecture that only requires user authentication towards the network. In contrast, the network itself is not authenticated to its users. This design flaw has subsequently been exploited to mount ''false base station attacks'': An attacker uses a device popularly called ''IMSI-catcher'', which pretends to be a legal base station with a superior signal quality. This causes mobile phones in the vicinity to associate themselves with the false base station, which then signals the mobile phones to switch off encryption, as investigated by Adoba et al. (2004). Similar attacks have been reported for Universal Mobile Telecommunication System (UMTS) networks by exploiting Global System for Mobile Communications (GSM) backward compatibility [3].

Although security attacks are well studied in 3G networks (the reader is referred e.g.to [4] for a study of security in 3G networks including some statistics on attacks in the past), the multihop nature of Wireless Mesh Backhauls (WMBs) exposes the network to new security threats which require additional measures to counter act. This article therefore extends the security threat analysis of 3G network architectures by 3GPP (2001) for the case of WMBs.

II. SYSTEM MODEL AND SECURITY MODEL

Fig1 shows the system security model of a traditional wireless access network with wired backhaul. It focuses on the transport stratum, i.e. all protocols required for the provisioning of a data transport between a user terminal (UT) and the core network. It further distinguishes between the management and control plane and the data plane of this stratum. The former divides into the user signaling part between the UT and its Point of Attachment (PoA) to the network, which in a mobile network is a wireless link, and the core network signaling part between the network elements of the access network and the core net work, which is typically wired, but may use non-meshed wireless links for backhaul. The data plane transports data between the UT and the core network. This data traffic is typically end-to-end encrypted. Note that the data plane from the point of view of the transport stratum may also carry management and control messages of the next higher stratum, i.e. the serving/home network stratum. User signaling, core network signaling and user data from three ''security domains'' , in the sense that if an attacker succeeds in overcoming the security features of one domain ,all subsystems with in this domain are compromised, but not necessarily those of other domains[6]. The latter depends on how well domains are ''firewalled'' from each other. Figure 2. shows the security domains of an access network using a WMB for backhaul. The figure also shows the security domains of the traditional access as grayed-out arrows, which are not covered in the present analysis, as it is assumed that proper security features to protect them are in place. Instead, the analysis will focus on these three sub- systems: the management and control traffic, the load-controlled data flows as well as the network entities of a WMB architecture.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

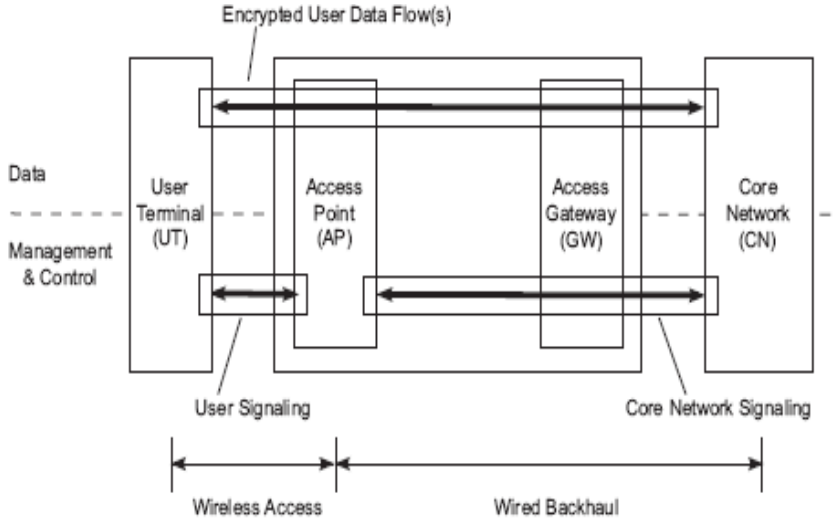

Fig1: System security model of a traditional wireless access network with wired backhaul.

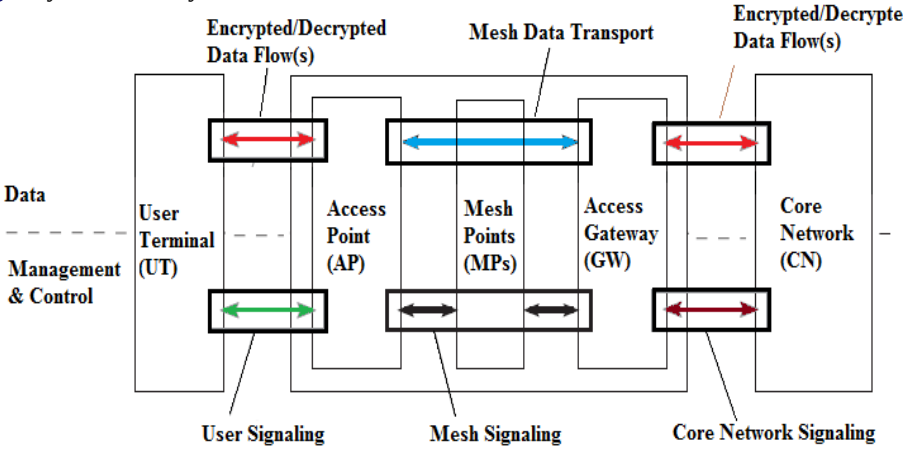

Fig2: The new system security model of a mobile operator's meshed access network.

A. Assumptions

To further delimit the scope of this analysis, the following assumptions are made that are in part a consequence of assuming a carrier-grade context: [7]

- All network entities of the mesh network are owned and operated by a single administrative entity.
- Likewise, UTs are not used for relaying of traffic.
- All network entities are static, so it can be assumed that their neighborhood only changes when a network entity of the WMB is activated or deactivated.
- The physical network entities are tamper-proof, i.e. there are physical countermeasures in place that prevent an attacker with physical access to the device to access information stored in the device.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

- Users have full control of the terminal.
- The terminal software as well as the software of network entities may be faulty.

B. Security Objectives

A secure WMB architecture should ensure the following security properties:

- Confidentiality: Confidentiality is the absence of disclosure of information to unauthorized individuals or systems.
- Integrity: Integrity is the absence of alteration of information by unauthorized individuals or systems.
- Authenticity: Authenticity is the establishment that information is genuine and has not been forged or fabricated.
- Non-repudiation: Non-repudiation means preventing that an individual or system can deny having participated in a transaction with another individual or system.
- Availability: Availability is the delivery of predictable and timely service.
- Privacy: Privacy means the protection of user data from disclosure to unauthorized individuals or systems.

C. Assets

WMBs store and transport different types of information, such as network state and user data, and require different types of resources for their operation. A security solution therefore needs to protect a wide range of assets:

- User-related assets: user data, (temporary or permanent) user identity, user location.
- Security-related assets: security credentials, session keys.
- Mesh management and control assets: measurement probes for network monitoring, signaling for radio resource management, routing etc.
- Mesh network assets: memory, computing and energy resources of network entities, wireless link bandwidth.

D. Communication Process

As shown in Figure 2, the user terminals send the request to the core network and receive response via meshed access network. In this new security model we use dual encryption for securing the data. First, when the user terminals send a request, the request first encrypted and transfer to the access point which add some security related assets like as session, after that the data will receive by meshed access network which provide services like measurement probes for network monitoring, signaling for radio resource management, routing etc. after completion the above process the request again encrypted and send to the core network access device. Where the request will be decrypted for each encryption. There are various encryption techniques. We can use any one.

For example:

Plaintext: comehometomorrow

Here we are using Simple Columnar Transposition Technique to encrypt the plain text. In this, write the plaintext message row by row in a rectangle of a pre-defined size. Read the message column by column, however, it need not be in the order of column 1,2,3,…., etc. It can be any random order such as 2, 3, 1,..., etc. The message thus obtained is the ciphertext message.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
c	O	m	E	h	o
m	E	t	O	m	o
r	R	o	W		

Figure 3. Simple Columnar Transposition Technique to encrypt the plaintext

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

Now let us decide the order of columns as some random order, say 4, 6,1,2,5,3. Then read the text.

Ciphertext: eowoocmroerhmmto

This ciphertext will transfer by the user terminals to the Mesh management and control point. The meshed access network adds some additional information to the packet receives and another encryption will be performed. Now the previous ciphertext will be the plaintext.

Plaintext: eowoocmroerhmmto

Again we are using Simple Columnar Transposition Technique to encrypt the plain text.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
e	O	w	O	o	c
m	R	o	E	r	h
m	M	t	O		

Figure 4. Simple Columnar Transposition Technique to encrypt the plaintext

Again we decide the order of columns as some random order, say 4, 6,1,2,5,3. Then read the text.

Ciphertext: oeochemmormorwot

Now the ciphertext will reached to the core network access device. The core network access device will first decrypt the encrypted data.

Ciphertext: oeochemmormorwot

Again we are using Simple Columnar Transposition Technique to decrypt the ciphertext. During encryption, we decide the order of columns as some random order such as 4, 6,1,2,5,3. Then write the text.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
e	o	w	o	o	c
m	r	o	e	r	h
m	m	t	o		

Figure 5. Simple Columnar Transposition Technique to decrypt the ciphertext

Now the:

Plaintext: eowoocmroerhmmto

This decrypted data send to the user terminals. Before receiving by the user terminals, the data again decrypted.

Ciphertext: eowoocmroerhmmto

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 6, August 2013

Again we are using Simple Columnar Transposition Technique to decrypt the ciphertext. During encryption, we decide the order of columns as some random order such as 4, 6,1,2,5,3. Then write the text.

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
c	O	M	e	h	o
m	E	T	o	m	o
r	R	O	w		

Figure 6. Simple Columnar Transposition Technique to decrypt the ciphertext

In the starting, we write the plaintext message row by row in a rectangle of a pre-defined size. Now read the message row by row. The message thus obtained is the plaintext message or original message.

Plaintext: comehometomorrow

This is the original text which is sent to the user terminals.

III. CONCLUSION

The objective of this paper is to provide a new system security model of a mobile operator's meshed access network. We cannot say that it is more secure but we just provide a new concept which performs dual cryptography.

REFERENCES

[1] 3GPP. Security threats and requirements. 3GPP TS 21.133 (V4.1.0); 2001.
[2] 3GPP. Access security review. 3GPP TR 33.801 (V1.0.0); 2005.
[3] Adoba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible authentication protocol (EAP). IETF RFC 3748; 2004.
[4] iGillott Research. 3G mobile network security. White Paper; 2007.
[5] Hu YC, Perrig A. A survey of secure wireless ad hoc routing. IEEE Security and Privacy 2004;2(3):28–39.
[6] Ren K, Yu S, Lou W, Zhang Y. PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks. IEEE Transactions on Parallel and Distributed Systems 2010;21(2):203–15.
[7] Zhang Y, Fang Y. ARSA: an attack-resilient security architecture for multihop wireless mesh networks. IEEE Journal on Selected Areas in Communications 2006;24(10):1916–28.

BIOGRAPHY

Sharad Kumar Verma, received his Bachelor of computer application (BCA) degree from MCRPV, Bhopal(MP), INDIA in 2004, Master of computer application (MCA) degree from UPTU Lucknow(UP), INDIA in 2007, and currently pursuing Ph.D in computer science (Network Security) from MEWAR University, Rajasthan, INDIA. He has more than five years of teaching experience in Meerut Institute of Engineering & Technology, Meerut (UP) INDIA. He is the author/co-author of more than 8 publications in reputed journals. The research fields of interest are Coding Theory and Time Synchronization in Wireless network.

Dr. Deo Brat Ojha, Birth Place & date Bokaro Steel City, (Jharkhand), INDIA on 05/07/1975. Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varanasi (U.P.), INDIA in 2004. The degree field is Optimization Techniques In Mathematical Programming. The major field of study is Functional Analysis. He has more than seven year teaching experience as PROFESSOR & more than ten year research experience. . He is working at MEWAR Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/co-author of more than 100 publications in technical journals and conferences