Rogue-base station detection in WiMax/802.16 wireless access networks

Michel BARBEAU*, Jean-Marc ROBERT**

Abstract

We address the problem of detecting a rogue base station (BS) in WiMax/802.16 wireless access networks. A rogue BS is a malicious station that impersonates a legitimate access point (AP). The rogue BS attack represents a major denial-of-service threat against wireless networks. Our approach is based on the observation that inconsistencies in the signal strength reports received by the mobile stations (MSS) can be seen if a rogue BS is present in a network. These reports can be assessed by the legitimate base stations, for instance, when a mobile station undertakes a handover towards another BS. Novel algorithms for detecting violations of received signal strength reports consistency are described in this paper. These algorithms can be used by an intrusion detection system localized on the legitimate BSS or on a global network management system operating the BSS.

Key words: Mobile radiocommunication, Access network, Wireless local loop, Base station, Communication security.

LA DÉTECTION DE FAUSSES STATIONS DE BASE DANS LES RÉSEAUX D’ACCÈS SANS FIL WIMAX/802.16

Résumé

Nous abordons le problème de la détection de fausses stations de base dans les réseaux d’accès sans fil WiMax/802.16. Une fausse station de base est une station qui usurpe l’identité d’une vraie station à des fins malicieuses. Ce type d’attaque représente une menace majeure. Notre approche à ce problème est fondée sur l’observation que la présence d’une fausse station de base se manifeste par des incohérences dans les rapports de puissance des signaux reçus. Ces rapports peuvent être en autre vérifiés lorsqu’une station mobile procède à un changement de station de base. De nouveaux algorithmes pour détecter des incohérences de rapports de puissance de signaux reçus sont décrits dans cet article. Ces algorithmes peuvent être intégrés à des systèmes de détection d’intrusions installés sur les stations de base réelles ou à un système de gestion de réseau veillant au fonctionnement des stations de base.

Mots clés: Radiocommunication service mobile, Réseau accès, Boucle locale radio, Station base, Sécurité communication.

* School of Computer Science, Carleton University – 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6
** Alcatel, CTO Security Research and Competence Center – 600 March Rd., Ottawa, ON, Canada K2K 2E6;
Current address: Département de Génie Logiciel et TI, École de technologie supérieure, 1100, rue Notre-Dame Ouest, Montréal (Québec), Canada, H3C 1K3 ; jean-marc.robert@etsmtl.ca.
I. INTRODUCTION

A wireless access network consists of access points (APS) and mobile stations (MSS). The APS provide network attachment to the MSS. As a serving AP selection strategy, a MS may choose the one that offers the strongest signal. A rogue AP is a malicious station that impersonates a legitimate AP. The rogue AP confuses a set of MSS trying to obtain network attachment through what they believe a legitimate AP. The exact method of attack depends on the type of network and state of associations between an impersonated AP and the victim MSS. For instance, in a WiFi/802.11 network, which uses the carrier sense multiple access (CSMA) scheme, a rogue AP attack may be conducted as follows. An attacker captures the identity, i.e. the medium access control (MAC) address, of a legitimate AP by listening to the traffic. The attacker builds a frame using the legitimate AP's MAC address. Then, it follows the CSMA scheme to send the frame.

In a WiMax/802.16 network, the attack is more difficult to do because of the time division multiple access (TDMA) scheme. To succeed, the attacker must use the MAC address as well as a time slot allocated to the impersonated base station (BS), the access point element providing attachment in a WiMax/802.16 network. Moreover, the attacker must transmit while the impersonated BS may be transmitting as well. The signal of the attacker, however, must arrive at the targeted receiver MSS stronger than the legitimate signal of the impersonated BS. In such a case, the legitimate signal would be seen as background noise. Therefore, the rogue BS attack may be conducted as follows. An attacker captures the MAC address of a legitimate BS by listening to the traffic. The attacker waits until a time slot allocated to the impersonated BS starts. Then, the attacker transmits his rogue signal and makes sure it arrives at a MS with received signal strength (RSS) higher than the one of the impersonated BS. The receiver MSS reduce their gain and decode the signal of the attacker instead of the original impersonated BS. This can happen because receivers are designed to operate over a wide range of signal levels, e.g. a 120 dB wide range [16]. They cannot, however, decode multiple signals spread over that wide range at the same time. This is because the demodulator inside a receiver must be fed with a relatively constant signal level, independently of the levels of the input signals. A mechanism called automatic gain control reduces the gain of the amplifier inside the receiver in presence of a strong signal to achieve the constant signal level required by the demodulator. A received signal may be strong enough to reduce the gain to a point where another received signal is relatively too weak to be interpreted by the demodulator and it just appears as background noise. The exact minimal difference $\alpha$ in strength between the two signals depends on the design of the receiver. A malicious higher RSS signal can be achieved in several ways. More power or a higher gain antenna can be used or the distance to the receivers can be shortened.