A Security Patch Addressing Bandwidth Request Vulnerabilities in the IEEE 802.16 Standard

Qiang Liu, Xiping Hu, Edith C.-H. Ngai, Min Liang, Victor C. M. Leung, Zhiping Cai, and Jianping Yin

Abstract

This article analyzes security vulnerabilities in bandwidth allocation and request mechanisms that are specified in the IEEE 802.16 Standard, and introduces a bandwidth request adversary model called UL-BRA based on these vulnerabilities. The goal of UL-BRA is to abuse the bandwidth request/grant operation of a WiMAX network, resulting in a significant decrease of the overall uplink transmission performance of the network. To overcome the challenge caused by the vulnerabilities of the standard, we propose a security patch incorporating a real-time anomaly detection and restoration (RADR) mechanism, which combines an MCDR scheme with an ATD scheme in order to eliminate the impacts of UL-BRA in real-time. We verify the effectiveness of RADR under UL-BRA threats via simulations, and demonstrate the effectiveness of the proposed patch in mitigating the threats of UL-BRA.

Worldwide interoperability for microwave access (WiMAX) and Third Generation Partnership Project (3GPP)-based Long Term Evolution (LTE) on the basis of orthogonal frequency-division multiplexing (OFDM) are two dominant standards in the fourth generation (4G) landscape. Basically, WiMAX provides wide-area broadband wireless access for subscriber stations (SSs). WiMAX is also a suitable solution in femtocell design [1] due to several attractive characteristics including wide transmission range, high access bit rate, effective quality of service (QoS) control, and so on. The IEEE 802.16 Working Group and WiMAX Forum are responsible for the specification and development of WiMAX networks. In 2012, the IEEE 802.16 Working Group released the IEEE 802.16-2012 standard [2] as the latest specification of the air interface for broadband wireless access systems. In large-scale access networks, network capacity is a prominent performance metric. Accordingly, most studies on IEEE 802.16 pay more attention to its capacity rather than its security [3] in order to offer high-speed networking. Nevertheless, the *buckets effect*, which states that the capacity of water in a bucket constructed using planks of varying lengths is determined not by the longest plank but by the shortest one, on the overall performance of large-scale networks reveals that a high level of security and privacy needs to be ensured. Although the security sublayer is specified in the IEEE 802.16 standard in order to offer a considerable level of protection from adversaries external to the network, it is weak to defend against adversaries internal to the network, which have proper credentials to operate over the network. On the other hand, the severe impact of intrinsic security vulnerabilities in the standard are rarely examined, which induces potential threats toward the standard itself. Uplink bandwidth request anomaly (UL-BRA) is a typical threat caused by exploiting security vulnerabilities in bandwidth allocation and request mechanisms that are specified in the standard [2]. When UL-BRA occurs, which abuses the bandwidth request/grant operations, the uplink throughput of the affected SSs could be significantly reduced. According to the standard, the base station (BS) scheduler can provide different levels of bandwidth polls and/or grants for subscribers by specifying a scheduling type and its associated QoS parameters. However, the specification has no defense against UL-BRA due to the fact that the generic medium access control (MAC) header is transmitted in the clear to facilitate normal operation of the MAC. Therefore, it is vital to implement a patch to overcome the weakness.

In this article, we first identify the vulnerabilities in bandwidth allocation in IEEE 802.16 during uplink transmission, then propose a real-time anomaly detection and restoration (RADR) mechanism to overcome the above security weakness of the standard in the presence of UL-BRA. Specifically, RADR combines a multi-source correlation-based detection and restoration (MCDR) scheme with an adaptive threshold determination (ATD) scheme to maintain the overall performance of a WiMAX network in terms of uplink throughput. The former scheme is used to detect UL-BRA caused by malicious WiMAX SSs in real time, whereas the latter one is used to dynamically adjust the detection threshold due to white noise, random signal jitters, and normal bandwidth contention when multiple uplink flows are present. We highlight the fact that RADR can be seamlessly incorporated into an extended version of the standard and implemented as a securi-

Qiang Liu, Zhiping Cai, and Jianping Yin are with the National University of Defense Technology.

Xiping Hu (corresponding author) is with Bravolol Limited.

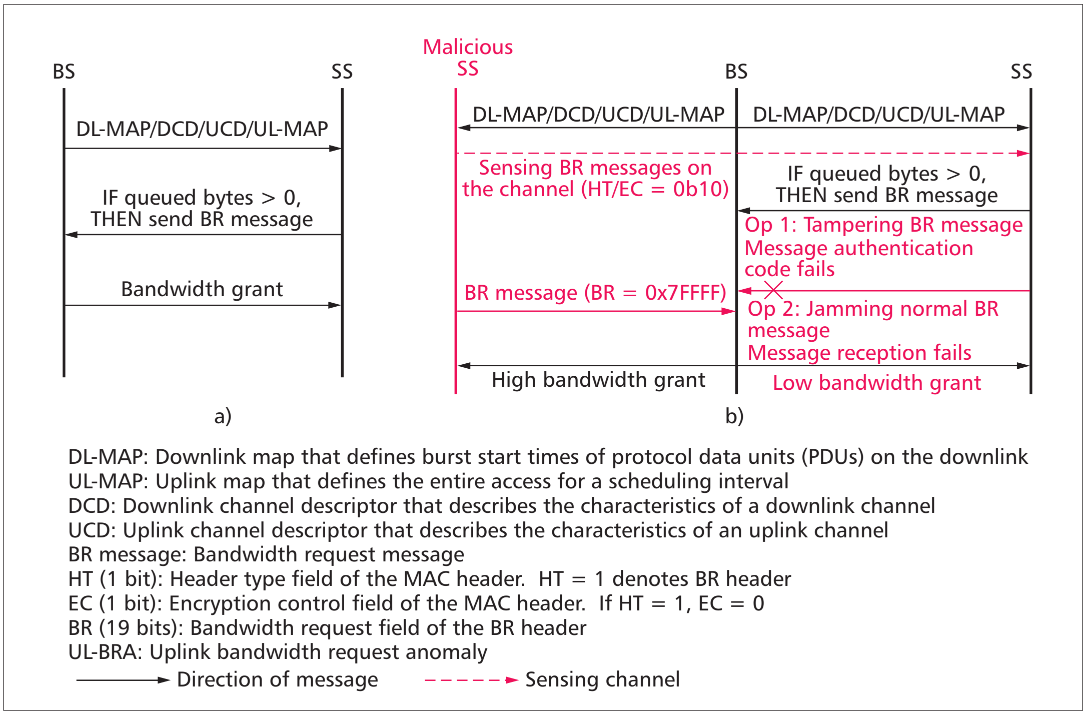
Edith C.-H. Ngai is with Uppsala University.

Min Liang is with IBM, China.

Victor C. M. Leung is with the University of British Columbia.

Zhiping Cai is also with Nanjing University of Information Science and Technology.

0890-8044/16/$25.00 © 2016 IEEE



DL-MAP: Downlink map that defines burst start times of protocol data units (PDUs) on the downlink
UL-MAP: Uplink map that defines the entire access for a scheduling interval
DCD: Downlink channel descriptor that describes the characteristics of a downlink channel
UCD: Uplink channel descriptor that describes the characteristics of an uplink channel
BR message: Bandwidth request message
HT (1 bit): Header type field of the MAC header. HT = 1 denotes BR header
EC (1 bit): Encryption control field of the MAC header. If HT = 1, EC = 0
BR (19 bits): Bandwidth request field of the BR header
UL-BRA: Uplink bandwidth request anomaly

Figure 1. Illustration of the UL-BRA threat: a) working flow of the normal bandwidth request/grant; b) working flow of the UL-BRA adversary model.

ty patch. To the best of our knowledge, this is the first attempt to design patches for fixing vulnerabilities in the standard, and we expect that our efforts would inspire more researchers and practitioners to pursue in-depth studies on the security of the standard. Moreover, we argue that the proposed RADR mechanism for WiMAX could easily be extended to LTE due to the fact that these two dominant 4G techniques are both based on the OFDM physical layer specification. The main contributions of this article are as follows:

- We analyze the security vulnerabilities in bandwidth allocation and request mechanisms in the IEEE 802.16 standard, and present a customized adversary model named UL-BRA that exploits these vulnerabilities to reduce the overall network performance in terms of uplink throughput.
- We propose RADR, which combines the MCDR scheme with the ATD scheme to protect 802.16 WiMAX networks against the above UL-BRA threat. By patching RADR to the regularized bandwidth request/grant procedure, we can effectively enhance the security of the standard by mitigating the threat of UL-BRA.

The rest of this article is organized as follows. We present the system model and some assumptions. We give a detailed description of RADR and discuss some practical issues of the mechanism. Then we describe an implementation of the proposed mechanism in a network simulator by extending WiMAX and present results that demonstrate the effectiveness of the patch. Finally, we conclude the article.

System Model and Assumptions

Network Model

In a WiMAX network, the OFDM physical layer specification operates on a frame-by-frame basis, where a frame consists of a downlink subframe and an uplink subframe [2]. Since the objective of the work is to address the challenge originating from vulnerabilities in bandwidth allocation and request mechanisms during the uplink transmission procedure, the uplink subframe is our main concern. Let us consider a WiMAX network consisting of one BS and multiple SSs connected to the BS directly. Furthermore, all WiMAX stations operate according to the IEEE 802.16 fixed broadband wireless access standard. Therefore, these stations are typically fixed in our discussion. For the convenience of discussion, we consider a signal-interface OFDM WiMAX network operating at time-division duplex or duplexing (TDD). In the TDD case, the downlink subframe comes first, followed by the uplink subframe at the same frequency. Basically, the WiMAX network guarantees QoS/quality of experience (QoE) for diverse applications by means of connection-oriented scheduling services, each of which is associated with a connection between the BS and an SS. We can see in Fig. 1a that an SS initializes a bandwidth request (BR) message to the BS if its connection queue is not empty.

Adversary Model

As mentioned above, the queue status of an SS's connection in terms of queued bytes plays a vital role in the bandwidth request/grant procedure, which is intuitively referred to in Fig. 1a. However, the BS is unable to inspect real changes of the queued bytes of the SS's connection queue, resulting in a security vulnerability. Specifically, the malicious SS sets the following fields of the generic MAC header according to the standard [2]: Header Type (HT) = 1 denoting BR header, Encryption Control (EC) = 0 denoting MAC protocol data unit (PDU) without data payload, and Bandwidth Request (BR) = 0x7FFFF. Moreover, the BR header shall not be encrypted by the security sublayer to facilitate normal operations, as specified in IEEE 802.16. Therefore, the existing security sublayer is weak in protecting BR messages against overhearing, tampering (i.e., Op1 in Fig. 1b), and jamming (i.e., Op2 in Fig. 1b), resulting in another security vulnerability.

As shown in Fig. 1b, the malicious SS exploits the above two vulnerabilities to illegally occupy uplink bandwidth resources or deny service of the normal SS. Specifically, the malicious SS initializes a BR message with any value of the BR field, for example, 0x7FFFF in Fig. 1b, since the BS is unable to inspect real changes of the queued bytes of the SS's connection queue. Furthermore, the malicious SS is able to sense

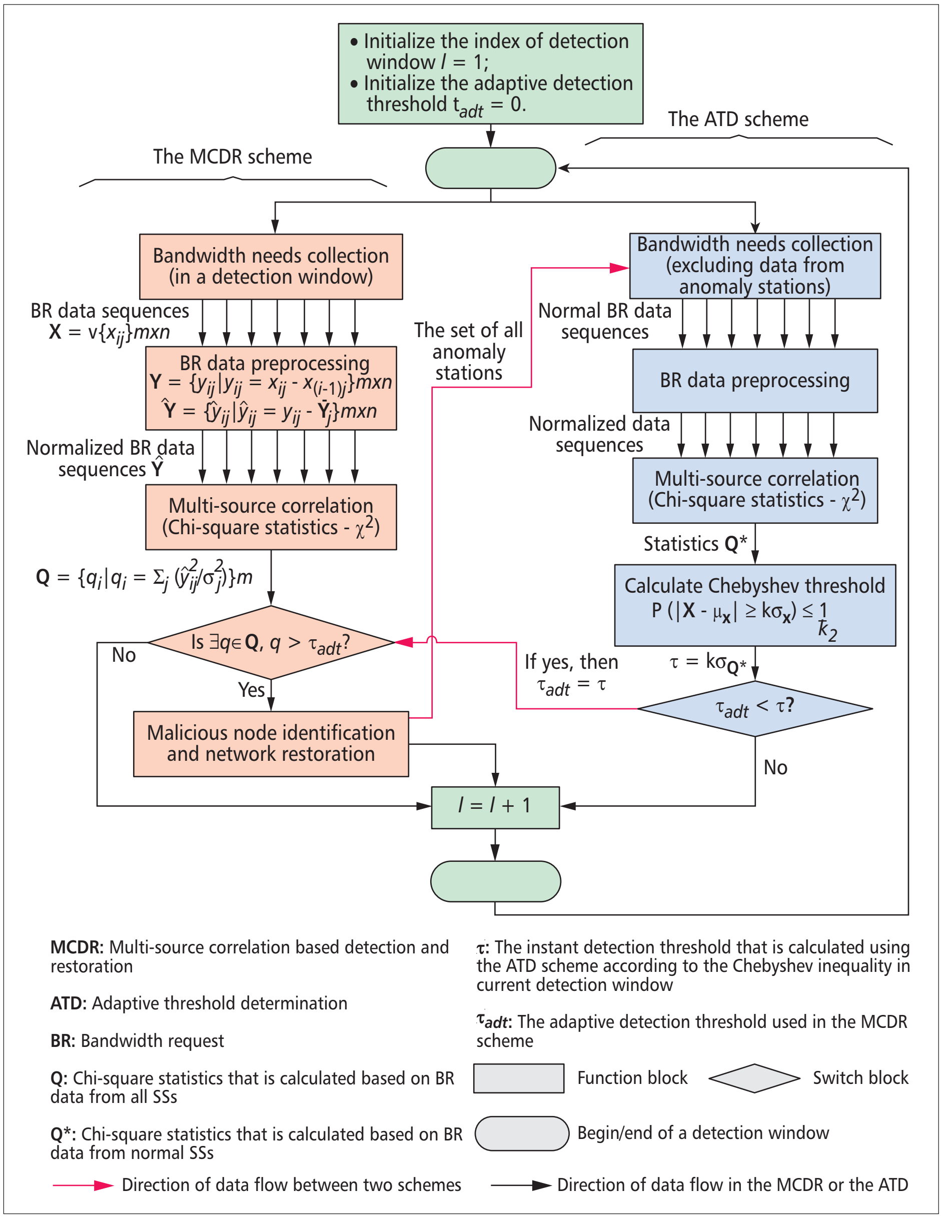

• Initialize the index of detection window l = 1;
• Initialize the adaptive detection threshold t_adt = 0.
The MCDR scheme
The ATD scheme
Bandwidth needs collection (in a detection window)
BR data sequences X = v{x_ij}mxn
BR data preprocessing
Y = {y_ij | y_ij = x_ij - x_(i-1)j}mxn
Ŷ = {ŷ_ij | ŷ_ij = y_ij - Ȳ_j}mxn
Normalized BR data sequences Ŷ
Multi-source correlation (Chi-square statistics - χ²)
Q = {q_i | q_i = Σ_j (ŷ²_ij/σ²_j)}m
Is ∃q∈Q, q > τ_adt?
No
Yes
Malicious node identification and network restoration
The set of all anomaly stations
l = l + 1
Bandwidth needs collection (excluding data from anomaly stations)
Normal BR data sequences
BR data preprocessing
Normalized data sequences
Multi-source correlation (Chi-square statistics - χ²)
Statistics Q*
Calculate Chebyshev threshold
P (|X - μ_X| ≥ kσ_X) ≤ 1/k²
τ = kσ_Q*
If yes, then τ_adt = τ
τ_adt < τ?
No
MCDR: Multi-source correlation based detection and restoration
ATD: Adaptive threshold determination
BR: Bandwidth request
Q: Chi-square statistics that is calculated based on BR data from all SSs
Q*: Chi-square statistics that is calculated based on BR data from normal SSs
τ: The instant detection threshold that is calculated using the ATD scheme according to the Chebyshev inequality in current detection window
τ_adt: The adaptive detection threshold used in the MCDR scheme
Function block
Switch block
Begin/end of a detection window
Direction of data flow between two schemes
Direction of data flow in the MCDR or the ATD

Figure 2. Working flow of RADR defeating the UL-BRA threat.

the transmission of BR messages originating from normal SSs because the BR header is not encrypted, then tampers with the BR field of these messages (Op 1) or even performs jamming against these messages (Op 2). Finally, the BS allocates a high bandwidth grant for the malicious SS and a low one for the normal SS. It is worth noticing that the bandwidth a normal SS will obtain should be determined by the QoS requirement specified in the bandwidth request packet; however, the successful delivery of the BR message without errors cannot be ensured. On the other hand, a malicious SS will construct a special BR message with a high but faked QoS requirement regardless of its true needs. Therefore, the typical impacts of such adversaries include low bandwidth grant for normal SSs and high bandwidth grant for malicious ones (optional). In practice, it is much harder for a malicious SS to interrupt normal BR messages by tampering with the specific BR field compared to direct jamming before they reach the BS. Thus, we figure out that Op 2 should be carefully examined in the real case. To conduct jamming attacks targeting the specific BR messages on the air along with minimizing the risk of being detected, reactive jamming is designed to target the receiver side. Typically, reactive jamming interferes with the current on-the-fly BR message, introducing several errors, or even preventing the recovery of the BR message on the receiver side [4]. Generally speaking, it is challenging and uneconomical for a malicious SS to design and implement reactive jamming due to strict real-time requirements. However, some state-of-the-art work makes such intelligent jamming feasible for use (e.g., software-defined reactive jamming). More details of the flexible and reliable software-defined reactive jamming can be found in [5].

Assumptions

As we know, an uplink data flow with a higher level of QoS has a higher priority to obtain bandwidth grant [2]. In order to focus on the vulnerability research of the standard, we make two assumptions as follows:

- We assume that all uplink flows are unicasting flows. As specified in IEEE 802.16 [2], one typical scheduling type in UL request/grant scheduling is unsolicited grant service (UGS), for example, voice over IP without silence suppression, and the bandwidth requirement of UGS connections do not change between connection establishment and termination. On the other hand, other types of UL scheduling are designed to support UL flows that transport variable-size data packets. Therefore, we consider that normal SSs may originate data flows with constant or changeable bandwidth needs.
- We also assume that the BS grants requested bandwidth needs from SSs in a round-robin (RR) fashion [6]. The RR method can ensure fair bandwidth allocation among multiple SSs.

Real-Time Anomaly Detection and Restoration Mechanism

Overview

Since all scheduling services toward SSs are connection-oriented, the BS enforces the bandwidth request/grant procedures on a periodic basis, where a scheduling period is equal to a MAC frame duration. Therefore, we define a detection window based on the scheduling period, typically the frame duration (denoted by DT0). It is worth noticing that it is important to select a proper value of the detection window to make a good trade-off between the detection capacity and the cost. A smaller value of the detection window size results in more powerful detection capacity but extra calculation operations, and vice versa. According to the experimental results, we select the value of the detection window as $10^*\Delta T_0$.

To overcome the security vulnerabilities on bandwidth allocation in the presence of UL-BRA, RADR, serving as a non-cryptographic security patch, uses the MCDR scheme to detect UL-BRA caused by malicious WiMAX SSs in real time, whereas the mechanism uses the ATD scheme to dynamically adjust the detection threshold in order to adapt to BR dynamics. The working flow of RADR is illustrated in Fig. 2, where the MCDR scheme generates the set of all anomaly SSs, which serves as an input of the ATD scheme; the ATD scheme, on the other hand, selects a proper detection threshold to be used in the MCDR scheme.

The MCDR Scheme: According to the numerical results regarding tens of millions of calls and billions of minutes of talk time collected from hundreds of U.S. code-division multiple access (CDMA)-based cell sectors, which were located in densely populated urban areas of northern California, over a period of three weeks, the normalized cell load varied widely over time and space but had high self-similarity in the real world [7], providing a capability of modeling and predicting normal traffic. The traffic prediction in mobile WiMAX was further studied in [8]; then a dynamic bandwidth provisioning method using auto-regressive integrated moving average (ARIMA) models was proposed accordingly. Therefore, the previous work suggests that the statistics of previous bandwidth requests can be used to detect the UL-BRA. Specifically, the fluctuations of the amount of bandwidth needs from different SSs in a detection window are used to perform correlation statistics. Then the BS compares the value of the statistics with the detection threshold. If the former value is larger than the latter one, indicating the occurrence of UL-BRA, the BS treats the SS with the maximal bandwidth needs as the malicious station and enforces some necessary restoration countermeasures. As shown in Fig. 2, the MCDR scheme consists of four function blocks and one switch block, which correspond to the following steps.

Bandwidth Needs Collection: It first collects the *BR data sequences* **X**, which is defined by four parameters: index of SS (jth), scheduling period (ith), length of the detection window (m), and number of SSs (n), which are associated with the BS.

BR Data Preprocessing: Taking **X** as the input, it generates the *normalized BR data sequences* $\hat{\mathbf{Y}}$, which is obtained through calculating the mean value toward each column of the changes of bandwidth needs $\mathbf{Y} = \{y_{ij} | y_{ij} = x_{ij} - x_{(i-1)j}\}_{m \times n}$ over all SSs. Specifically, $\hat{\mathbf{Y}} = \{\hat{y}_{ij}\}_{m \times n}$, where $\hat{y}_{ij} = y_{ij} - \overline{\mathbf{Y}}_j$, and $\overline{\mathbf{Y}}_j$ is the mean value of bandwidth needs over the detection window with respect to the jth SS.

Multi-Source Correlation: It calculates the *detection statistics* **Q** based on $\hat{\mathbf{Y}}$. To be more precise, it figures out the standard deviation toward each column of **Y** when calculating **Q**, that is, $\mathbf{Q} = \{q_i | q_i = \Sigma_j(\hat{y}_{ij}^2/\sigma_j^2)\}_m$. As discussed above, the fluctuations of the bandwidth needs from SSs are considered as Gaussian random variables. Therefore, each element of **Q** is a *Chi-square variable* with n degrees of freedom [9]. The Chi-square statistic technology is regarded as an effective solution of detecting anomalous behaviors in real-time applications due to the following two reasons:

- The Chi-square statistics can properly characterize the normal distribution of each element of **Q** based on the multivariate Gaussian distribution of the fluctuations of the bandwidth needs.
- Since the time complexity of calculating and processing Chi-square statistics is low, a Chi-square-based detection approach is suitable for detecting unusual behaviors in a real-time manner, for example, the incremental anomaly detection approach proposed in [10].

Switch Block: It makes a decision whether or not a UL-BRA occurs by comparing the Chi-square statistics with detection threshold τ_{adt} (provided by the ATD scheme). If the value of an element of current **Q** statistics is larger than the threshold, a UL-BRA occurs in the probabilistic perspective. Therefore, the malicious SS can be identified by examining the index of the specific element that has the largest value, as adopted in [11]. Since the proposed RADR mechanism focuses on detecting the UL-BRA anomaly, we simply treat the SS with the maximal bandwidth needs as the malicious one in the attacking scenario illustrated in Fig. 1b. The malicious node identification and network restoration are interesting topics to be studied in future work.

Malicious Node Identification and Network Restoration: Finally, it updates the set of anomaly stations selected by the MCDR and enforces restoration countermeasures, for example, disassociating and disconnecting the malicious station, generating a security report, and alerting network operators. It is worth noting that the proposed mechanism focuses on UL-BRA detection using the statistics of bandwidth requests. The specific countermeasures toward the adversary model are beyond the scope of this article. Nevertheless, we would like to present some countermeasure examples here. For example, we can adopt a bio-inspired method to defend against Op2 in the adversary model. More details can be found in [12].

In summary, the scheme consists of three phases:

- Calculating the normalized data sequences that can be done in $O(m)$ by vector operations
- Calculating the multi-source correlation statistics that can be done in $O(mn)$
- Making a decision by comparing the statistics with the detection threshold

Thus, the time complexity of this scheme is $O(mn)$. Since the number of SSs is generally small in a metropolitan area due to intrinsic features of the WiMAX network, the scheme is approximately linear, which meets the requirement of real-time detection and restoration.

The ATD Scheme — In practical usage, 802.16 WiMAX networks experience BR dynamics due to white noise, random signal jitters, and normal bandwidth contention when multiple uplink flows are present. On the other hand, the performance of RADR highly depends on the detection threshold selection. A larger value of the detection threshold induces a higher false negative rate but a lower false positive rate, and vice versa. Hence, the selection of an appropriate threshold is also important for the performance of MCDR. Therefore, we further propose the ATD scheme to dynamically adjust the detection threshold to adapt to BR dynamics. As shown in Fig. 2, the ATD scheme selects the threshold by combining multi-source correlation statistics based on normal BR data sequences with the Chebyshev inequality [11]. With a confidence level of $(1 - 1/k^2)$, the threshold is selected as τ_{adt}, which depends on the Chi-square statistics $\mathbf{Q}^*$ and the configurable nonzero constant k. Similarly, the time complexity of the scheme is also approximately linear due to the fact that the number of SSs is generally small.

Extension to Multihop Relay Case

It is well known that an increase of the transmission range of stations will lead to a decrease of signal quality, resulting in a decrease of network capacity [13]. Thus, the contradiction between wide-range network coverage and high network capacity makes the practical usage of WiMAX a challenge in a wireless metropolitan area. Similar to the mesh networking specified in the IEEE 802.11-2012 standard [14], IEEE 802.16 and the WiMAX Forum released relay enhanced WiMAX [2] to overcome the challenge. Although the RADR mechanism in this article is designed for conventional OFDM WiMAX, it makes sense in the multihop relay case as well. Specifically,

Parameters	Values	Parameters	Values
Total number of subcarriers	256	Number of used subcarriers	200
Channel bandwidth	5 MHz	Sampling factor	144/125
Sampling frequency	5.76 MHz	Useful symbol time	44.4 μs
Ratio of cyclic prefix (CP) time to useful symbol time	1/4 or 1/8 or 1/16 or 1/32	Ratio of downlink time to frame duration	0.2
Queue type	PriQueue	Maximal queue length	50
Required receiving power	–30 dBm	Maximal transmitting power	83 dBm
Height of transmitting antenna	1.5 m	Height of receiving antenna	1.5 m
Transmitting/receiving gain	1.0	Path loss exponent	4
Frame duration	5 ms	Propagation model	TwoRayGround

Table 1. Summary of simulation parameters.

we first construct a decision tree consisting of the BS, relay stations (RSs), and SSs from the security association point of view. Then we patch RADR to the root (i.e., the BS) and all intermediate nodes (i.e., RSs) of the tree. Finally, the root and intermediate nodes run RADR independently to detect malicious child nodes. In practical usage in the multihop relay case, the merits of RADR stem from two aspects: first, it is able to detect malicious stations locally by means of hierarchical deployment and distributed operation, which makes RADR robust to the transmission delay introduced by the RSs; and second, the overhead of RADR is low because the number of stations in the local decision domains is much smaller than the network size.

Evaluation

Setup

Due to various constraints, we use network simulator ns2 (v2.31) for simulations and evaluate network performance in terms of uplink network throughput (megabits per second), detection accuracy, and false positive rate. We implemented data structures and protocols of an OFDM WiMAX network operating in TDD mode to facilitate all simulations of the fixed broadband wireless network. We also implemented the malicious behavior of sending customized BR messages and RADR into the scheduler modules of abnormal SSs and the scheduler module of the BS, respectively. Furthermore, the BS granted bandwidth requests in RR when multiple SSs simultaneously transmitted data packets.

The evaluated network consists of a BS, four SSs, and a sink node. The BS connects with SSs via 802.16 wireless links, whereas it connects with the sink node via a duplex wired link. For the sake of simplicity without loss of generality, node SS4 is a mobile node, while other nodes are stationary in the simulations. Specifically, the moving space of SS4 is specified to be a rectangle with a length of 200 m and a width of 50 m in order to simulate a real mobile scenario where a car typically moves around an urban block. The parameters corresponding to the duplex wired link are wired link bandwidth, delay, and queue type, respectively. In the simulations, SS1 and SS4 are normal SSs, whereas SS2 and SS3 are malicious ones. The start time and stop time of the default data flow originating from SS1 are 20 s and 60 s, respectively, whereas the start time of the second flow originating from SS4 is set to 70 s. The destinations of both data flows are set to the sink node. To simulate complex and changeable flows, the source node SS1 originates User Datagram Protocol (UDP)/exponential (EXP) flows with a packet size of 2500 bytes, a burst time of 2 s, an idle time of 1 s, and a burst peak rate of 20 Mb/s. On the other hand, node SS4 originates UDP/constant bit rate (CBR) flows with a packet size of 2500 bytes and a transmission interval of 0.001 s. Moreover, SS2 launches the UL-BRA threat at simulation time 40 s, while SS3 performs UL-BRA at a random value of time between 30 s and 40 s. For simplicity, all WiMAX stations operate based on the same air interface specification. Each simulation lasts 100 s, and the maximal transmission range of WiMAX stations is 1000 m. An omni-antenna is used as the antenna model, and Destination Sequence Distance Vector (DSDV) protocol [15] is adopted to function as the routing protocol. More parameters are shown in Table 1. On the other hand, we consider seven types of modulation and coding schemes as specified in the standard [2]:

- OFDM BPSK_1_2: It denotes overall coding rate 1/2 and modulation type binary phase shift keying (BPSK).
- OFDM QPSK_1_2: It refers to overall coding rate 1/2 and modulation type quadrature phase shift keying (QPSK).
- OFDM QPSK_3_4 It represents overall coding rate 3/4 and modulation type QPSK.
- OFDM 16QAM_1_2: It denotes overall coding rate 1/2 and mudulation type quadrature amplitude modulation (QAM).
- OFDM 16QAM_3_4: It refers to overall coding rate 3/4 and modulation type 16-QAM.
- OFDM 64QAM_2_3: It refers to overall coding rate 2/3 and modulation type 64-QAM.
- OFDM 64QAM_3_4: It represents overall coding rate 3/4 and modulation type 64-QAM.

We present results that demonstrate the effectiveness of the proposed mechanism in two cases. First, we examine the adaptation of the detection threshold regarding different network loads by changing the number of data flows in the network. Then we suppose that both SS1 and SS4 transmit data flows to the sink node, and evaluate the performance regarding different numbers of malicious nodes.

Performance Comparison with Respect to Different Parameter Settings

Figures 3a and 3b illustrate the adjustment of the detection threshold in two cases: the number of data flows is fixed during simulations, and the number of data flows changes along with simulation time. In both cases, the modulation and coding scheme was selected as OFDM 64QAM_3_4, and the ratio of CP time to useful symbol time was set to 1/8. Furthermore,

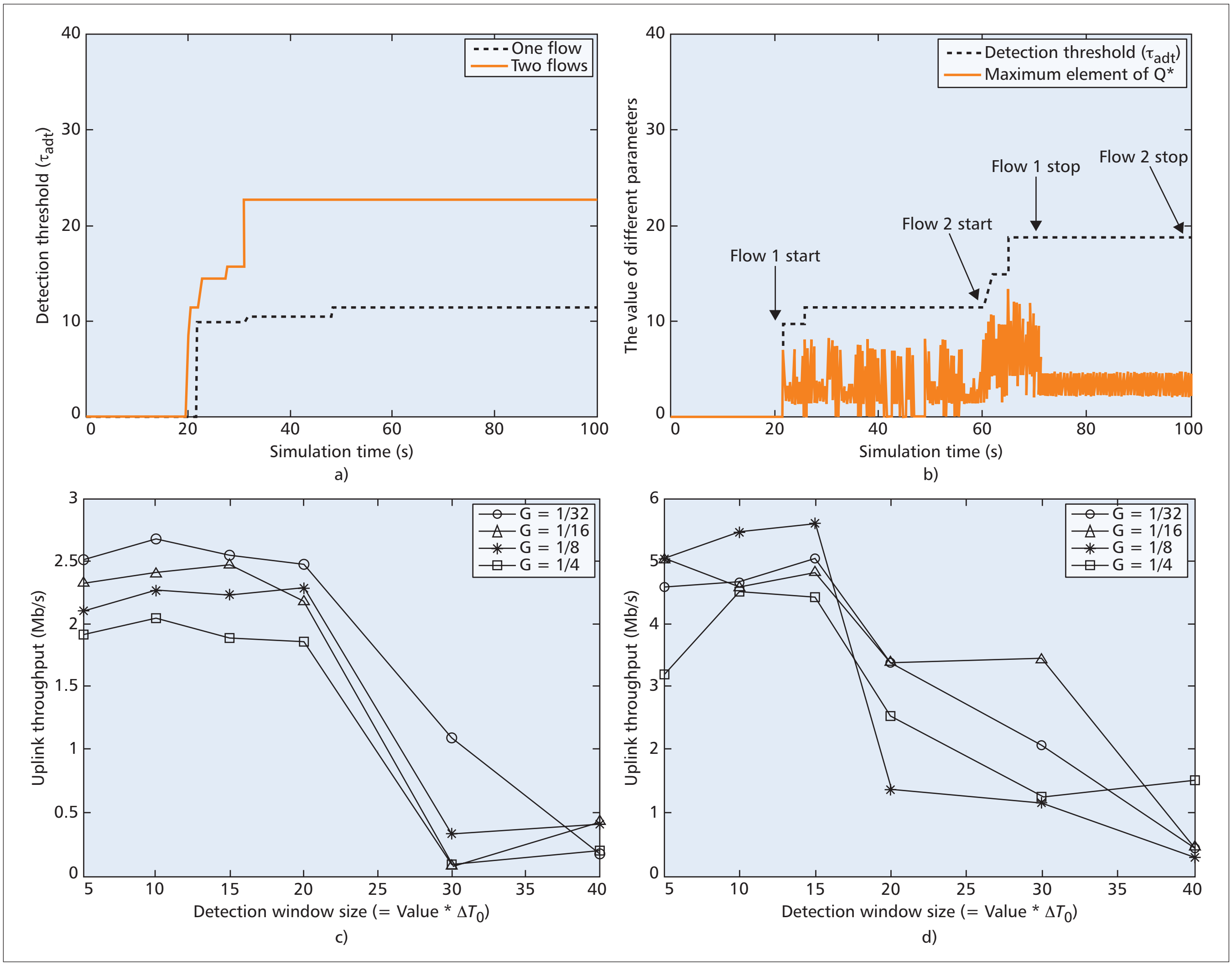


Figure 3. Performance comparison with respect to different parameter settings: a) adaptation of the detection threshold (fixed number of data flows); b) adaptation of the detection threshold (varied number of data flows with time); c) performance comparison with respect to different sizes of the detection window (OFDM QPSK_3_4); d) performance comparison with respect to different sizes of the detection window (OFDM 64QAM_3_4).

both data flows start at simulation time 20 s in the former case, while in the latter case, the start time and stop time of the default data flow was 20 s and 70 s, respectively, whereas the start time of the second flow was set to 60 s. As shown in Fig. 3, no matter if the number of data flows is fixed or not, the proposed threshold determination scheme is able to adjust the threshold adaptively. Specifically, the results of Fig. 3a show that the threshold under two data flows is higher than that under one data flow. The reason is that the BS grants BR of these two data flows in RR, resulting in a larger change of requested bandwidth from different SSs in a detection window. On the other hand, we see in Fig. 3b that the Chi-square statistics **Q*** dynamically adjusts along with the changes of BR needs induced by the appearance and disappearance of two data flows in the network. Note that there are more fluctuations of the maximum element of **Q*** in the time period of (20 s, 60 s) compared to those in the time period of (70 s, 100 s). The reason is that the EXP flow1 is a changeable flow, resulting in larger changes of **Q***. Nevertheless, the detection threshold also adapts to these changes accordingly via the proposed threshold determination scheme. The above results demonstrate that the RADR mechanism can effectively adapt to BR dynamics.

On the other hand, it is important to determine a proper value of the detection window. For ease of explanation, we select two representative modulation and coding schemes, OFDM QPSK_3_4 and 64QAM_3_4, to examine the change of uplink throughput along with different sizes of the detection window. Figures 3c and 3d show the comparative results of uplink throughput with respect to different sizes of the detection window in the presence of the UL-BRA threat, where the symbol *G* refers to the ratio of CP time to useful symbol time. According to the results, it is recommended to select the detection window size from [5*ΔT_0, 15*ΔT_0]. Therefore, we select the value of the detection window as 10*ΔT_0 in the following experiments.

Performance Improvement after Patching the Proposed Mechanism

For the convenience of performance comparison, we carried out three groups of simulations as follows:

- RADR is deactivated, and the UL-BRA threat occurs (denoted by UL-BRA = ON, RADR = OFF).
- RADR is activated, and the UL-BRA threat occurs (denoted by UL-BRA = ON, RADR = ON).
- RADR is deactivated in the normal case (denoted by UL-BRA = OFF, RADR = OFF).

Note that the results of the last group of simulations serve as the baseline in performance comparison.

All simulations were based on the same settings of the fol-

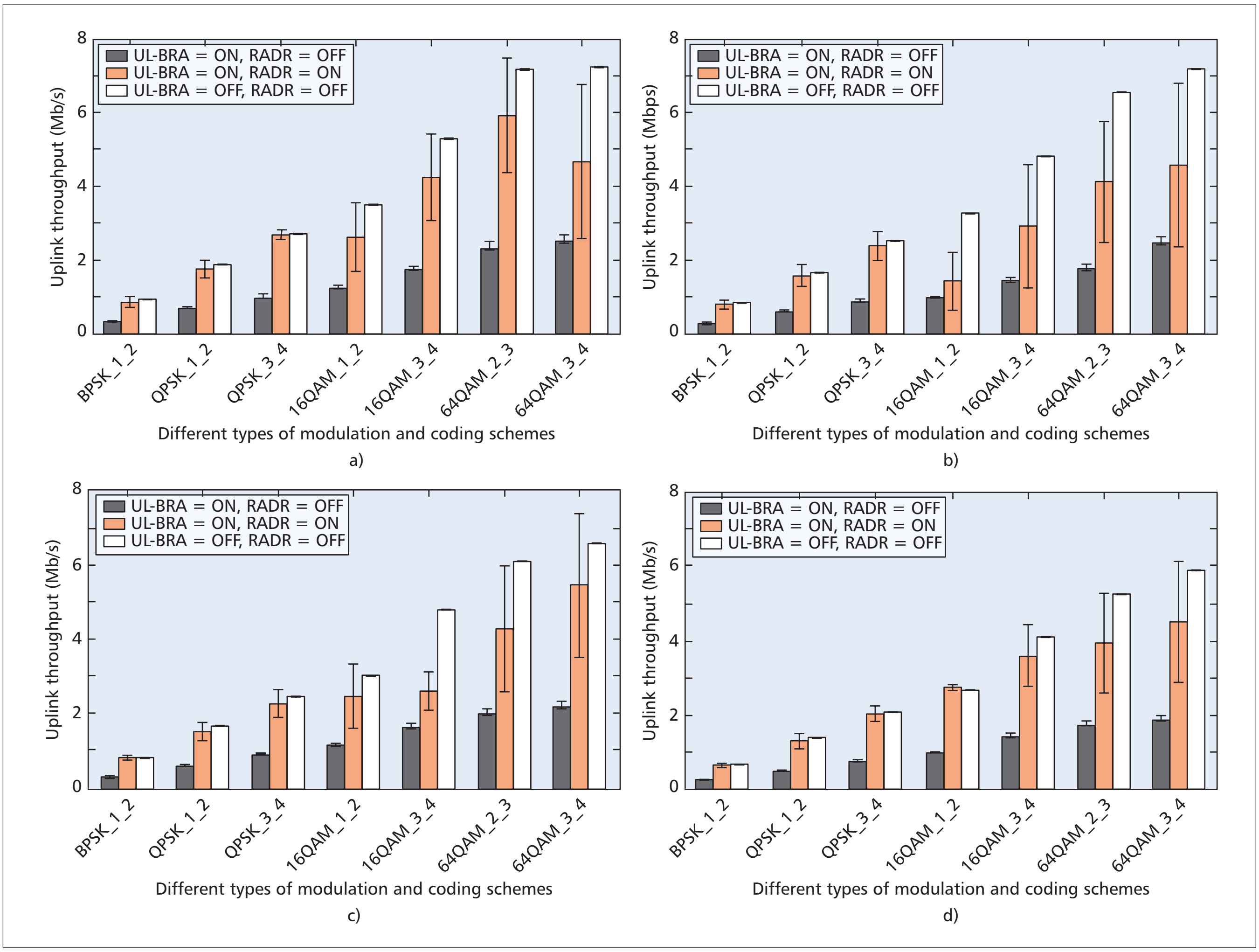


Figure 4. Performance comparison under different settings of UL-BRA and RADR: a) G = 1/32; b) G = 1/16; c) G = 1/8; d) G = 1/4.

lowing parameters. The start time and stop time of the default data flow are 20 s and 60 s, respectively, whereas the start time of the second flow is set to 70 s. The modulation and coding scheme was selected from seven options as described before. The ratio of CP time to useful symbol time (denoted by G) was selected from {1/32, 1/16, 1/8, 1/4}. Each data bar and corresponding error bar in Fig. 4 refer to the average value of uplink throughput (megabits per second) and the error distance over 20 independent runs. We find in Fig. 4 that when the UL-BRA threat occurs, no matter what the modulation and coding scheme is and which value of parameter G is selected, the uplink throughput after patching RADR significantly outperforms that before patching. Furthermore, we can draw another conclusion from the performance comparison between the results of UL-BRA = ON, RADR = ON with the baseline results: that the proposed mechanism is able to restore the performance of the evaluated network to the normal level.

We can also see in Fig. 4 that the uplink throughput experiences more fluctuations along with a higher efficiency of modulation and a smaller value of G. The reason is that higher efficiency of modulation and a smaller value of G introduce a larger amount of bits per uplink subframe. Then the change of requested bandwidth from different SSs in a detection window becomes even greater when two data flows change during simulations, resulting in a higher value of the detection threshold and a greater false negative rate. Therefore, some instances of UL-BRA evade the detection of RADR. However, RADR is still effective to enhance the uplink network throughput in these cases.

Numerical Results of the Proposed Mechanism in Different Network Sizes

To justify the advantages of the proposed scheme, we further conducted more simulations under different settings of the network size. Specifically, we added more SSs to the evaluated network, resulting in five different settings of the network size, which are 5, 10, 15, 20, and 25 SSs. The adversary stations were randomly selected from SSs with a probability of 0.3 except for SS1 and SS4, which originated a normal UDP/CBR flow and a normal UDP/EXP flow, respectively. The modulation and coding scheme was selected as OFDM 64QAM_3_4, and the value of G was set to 1/8. Furthermore, we adopted four metrics to evaluate the performance of RADR: uplink throughput, detection accuracy, true positive rate (TPR), and false positive rate (FPR). Here, the detection accuracy is defined by $(TP + TN)/(TP + TN + FP + FN)$, the TPR is calculated by $TP/(TP + FN)$, and the FPR is calculated by $FP/(TP + FP)$, where TP, TN, FP, and FN are true positives, true negatives, false positives and false negatives, respectively. In each group of simulations, we ran independent trials for 20 times to get average results.

Figure 5 shows the numeric results of RADR under different settings of the network size, where the results in Fig. 5a with respect to "UL-BRA = OFF, RADR = OFF" are the baseline results. We see from Fig. 5a that no matter what the

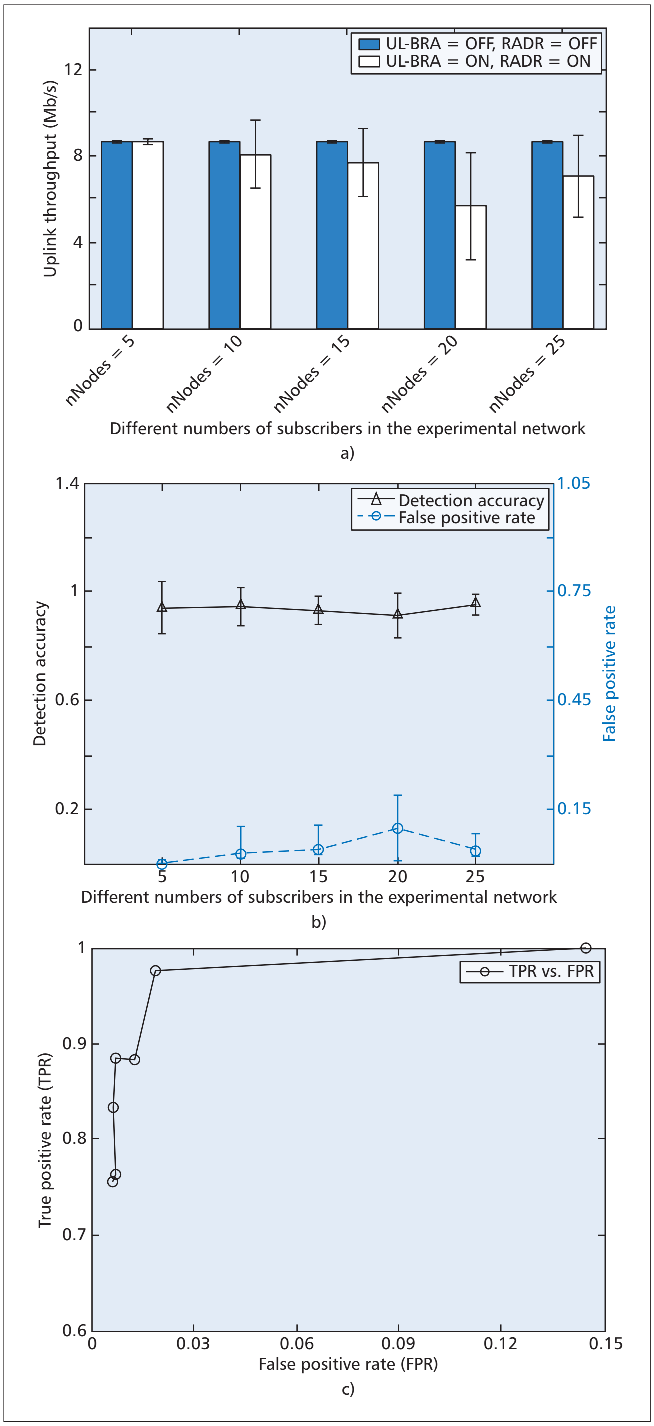


Figure 5. Numerical results of RADR under different settings of the network size: a) performance comparison in terms of uplink throughput; b) performance comparison in terms of detection accuracy and false positive rate; c) results of true positive rate vs. false positive rate, where *nNodes* = 10, G = 1/8.

network size is, the proposed RADR can maintain the network performance compared to the baseline results in terms of uplink throughput, which is consistent with the above results. Moreover, we conclude from Fig. 5b that under different settings of network size, the average results of the detection accuracy and the FPR are more than 0.9 and less than 0.15, respectively. To clearly evaluate the overall performance of the proposed scheme, we particularly analyze the relationship between the TPR and the FPR. Taking a network with 10 SSs as an example, Fig. 5c illustrates the average changes of TPR along with the increase of FPR, where G = 1/8. We can see from Fig. 5c that RADR achieves more than 90 percent TPR when the FPR is near 2 percent, demonstrating its superior detection performance. The above results show that the proposed scheme is still valid with different network scales, and it achieves high detection accuracy but relatively low false positive rate with the presence of adversary stations.

Conclusions

In this article, we have identified the UL-BRA threat that exploits security vulnerabilities in bandwidth allocation and request mechanisms in the IEEE 802.16 standard. Then we have proposed a security patch incorporating the RADR mechanism in order to improve the resilience of 802.16 WiMAX networks against the UL-BRA threat. Specifically, the MCDR and ATD schemes have been proposed to detect UL-BRA caused by malicious WiMAX SSs and to dynamically adjust the detection threshold due to normal BR fluctuations in real time. The results show that the proposed mechanism is effective to detect the existence and eliminate the impacts of UL-BRA, resulting in a normal level of network performance regardless of the threat. In the next step, the work in this article can serve as a reference for researchers, engineers, and service providers to protect 3GPP LTE against similar security threats.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (Grant Nos. 61170287, 61232016, 61070198 and 61379145), the PAPD, and CICAEET.

References

[1] Y. Li *et al.*, "Overview of Femtocell Support in Advanced WiMAX Systems," *IEEE Commun. Mag.*, vol. 49, no. 7, 2011, pp. 122–30.
[2] IEEE Std 802.16TM-2012, "IEEE Standard for Air Interface for Broadband Wireless Access Systems," 2012.
[3] A. Oliveira *et al.*, "Packet Dispersion Techniques over WiMAX Links: Challenges and Problems," *IEEE Commun. Mag.*, vol. 51, no. 3, 2013, pp. 154–59.
[4] R. D. Pietro, and G. Oligeri, "Silence is Golden: Exploiting Jamming and Radio Silence to Communicate," *ACM Trans. Info. Sys. Security*, vol. 17, no. 3, 2015, pp. 9:1–24.
[5] M. Wilhelm *et al.*, "Short Paper: Reactive Jamming in Wireless Networks: How Realistic Is the Threat?," *Proc. ACM WiSec '11*, 2011, pp. 47–52.
[6] C. So-In, R. Jain, and A.-K. Tamimi, "A Deficit Round Robin with Fragmentation Scheduler for IEEE 802.16e Mobile WiMAX," *Proc. 2009 IEEE Sarnoff Symp.*, 2009, pp. 1–7.
[7] D. Willkomm *et al.*, "Primary User Behavior in Cellular Networks and Implications for Dynamic Spectrum Access," *IEEE Commun. Mag.*, vol. 47, no. 3, 2009, pp. 88–95.
[8] H.-W. Kim *et al.*, "Dynamic Bandwidth Provisioning Using ARIMA-Based Traffic Forecasting for Mobile WiMAX," *Computer Commun.*, vol. 34, no.1, 2011, pp. 99–106.
[9] D. S. Moore, G. P. McCabe, and B. A. Craig, *Introduction to the Practice of Statistics*, 6th ed., W. H. Freeman and Co.y, 2007.
[10] Y. Fang, O. A. Omitaomu, and A. R. Ganguly, "Incremental Anomaly Detection Approach for Characterizing Unusual Profiles," *LNCS 5840: Knowledge Discovery from Sensor Data*, 2010, pp. 190–202.
[11] Z. R. Zaidi *et al.*, "Real-Time Detection of Traffic Anomalies in Wireless Mesh Networks," *Wireless Net.*, vol. 16, no. 6, 2010, pp. 1675–89.
[12] Q. Liu, J. Yin, and S. Yu, "A Bio-Inspired Jamming Detection and Restoration for WMNs: In View of Adaptive Immunology," *Proc. CSS, LNCS 8300*, 2013, pp. 243–57.
[13] Y.-H. Lee *et al.*, "The Measurement and Analysis of WiMAX Base Station Signal Coverage," *Progress In Electromagnetics Research C*, vol. 25, 2012, pp. 223–32.
[14] IEEE Std 802.11TM-2012, "IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2012.
[15] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. SIGCOMM*, 1994, pp. 234–44.

Biographies

QIANG LIU [M] (libra6032009@gmail.com) received his Ph.D. degree in computer science and technology from the National University of Defense Technology, Changsha, China, in 2014. He has contributed several archived journal papers and international conference papers in publications including *IEEE Transactions on Wireless Communications*, *IEEE Communications Letters*, *Neural Computing and Applications*, and so on. He was invited as a TPC member of Chinacom '14 and a Session Chair of HPCC '13. He is a member of the China Computer Federation (CCF). His research interests include protocol design and performance evaluation, machine learning, denial-of-service detection, as well as other security issues in emerging wireless networks.

XIPING HU (xipingh@bravolol.com) is the co-founder and CTO of Bravolol Limited in Hong Kong, a leading language learning mobile application company with over 70 million accumulated downloads and more than 6 million monthly active users, and listed as the top 2 language education platform globally according to the report of App Annie in May 2015. He is the winner of silver prizes in national Olympic competitions in mathematics and physics in China, and a Microsoft certified specialist in web applications, .NET Framework, and SQL server. Also, he participated as a key member in several research projects, like web service security identification at Tsinghua University in China, SAVOIR project at National Research Council of Canada — Institute for Information Technology (NRC-IIT), and NSERC DIVA strategy research network at the University of British Columbia (UBC). As first author, his research contributions have been published and presented in approximately 20 international conferences and journals, such as *HICSS*, *IEEE Transactions on Emerging Topics in Computing*, *IEEE Communications Magazine*, *ACM Transactions on Multimedia Computing, Communications, and Applications*, and ACM MobiCom. His research areas are mobile social networks, mobile systems and application, mobile/service/cloud computing, and crowdsourced-sensing. He holds a Ph.D. in electrical and computer engineering from UBC.

EDITH C.-H. NGAI (edith.ngai@it.uu.se) is currently an associate professor in the Department of Information Technology, Uppsala University, Sweden. She received her Ph.D. from the Department of Computer Science and Engineering, Chinese University of Hong Kong in 2007. She did her postdoctoral work at Imperial College London, United Kingdom in 2007–2008. She has been a visiting scholar at the University of Caifornia at Los Angeles, Simon Fraser University, and Tsinghua University. Her research interests include wireless sensor and mobile networks, information-centric networking, QoI-aware data collection, Internet of Things, and network security and privacy. She has been a TPC member for many networking and communication conferences, including IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE DCOSS, IEEE LCN, IEEE CloudCom, and so on. She was a TPC Co-Chair of the Swedish National Computer Networking Workshop (SNCNW'12), Publicity Co-Chair of IEEE MSN '12, and Web Chair of IWQoS '14. Her co-authored papers received best paper runner-up awards at IWQoS '10 and IPSN '13. She is a VINNMER Fellow (2009) awarded by VINNOVA, Sweden.

MIN LIANG (gzliangm@cn.ibm.com) is an chief architect for IBM China Global Technology Services and a core leader of the Greater China Group big data research community. He has regional responsibility for cloud computing services, big data and analytic services, mobility services, and smarter city project delivery. He holds a Master's degree in information technology from the University of South Australia.

VICTOR C. M. LEUNG [F] (vleung@ece.ubc.ca) is a professor of electrical and computer engineering and holds the TELUS Mobility Research Chair at UBC. His research is in the areas of wireless networks and mobile systems. He has co-authored more than 800 technical papers in book chapters, archival journals, and refereed conference proceedings, several of which have won best-paper awards. He is a Fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada. He is serving/has served on the Editorial Boards of *IEEE JSAC*, *IEEE Transactions on Computers*, *IEEE Wireless Communications*, *Vehicular Technology*, *Wireless Communications Letters*, and several other journals. He has provided leadership to the Technical Program Committees and Organizing Committees of numerous international conferences. He was the recipient of the 1977 APEBC Gold Medal, NSERC Postgraduate Scholarships from 1977 to 1981, a 2012 UBC Killam Research Prize, and an IEEE Vancouver Section Centennial Award.

ZHIPING CAI (zpcai@nudt.edu.cn) [M'08] received his Ph.D. degree in computer science and technology from the National University of Defense Technology (NUDT), Changsha, China, in 2005. He is an associate professor of the College of Computers, NUDT. His current research interests include network security and network virtualization.

JIANPING YIN (jpyin@nudt.edu.cn) received his Ph.D. degree in computer science and technology from NUDT in 1990. He is a professor with the College of Computers, NUDT. He currently holds the positions of dean of the Department of Computer Science and Technology and head of the China Computer Federation Technical Committee on Theoretical Computer Science. His research interests include artificial intelligence, network algorithms, and information security.