Security Considerations for Handover Schemes in Mobile WiMAX Networks

Junbeom Hur*, Hyeongseop Shim*, Pyung Kim*, Hyunsoo Yoon*, Nah-Oak Song†
*Division of Computer Science,
†Mobile Media Platform Center,
Korea Advanced Institute of Science and Technology,
373-1, Guseong-dong, Yuseong-gu, Daejeon 305-701, Republic of Korea
Email: {jbhur, hsshim, pkim, hyoon}@nslab.kaist.ac.kr, nsong@mmpc.kaist.ac.kr

Abstract—IEEE 802.16e uses EAP-based authentication and key management for link layer security. Due to the lack of ability to support mobility, however, EAP-based key management becomes a principal impediment to the achievement of an efficient and secure handover in IEEE 802.16e mobile WiMAX networks. In this paper, an overview of the EAP-based handover procedures of the latest IEEE 802.16e standard is given and their security flaws are analyzed. Possible solutions for secure handover in IEEE 802.16e networks are also proposed in this paper. The proposed handover protocol guarantees a backward/forward secrecy while gives little burden over the previous handover protocols.

I. INTRODUCTION

Mobile WiMAX (Worldwide Interoperability Microwave Access) is a wireless networking system based on the IEEE 802.16e standard [1]. Developing IEEE 802.16e aims to amend previous standard IEEE 802.16-2004 [2] and provide mobility in broadband wireless access. The latest revised version of IEEE 802.16e [3], which is a revision of IEEE 802.16-2004 as amended by IEEE 802.16-2004/Cor1-2005 [1], also supports the mobility of a mobile station (MS). In the IEEE 802.16e standard, three basic types of handover are specified for portability and simple/full mobility of users: Hard Handover (HHO), Macro Diversity Handover (MDHO), and Fast Base Station Switching (FBSS). HHO is mandatory in WiMAX systems. Other two types of handover are optional.

IEEE 802.16e uses Extensible Authentication Protocol (EAP) as an authentication procedure and key management for link layer security as well as an RSA-based authentication procedure. Due to the flexibility and ability to interact with Authentication, Authorizing, Accounting (AAA) infrastructures, it is very likely that EAP will become the de facto authentication method for 802.16e access control [4]. However, EAP lacks the ability to support MS mobility or to deal with the need for an MS to quickly extend its session before the initially authorized session expires. As a full EAP authentication latency requires about 1000 ms [5], every full authentication per handover cannot support mobile WiMAX applications such as video conference or streaming data. According to the latency/jitter guideline identified by the WiMAX Forum to assure a quality user experience, the latency should not exceed about 50 ms in VoIP or video conference, and 100 ms in streaming media [6].

In anticipation of a handover, an MS may seek to use pre-authentication to facilitate an accelerated reentry at a particular target base station (BS). Pre-authentication results in establishment of an authorization key (AK) in the MS and target BS. Even if the specific mechanism for pre-authentication is out of the scope of IEEE 802.16e [3], it is clear that the enhanced Privacy Key Management protocol version 2 (PKMv2) proposed in the standard may not be suitable to the secure pre-authentication procedure since secret information are supposed to be shared among neighbor BSs in the current PKMv2 protocol.

In this paper, an overview of handover procedures proposed in IEEE 802.16e standard is given and their security flaws are analyzed. Possible solutions for secure handover in mobile WiMAX networks are also proposed. To solve the security problem, the key management of PKMv2 is slightly modified and a pre-authentication scheme is proposed based on the modified key hierarchy. The proposed pre-authentication scheme enables the MS to establish a unique authorization key with each neighbor BS, or with each BS in the diversity set before handover. The proposed scheme guarantees a backward and forward secrecy while gives little burden over the handover procedures in IEEE 802.16e. The backward secrecy implies that the target BS should not access to the communications that have been exchanged between the MS and the previous serving BS. The forward secrecy implies that the serving BS should not be able to access to the communications that will be exchanged between the MS and the target BS.

The paper is organized as follows. In Section II, we describe the IEEE 802.16e PKMv2 key management and handover mechanisms. In Section III, we propose a modified key management and secure pre-authentication schemes for mobile WiMAX networks. In Section IV, we analyze the performance and security of the proposed scheme compared with the PKMv2-based handover schemes of IEEE 802.16e, and remark the conclusion of the paper in Section V.

II. OVERVIEW OF IEEE 802.16E HANDOVER AND SECURITY CONSIDERATION

IEEE 802.16e security sub-layer includes two component protocols: an encapsulation protocol for securing data packet and a privacy key management (PKM) protocol providing...
the secure distribution of keying material from the BS and the MS. There are two privacy key management protocols supported in IEEE 802.16e: PKMv1 and PKMv2. PKMv1 is a subset of PKMv2 in function. PKMv2 offers more enhanced features such as new key hierarchy, AES-CCM, AES key wrap algorithm, and multicast and broadcast service (MBS). Thus, the security of the IEEE 802.16e is introduced in term of the PKMv2 in this paper.

A. Privacy Key Management Protocol

There are two main authentication schemes defined in PKMv2 of IEEE 802.16e, one based on RSA and the other based on EAP. Thus, there are two primary sources of keying material defined in PKMv2. To choose both or one of them as the authorization mechanism is decided by basic capabilities negotiation procedure at the initial network entry. In this paper, we focus on the EAP-based authorization, especially single EAP mode for simplicity. The root of the key hierarchy in the EAP authentication mode is the master session key (MSK). The EAP-based authentication process yields the MSK, then the other keys such as the key encryption key (KEK) and HMAC/CMAC key are derived from the MSK.

The flow of message exchange and key derivation/delivery procedure using the EAP-based authentication mode are described in Fig. 1. At the initial entry, the MS and the authentication server (AS) mutually authenticate each other using the EAP-based authentication scheme. The EAP authentication should fulfill the mandatory criteria listed in [7] such as the mutual authentication support and protection against the man-in-the-middle attack. EAP-PSK and EAP-AKA are recommended in IEEE 802.16e [3], and EAP-PEAP is recommended in [8].

The product of the EAP exchange is the 512-bit MSK, which is transferred to IEEE 802.16 layer and known to the AS and the MS. MSK is then transferred to the authenticator, that is the BS, from the AS. In the IEEE 802.16e standard, the message for the MSK distribution is not defined. Thus, an Access Accept message is assumed to take the role of the distribution in this paper. The MS and the BS then derive a pairwise master key (PMK) by truncating the MSK to 160 bits, and derive an authorization key (AK) from the PMK. The generation process is shown as follows:

\[
PMK = \text{Truncate}(\text{MSK}, 160),
\]

\[
AK = \text{Dot16KDF}(\text{PMK, MS MAC Address})
\]

The Dot16KDF algorithm [3] is a counter (CTR) mode construction which is used to derive an arbitrary amount of keying material from source keying material. BSID denotes the identification of the BS, and | denotes a concatenation in (1).

After deriving the AK, both of the BS and the MS can derive a shared KEK and HMAC/CMAC key from the AK. Then the BS and the MS perform the 3-way handshake to negotiate and distribute keying parameters related to all security associations (SA) between them. The 3-way handshake is executed at the initial network entry or at the re-entry procedure such as at a handover. The flow in SA-TEK 3-way handshake is shown as follows:

1) PKMv2 SA-TEK-Challenge message (MS ← BS): BS_Random, AK sequence number, AKID, PMK life time, HMAC/CMAC digest
2) PKMv2 SA-TEK-Request message (MS → BS): MS_Random, BS_Random, AK sequence number, AKID, security capabilities, security negotiation parameters, HMAC/CMAC digest
3) PKMv2 SA-TEK-Response message (MS ← BS): MS_Random, BS_Random, AK sequence number, AKID, [SA-TEK-Update], frame number, SAdescriptor, security negotiation parameters, PKMv2 configuration settings, HMAC/CMAC digest

The integrity of all the 3-way handshake messages are protected by the HMAC/CMAC digest against a forgery attack. It is important to note that the SA-TEK-Update is included in the message 3) only at re-entry procedure, which contains all the keying materials for the traffic encryption key (TEK) update and distribution. SA-TEK-Update is encrypted with the KEK. The 3-way handshake provides the following security guarantees:

- Full mutual authentication.
- Message 2) indicates to the MS that the MS is alive and that the MS possesses the AK.
- Message 3) indicates to the MS that the BS is alive
- MS is guaranteed that SA-TEK-Update is sent by the BS and is fresh.

After a successful authorization, the MS dynamically requests parameters for dynamic SAs including old and new TEKs to the BS for securing data packets. In a network
environment where the multicast and broadcast service (MBS) is supported, additional group key (GTEK) generation and delivery process is performed optionally after the TEK distribution procedure.

B. Handover and Security Settings

As mentioned in Section I, IEEE 802.16e defines three types of handover: HHO, MDHO, and FBSS. MDHO and FBSS can be called soft handovers [11].

1) HHO: In HHO, the MS communicates with just one BS in each time. All connections with the old BS (called serving BS) are broken before the connection to a new BS (target BS) is established. The BS periodically broadcasts a neighbor advertisement message, MOB_NBR-ADV, for identification of the network. The MOB_NBR-ADV message includes the information for the neighbor BSs such as the number of neighbor BSs and their BSIDs. After scanning neighbor BSs identified by BSIDs in the MOB_NBR-ADV message, the MS switches its link to the selected target BS, and executes ranging, authentication, and finally registers with the target BS. This type of HO is less complex, fairly simple but it has high latency which is typically on the order of 100ms or more [9]. For the HO optimization, IEEE 802.16e suggests different HO scenarios with three different security settings of HO optimization bit #1 and #2 in the RNG-RSP message as described in Table I.

<table>
<thead>
<tr>
<th>Optimization Bit</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit#1=0 and Bit#2=0</td>
<td>Perform re-authentication and SA-TEK 3-way handshake.</td>
</tr>
<tr>
<td>Bit#1=1 and Bit#2=0</td>
<td>Re-authentication is not performed. TEKs for all SAs are updated.</td>
</tr>
<tr>
<td>Bit#1=1 and Bit#2=1</td>
<td>Re-authentication and SA-TEK 3-way handshake are not performed. (All the TEKs received from the serving BS are reused.)</td>
</tr>
</tbody>
</table>

2) MDHO: In MDHO, the MS and the BS maintain a diversity set, which is a list of the BSs involved in the handover procedure. The MS continuously monitors the BSs in the diversity set and registers with one of the BSs in the diversity set, that is an anchor BS. For downlink, two or more BSs transmit data to the MS such that diversity combining can be performed at the MS. For uplink, the MS transmission is received by multiple BSs and selection diversity of the received information is performed. BSs involved in MDHO are required to share or transfer MAC context, which includes current authentication and encryption keys associated with the connections.

3) FBSS: In FBSS, the diversity set is maintained by the MS and the BS like in MDHO. However, the MS communicates only with the anchor BS for all types of uplink and downlink traffic. The anchor BS can be changed from frame to frame depending on a BS selection scheme. BSs involved in FBSS are also required to share or transfer MAC context, which includes current authentication and encryption keys associated with the connections.

C. Security Analysis of IEEE 802.16e Handover Schemes

As shown in Table I, each HO scenario supports different level of security and handover efficiency. There is a trade-off between them. In case of Bit#1=1 and Bit#2=1, all secret keys used before the handover will be reused after the handover. This creates the domino effect [4], which means that if the security of one BS is compromised, it can lead to the security compromise of all the previous BSs (backward secrecy) and following BSs (forward secrecy). In case of Bit#1=1 and Bit#2=0, TEKs are updated but AKs are not updated due to the omission of re-authentication procedure. This scenario cannot guarantee the forward secrecy since a serving BS can decrypt the updated TEKs for all the following target BSs using the unchanged KEK derived from the unchanged AKs. Therefore, to guarantee a secure sharing of the keying materials for secure communications, both of the optimization bit #1 and #2 should be set to 0 so that the re-authentication and SA-TEK 3-way handshake are performed upon a handover.

Clearly, the MDHO and FBSS are also vulnerable to the domino effect since all the MS and the BSs in the diversity set share the same secret keys. To prevent the domino effect, a secret key should not be reused in other BSs. Therefore, an efficient SA re-establishment scheme is needed to guarantee the backward and forward secrecy upon a handover while reducing the delay associated with the SA establishment.

III. PROPOSED SCHEME FOR SECURE HANDOVER

The EAP framework does not provide a support for low latency security establishments during a handover and re-authentication. To reduce the delay associated with the SA re-establishment, many network architectures including the IEEE 802.16e working group and several schemes such as [10] have chosen to transfer the link security keys from one BS to the next. However, those approaches cannot guarantee the backward or forward secrecy.

Even if IEEE 802.16e specification does not define a pre-authentication scheme, it considers the use of the pre-authentication mechanism to facilitate an accelerated re-entry
2. The PMK and AK are generated as follows: PMK is delivered to the corresponding BS as shown in Fig. 3(a). In the proposed scheme, the PMK generation is performed to prevent any security degradation. Additionally, the AS is assumed to know the neighbor BSs of each BS.

A. Pre-authentication for Handover

As shown in Fig. 1, the MSK of an MS is delivered to the serving BS from the AS. This MSK delivery, however, cannot be adopted to design a secure pre-authentication procedure. Since the MSK is the root of the key hierarchy and it does not bind the BSID and the identification of the MS, any BS that received the MSK from the AS can derive the PMKs and AKs of other neighbor BSs using (1) with the known identifications of the BSs and the MS, and the received MSK. Thus, for a secure pre-authentication, a unique key which binds the BSID and the MAC address of the MS should be generated by the AS securely, and delivered to the corresponding BS instead of the MSK. In the proposed scheme, the PMK generation is modified to bind the identifications of the MS and BS, and the PMK is delivered to the corresponding BS as shown in Fig. 2. The PMK and AK are generated as follows:

\[
\text{PMK} = \text{Dot16KDF(MSK, MS MAC Address, BSID, PMK)}
\]

where \( \text{PRF}(\text{PMK}, 160) \) is a cryptographically secure pseudo-random number function that generates an output of 160-bit length on the input of PMK. Thus, a BS receives a unique PMK which no other than the MS and the AS can derive.

The proposed pre-authentication procedure is described in Fig. 3(a). In the pre-authentication phase, the AS generates unique PMKs for the neighbor BSs and distributes them to the corresponding BSs. Then, the neighbor BSs derive their AKs for the MS. Likewise, the MS derives the PMKs and then AKs for its neighbor BSs with the BSIDs included in the MOB_NBR-ADV message. It identifies the network and defines the characteristics of neighbor BSs to which the MS would potentially perform initial network entry or HO. PMK_i represents the PMK of a BS_i. In the proposed pre-authentication process, as the serving BS can know neither the MSK and the PMK_i of its neighbor BSs, it cannot derive the AK_i of its neighbor BSs.

Upon a handover, as the MS and the target BS already have the AK, only the 3-way handshake is performed and the TEK is updated. The updated TEK is included in the SA-TEK-Update field in the SA-TEK-Response message and delivered from the BS to the MS. The re-authentication process is described in Fig. 3(b).

B. Pre-authentication for Soft Handover

In the soft handovers, MDHO and FBSS, BSs involved in MDHO or FBSS are required to share or transfer MAC context. The MAC context includes all information the MS and BS normally exchange during a network entry, particularly authentication state. Thus, the MS authenticated with one of the BSs in the diversity set is automatically authenticated with the other BSs from the same diversity set. The context also includes a set of service flows and corresponding mapping to connections associated with the MS, current authentication, and encryption keys associated with the connections. The
TABLE II
PERFORMANCE ANALYSIS OF AUTHENTICATION SCHEMES

<table>
<thead>
<tr>
<th></th>
<th>IEEE 802.16e</th>
<th>IEEE 802.16e</th>
<th>Proposed</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hard handover</td>
<td>soft handover</td>
<td>hard handover</td>
<td>soft handover (FBSS)</td>
</tr>
<tr>
<td>Communication</td>
<td>Pre-authentication</td>
<td>0</td>
<td>m (MSK distribution), m (TEK distribution)</td>
<td>m (PMK distribution), m (3-way handshake)</td>
</tr>
<tr>
<td></td>
<td>Re-authentication</td>
<td>EAP authentication, 3-way handshake</td>
<td>0</td>
<td>3-way handshake</td>
</tr>
<tr>
<td>Computation</td>
<td>MS</td>
<td>PMK, AK</td>
<td>PMK, AK</td>
<td>m × PMK, m × AK</td>
</tr>
<tr>
<td></td>
<td>BS</td>
<td>PMK, AK</td>
<td>AK</td>
<td>m × PMK</td>
</tr>
<tr>
<td></td>
<td>AS</td>
<td>–</td>
<td>–</td>
<td>m × PMK</td>
</tr>
<tr>
<td>Memory requirement</td>
<td>MS</td>
<td>MSK, PMK, AK, TEK</td>
<td>MSK, PMK, AK, TEK</td>
<td>MSK, m × PMK, m × AK, TEK</td>
</tr>
<tr>
<td></td>
<td>BS</td>
<td>MSK, PMK, AK, TEK</td>
<td>MSK, PMK, AK, TEK</td>
<td>PMK, AK, TEK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backward/forward secrecy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Fig. 5. Modified message exchange and key sharing procedure in the proposed soft handover (FBSS)

security context sharing and transferring procedure in IEEE 802.16e can be described like Fig. 4. The Key Share message is introduced for TEK sharing among the diversity set, which is not explicitly defined in the IEEE 802.16e standard.

As it is mentioned, the sharing policy of the secret keys among the BSs in the diversity set has a severe security flaw which creates the domino effect. In term of the efficiency, the secret information sharing can have an advantage of performing less cryptographic operations than a symmetric key sharing management. However, if the security of a BS is compromised, it can lead to the compromise of the security of all the BSs in the diversity set. Thus, to avoid the problem of domino effect, the least privilege principle [4] should be applied where each entity gets the minimum amount of security information to continue its operation.

Like the proposed key management for HHO in the previous Section III-A, the least privilege principle can be also applied to design a secure FBSS handover by splitting a key distributor and a key receiver so that the MSK is kept hidden from BSs and the PMK of a BS are kept hidden from other BSs. Thus, instead of delivering the MSK, the AS is required to generate a unique PMK using (2) and deliver the PMK to each BS in the diversity set. Between the MS and the BS to which the MS associated and authenticated at initial network entry, the authentication message exchange and key derivation are performed following the procedure described in Fig. 2. In the proposed pre-authentication phase for FBSS, the AS generates a unique PMK for each BS in the diversity set, and distributes it to each of them like the proposed HHO pre-authentication. Then, with BSs in the diversity set, the BS only performs 3-way handshake and receives the TEKs from each of the BSs. This pre-authentication process for FBSS is pictorially described in Fig. 5.

In MDHO, however, such a unique key distribution scheme cannot be applied to design a secure MDHO. Since the diversity technique such as a diversity combine needs the replicas of same signal for improving the reliability of a message in the diversity set [12], a secret key sharing among the entities in the diversity set is inevitable to make a same signal. In cellular wireless networks, the BSs are not trusted to perform key management because they can be easily tampered [13]. Therefore, a strong security assumption that all entities in the diversity set trust each other and are protected by tamper-proof equipments is needed to guarantee a secure MDHO. In a network where such an assumption cannot be realized, the MDHO cannot be a promising choice as a secure handover.

IV. PROTOCOL ANALYSIS

In this section, the performance and security analysis of the proposed authentication scheme for handover are given compared with those of the IEEE 802.16e [3]. In the analysis, it is assumed that the HO optimization bit #1 and #2 are both set to 0 for secure handover.

A. Performance Analysis

The analysis result is summarized in Table II. In the table, m denotes the average number of neighbor BSs. It is assumed that the number of BSs in the diversity set is also same as the number of neighbor BSs, m.

The communication property represents the number of communication exchanges for authentication and key distribution. Typically, the communication cost is the most important factor to evaluate the efficiency of a protocol. In this analysis,
communications for the common message exchanges such as
for the initial authentication exchanges between the MS and
the serving BS are not included.

The computation property represents secret keys that each
entity is supposed to generate in each scheme. The MSK and
TEK are not derived from other keying materials so that they
are not included in the analysis.

The memory requirement property represents the secret keys
that each entity should maintain. In the IEEE 802.16e, there
are two kinds of TEK per SA at a given time, one is an
old TEK and the other is a new TEK whose life times are
overlapped for a seamless secure connection. In addition, the
TEK can be created and revoked dynamically for the dynamic
SA associated with the dynamic service flow management.
However, TEKs for the dynamic SAs are not included in the
analysis for simplicity.

The backward/forward secrecy represents that whether each
scheme satisfies the backward and forward secrecy, and resists
the domino effect.

In the proposed hard handover scheme, the MS should
generate and store \( m \) PMKs and \( m \) AKs during the pre-
authentication phase; whereas, the MS is required to generate
and store only the current PMK and AK related to the serving
BS in the IEEE 802.16e hard handover scheme. Upon a
handover, however, the re-authentication phase in the proposed
handover scheme requires only 3-way handshake since
the PMK is delivered to the target BS and the AK is already
shared in the pre-authentication phase before handover. Thus,
the most time-consuming process of EAP-based authentication
is eliminated during the handover process.

Likewise, in the proposed soft handover scheme for FBSS,
the MS is required to generate and store \( m \) PMKs, \( m \) AKs,
and \( m \) TEKs. The communication cost for a key distribution in
the proposed scheme is almost same as the IEEE 802.16e soft
handover schemes. The Key Request and Key Reply message
in the IEEE 802.16e soft handover schemes are replaced by the
3-way handshake, which needs one more message exchange
per BS in the diversity set. Since the 3-way handshake does
not execute at a significantly higher frequency than the TEK
distribution, the additional communication cost seems trivial.
The IEEE 802.16e soft handover schemes cannot guarantee the
backward or forward secrecy due to the domino effect resulted
from the share of the same key. In contrast, the proposed soft
handover scheme for FBSS satisfies the backward and forward
secrecy due to the independent key management among the
BSs in the diversity set.

B. Security Analysis

In the proposed handover scheme, a unique PMK is gener-
ated by the AS and distributed to each of the neighbor BSs in
the pre-authentication phase. As we can see in (2), the PMK
is generated from the secret MSK which is only known to the
MS and the AS. Although the identifications of the MS and
BS are exposed to the public, even insider adversaries such as
compromised BSs cannot derive the PMKs and AKs of other
BSs due to the secrecy of the MSK and the one-way property
of the Dot16KDF key generation function. Thus, for the
adversaries, \( 2^{160} \) brute-force searches are needed to determine
the AK, which is considered computationally infeasible.

Additionally, as a same AK or TEK are not shared by
neighbor BSs or BSs in the diversity set, the domino effect
can be avoided in the proposed scheme. The independent key
management per BS and the least privilege principle prevent
the previous serving BS from guessing an AK of the following
target BS, and prevent the target BS from guessing an AK of
the previous serving BS. Without possessing the AK, attackers
cannot decrypt the TEKs.

V. CONCLUSION

In this paper, an overview and the security analysis of the
handover schemes defined in the IEEE 802.16e are given. The
design of the IEEE 802.16e handover procedures has several
security flaws. In addition, the pre-authentication process is not
defined in the specification. The proposed handover schemes
give a simple but secure pre-authentication protocol that fol-
 lows the least privilege principle to solve the domino effect. To
the best of our knowledge, this is the first study that analyzes
the key management protocol of PKMv2 in term of the secure
handover in IEEE 802.16e mobile WiMAX networks.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of
MIC/IITA. (2005-S609-02, Development of Core Technolo-
gies for Next Generation Mobile Multimedia Platform)

REFERENCES

ment2 for Physical and Medium Access Control Layers for Combined
[4] IEEE C802.16am-07/0209, “Mobility Sensitive Master Key Derivation and
Fast Re-authentication for 802.16m”, February 2007.
(EAP) Method Requirements for Wireless LANs”, RFC 4017, March
2005.
Management and Network Architecture in WiMAX”, in proceedings of
the IEEE Mobile WiMAX Symposium, 144–149, March 2007.
management protocols of IEEE 802.16”, in proceedings of the 44th annual
[12] N. C. Beaulieu, “Introduction to Linear Diversity Combining Tech-
Scheme for Heterogeneous Wireless Networks”, IEEE/ACM Transactions

2536