PAPER

Analysis of Effect of User Misbehaviours on the Reservation-Based MAC Protocols in Wireless Communication Networks

Norrarat WATTANAMONGKHOL[†], **Warakorn SRICHAVENGSUP**[††], **Pisit VANICHCHANUNT**[†††], **Robithoh ANNUR**[†], *Student Members*, **Jun-ichi TAKADA**[††††], *Senior Member*, *and* **Lunchakorn WUTTISITTIKULKIJ**[†a)], *Member*

SUMMARY In a shared medium communication system, mobile users contend for channel access according to a given set of rules to avoid collisions and achieve efficient use of the medium. If one or more users do not comply with the agree rules either due to selfish or malicious behaviours, they will cause some impacts on the system performance, especially to the well-behaved users. In this paper, we consider the problem of user misbehaviours on the performance of a wireless infrastructure-based network using reservation-based MAC protocols. Key misbehaving strategies possible in such a network are identified and explained. To quantify the impact of these misbehaviours upon the network performance, three different misbehaving scenarios are developed to allow a systematic investigation of each misbehaving strategy. For each scenario, we have derived mathematical formulations for evaluating and analyzing the key performance metrics, i.e., probabilities of success of well-behaved and misbehaved users and the fairness index. Numerical results show that the presence of misbehaviours can cause different levels of damage depending on the misbehavior strategy used. The combined multi-token and increasing permission probability strategies where the misbehaved user selfishly accesses the channel more times and with higher probabilities than allowed is shown to cause the most severe impairment of performance and fairness.

key words: *channel reservation, MAC protocols, selfish users, misbehaviours, wireless networks*

1. Introduction

In wireless networks, Medium Access Control (MAC) protocols are responsible for coordinating the access of multiple users contending for the common radio channel. Most wireless MAC protocols are designed based on the assumption that all users cooperate with each other and are compliant to predefined rules, which is to ensure fair and efficient sharing of communication channel among competing users. Recent studies [1]–[5] have suggested that these cooperative MAC protocols are vulnerable to user misbehaviours, in which some users do not strictly conform to the agreed rules due to their selfishness or maliciousness. A selfish user may deviate from the standard protocol specification, such as modifying the channel access parameters, to gain an unfair share of network resources. A malicious user may violate the rule aiming to cause disturbance to either other users or to the underlying system as a whole without attempting to gain a short-term benefit. Since the existence of misbehaviours will negatively impact well-behaved users, the problem of misbehaviours at the MAC layer has become a growing concern in broadband wireless access networks, especially from the points of view of performance and security.

Various different aspects of misbehaviours at the MAC layer have been investigated in the literature, particularly in the context of IEEE 802.11 wireless Local Area Networks (LANs). The misbehaviours manipulate the backoff parameter of the distributed coordination function (DCF) in the IEEE 802.11 standard [6], to obtain an unfair share of the channel. For example, the backoff interval can be selected smaller than that specified by DCF, or using a different retransmission strategy that does not double the contention window (CW) after collision [2]–[5], or setting the duration field to a larger value than the actual transmission time required for the frame [7], [8] resulting in an enlarged Network Allocation Vector (NAV) of other mobile users.

Moreover, misbehaviours at higher layers such as routing have also been examined. For example, in wireless ad hoc, a selfish user may refuse to always relay packets on behalf of other users in order to minimize its power consumption or other costs [9], [10]. This will usually affect the system throughput or even lead to user disconnection. A possible Denial of Service (DoS) attack on the signaling/control plane of the 3G wireless networks based on CDMA2000 and UMTS is introduced and studied in [11], [12]. The key objectives of these studies include classifying different MAC misbehaviour techniques, determining their impact upon well-behaved users, and mitigating the selfish MAC behaviour by designing a new MAC layer protocol that discourages misbehaviour [3] or introducing efficient misbehaviour detection algorithms [13]–[17] together with proper penalty schemes [4]. In non-cooperative environments where users behave selfishly and aim at optimizing their own individual benefits, the game theoretic approach is often applied to model network problems as a game and seek for an efficient Nash equilibrium, see [18]–[20] for some interesting models.

We consider, in this paper, the problem of user misbehaviours in a wireless infrastructure-based network using reservation-based MAC protocols where a mobile user

Manuscript received October 5, 2011.
Manuscript revised March 28, 2012.

[†] The authors are with the Department of Electrical Engineering, Chulalongkorn University, Thailand.
[††] The author is with the Department of Computer Engineering, Thai-Nichi Institute of Technology, Thailand.
[†††] The author is with the Department of Electrical Engineering, KMUTNB, Thailand.
[††††] The author is with the Department of International Development Engineering, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
a) E-mail: wlunchak@chula.ac.th

DOI: 10.1587/transcom.E95.B.2794

is required to contend for access in the uplink channel before its actual data packet transmission can take place. Reservation-based MAC protocols are known to provide several desirable characteristics including on-demand bandwidth allocation, support of multiple services with different Quality of Service (QoS) requirements, and effective bandwidth utilization. Some commonly known examples of early reservation-based MAC protocols are ALOHA-reservation [21], Dynamic reservation TDMA (DR-TDMA) [22], Dynamic TDMA with Piggybacked Reservation (DTDMA/PR) [23], Multiservices Dynamic Reservation (MDR) TDMA [24], and others [25]–[27]. More recently, IEEE 802.16 MAC protocol defines a contention-based request scheme for best-effort and non-real time polling services in Point-to-MultiPoint (PMP) architecture [28]–[30]. A subscriber station that wishes to send a data packet is required to transmit a request message (REQ) first. If the REQ is received correctly, then the base station will grant data slots to the subscriber station in the later frame provided that there are sufficient bandwidth resources. Since user misbehaviours can occur during the reservation period, but not the data transfer period because this latter period is controlled by the base station, the selfish user must somehow try to attain more successful REQs. This can be seen as a unique characteristics of reservation-based MAC protocols with respect to user misbehaviours that differs from other classes of MAC protocols. Therefore, it is interesting to investigate and explore the possibilities of how a selfish mobile user can misbehave and more importantly the impact of the misbehaving action upon well-behaved users.

During the reservation period, there exist many contention resolution algorithms that can be applied to resolve contention. Many algorithms have been proposed, studied, and analyzed. They can be classified into two major categories [31]–[33]: ALOHA-based and splitting algorithms. For ALOHA-based algorithms, a user is allowed to send its packet whenever the user has a packet ready for transmission. If more than one user transmits a packet in a slot simultaneously, then it will result in a collision and these packets are destroyed. All collided users have to retransmit their packet after a random delay, aiming to avoid continually repeated collision. Variations of ALOHA-based algorithms include p-persistent, binary exponential backoff and many other schemes. On the other hand, for splitting algorithms, each user randomly selects a branch among n sub-branches for contention with others. User who selects the first sub-branch is permitted to transmit first while other users in the remaining sub-branches postpone their transmission until the contention in the previous sub-branch has been resolved. In case of collision, each collision produces n new sub-branches which can be represented as a tree diagram. By using this algorithm, the probability of collision will be reduced in comparison to ALOHA-based algorithms because users are forced to retransmit their packets in different sub-branches in the future. The n-ary tree and stack algorithms are examples of this category. In principle, the splitting algorithms are more efficient than the ALOHA-based algorithms, but it is more complicated, as each user needs to keep track of the channel states. Hence, ALOHA-based algorithms have been widely used due to their simplicity and easy to implement. For example, p-persistent algorithm is applied to Carrier Sense Multiple Access (CSMA) for transmission of RTS/CTS packets in the split-channel MAC [34], [35]. In this paper, we selected the p-persistent algorithm for our system model.

The objective of this paper is to identify and explore various possible misbehaving strategies, and examine the impact of each upon those well-behaved users. To meet this objective, the user misbehaviour study is classified into three different scenarios, each of which is based on different combination of the following misbehaving strategies, i.e., changing the permission probability to other values than assigned, making more accessing attempts than allowed and shifting the access time selfishly to avoid contention; details of each strategy will be explained later. To fully understand the effect of different misbehaviours in reservation-based MAC protocols, the performance measured in terms of the probabilities of success of well-behaved and misbehaved users is analyzed and evaluated. Within this study, mathematical formulations are derived for every misbehaving scenario and verified by extensive computer simulations. We then investigate the interaction between misbehaved users who are applying different misbehaving strategies. In addition, a well known Jain's fairness index is used to quantify how much fairness is affected by the user misbehaviours.

The rest of this paper is organized as follows. In Sect. 2, the transmission procedure and mathematical derivation of the reservation-based MAC protocol is described. The performance analyses of three different selfish misbehaving scenarios are shown in Sect. 3. In Sect. 4, the numerical results and discussions of the three classified misbehaving scenarios are presented. Finally, the paper is concluded in Sect. 5.

2. Reservation-Based MAC Protocol Description

2.1 Protocol Description

In this section, we shall describe the transmission procedure of a reservation-based MAC protocol suitable for wireless broadband infrastructure-based networks, in which the transmission of radio signals between mobile users always takes place via a central base station. The uplink channel bandwidth of the reservation-based MAC protocol is divided into frames, where each frame consists of two alternating periods, namely, contention period and data transfer period, as in [21]–[24] see Fig. 1. The contention period is composed of a fixed number of contention slots while the data transfer period consists of a varied number of data slots assigned by the base station to accommodate only for those successful reservation requests. During the contention period, each user attempts to make reservation by sending a request packet to the base station on each contention slot in sequence from the first to the last slot. To help resolve

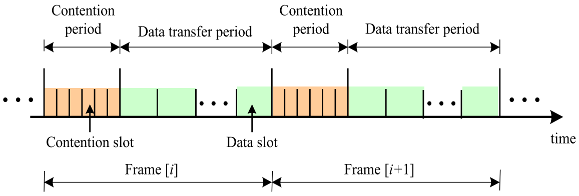


Fig. 1 A reservation-based MAC frame structure.

the contention, the well known p-persistent algorithm [31] is adopted, where each user is permitted to access each slot with a certain probability of p, referred to here as permission probability. Feedbacks from the base station indicating the request results are broadcast at the end of each contention period. A user with successful request will be assigned a data slot during the data transfer period for their data transmission while unsuccessful users can retransmit a request packet at the contention period of the next frame.

2.2 Performance Analysis

Consider a finite population of N mobile users, where each user has a packet ready to send at all frames. At the beginning of each contention period, all N users independently attempt to transmit a request packet with probability p. Let M be the number of contention slots in a frame. The probability that exactly k out of N users succeed in contention at the end of each frame can be expressed in a recursive form as [27]:

$$\begin{aligned} &P[k|M,N,p] \\ &\quad = \binom{N}{0}(1-p)^N P[k|M-1,N,p] \\ &\qquad + \binom{N}{1}\left((1-p)^{N-1}p\right)P[k-1|M-1,N-1,p] \\ &\qquad + \sum_{i=2}^{N}\binom{N}{i}\left((1-p)^{N-i}p^i\right)P[k|M-1,N-i,p] \end{aligned} \tag{1}$$

with the following boundary condition:

$$P[k|m,n,p] = \begin{cases} 0, & k<0, m\geq 0, n\geq 0 \\ 1, & k=0, m=0, n\geq 0 \\ 0, & k>0, m=0, n\geq 0 \\ 1, & k=0, m\geq 0, n=0 \\ 0, & k>0, m\geq 0, n=0 \end{cases} \tag{2}$$

where $m \in \{0,1,\ldots,M\}$ and $n \in \{0,1,\ldots,N\}$.

The probability of success for each user in each frame is then given by:

$$S = \frac{1}{N}\sum_{k=0}^{M} kP[k|M,N,p]. \tag{3}$$

In each slot, the request is successful, if and only if, exactly one request packet is transmitted in the slot. The success probability of each slot is not the same and can be derived. Let X_i be the event that slot ith contains exactly one packet (a successful request). The probability of event X_i is given by:

$$P(X_i) = \binom{N}{1}(1-p)^{i-1}p\left(1-(1-p)^{i-1}p\right)^{N-1}. \tag{4}$$

This relation can also be used to determine S by summing the success probabilities over all contention slots and divided by N. That is,

$$S = \frac{1}{N}\sum_{i=1}^{M}P(X_i) = \sum_{i=1}^{M}(1-p)^{i-1}p\left(1-(1-p)^{i-1}p\right)^{N-1}. \tag{5}$$

3. Misbehaving Scenarios and Performance Metrics

This section describes the details of each misbehaving scenario and presents mathematical formulations for analyzing the probabilities of success of well-behaved and misbehaved users. Other performance metrics used in this paper including the probability ratio and the fairness index are also defined.

3.1 Scenario I: Changing the Permission Probability

In the first scenario, well-behaved users apply the appropriate permission probability which can be obtained by (3) or (5) whereas misbehaved users change their permission probability to either greater or smaller than that of well-behaved users aiming to gain better access. Therefore, this scenario is referred to as *changing permission probability*.

Let N_1 be the number of well-behaved users and N_2 be the number of misbehaved users; $N_1+N_2=N$. At the beginning of each contention period, all N_1 and N_2 users independently attempt to transmit a request packet with probability p and p_m respectively. The joint probability that exactly k_1 out of N_1 users and k_2 out of N_2 users succeed in contention in each frame is expressed as [36]:

$$\begin{aligned} &P[k_1,k_2|M,N_1,N_2,p,p_m] \\ &= \binom{N_1}{0}(1-p)^{N_1}\binom{N_2}{0}(1-p_m)^{N_2}P[k_1,k_2|M-1,N_1,N_2] \\ &+ \binom{N_1}{1}\left((1-p)^{N_1-1}p\right)\binom{N_2}{0}(1-p_m)^{N_2}P[k_1,k_2|M-1,N_1-1,N_2] \\ &+ \binom{N_1}{0}(1-p)^{N_1}\binom{N_2}{1}\left((1-p_m)^{N_2-1}p_m\right)P[k_1,k_2-1|M-1,N_1,N_2-1] \\ &+ \sum_{i_1=2}^{N_1}\binom{N_1}{i_1}\left((1-p)^{N_1-i_1}p^{i_1}\right)\binom{N_2}{0}(1-p_m)^{N_2}P[k_1,k_2|M-1,N_1-i_1,N_2] \\ &+ \sum_{i_2=2}^{N_2}\binom{N_1}{0}(1-p)^{N_1}\binom{N_2}{i_2}\left((1-p_m)^{N_2-i_2}p_m^{i_2}\right)P[k_1,k_2|M-1,N_1,N_2-i_2] \\ &+ \sum_{i_1=1}^{N_1}\sum_{i_2=1}^{N_2}\binom{N_1}{i_1}\left((1-p)^{N_1-i_1}p^{i_1}\right)\binom{N_2}{i_2}\left((1-p_m)^{N_2-i_2}p_m^{i_2}\right) \\ &P[k_1,k_2|M-1,N_1-i_1,N_2-i_2,p,p_m] \end{aligned} \tag{6}$$

and the boundary condition is

$$P[k_1,k_2|m,n_1,n_2]$$

$$= \begin{cases} 0, k_1 < 0 \text{ or } k_2 < 0, m \geq 0, n_1 \geq 0, n_2 \geq 0 \\ 0, k_1 + k_2 > m, m \geq 0, n_1 \geq 0, n_2 \geq 0 \\ 0, k_1 > n_1 \text{ or } k_2 > n_2, m \geq 0, n_1 \geq 0, n_2 \geq 0 \\ 1, k_1 + k_2 = 0, m = 0, n_1 \geq 0, n_2 \geq 0 \\ 1, k_1 + k_2 = 0, m \geq 0, n_1 = n_2 = 0 \end{cases} \quad (7)$$

where $m \in \{0, 1, \ldots, M\}$, $n_1 \in \{0, 1, \ldots, N_1\}$ and $n_2 \in \{0, 1, \ldots, N_2\}$.

Therefore, the probabilities of success of well-behaved and misbehaved users respectively are given by

$$S_w = \frac{1}{N_1} \sum_{k_1=0}^{N_1} k_1 \left(\sum_{k_2=0}^{N_2} P[k_1, k_2 | M, N_1, N_2, p, p_m] \right) \quad (8)$$

and

$$S_m = \frac{1}{N_2} \sum_{k_2=0}^{N_2} k_2 \left(\sum_{k_1=0}^{N_1} P[k_1, k_2 | M, N_1, N_2, p, p_m] \right). \quad (9)$$

The probabilities of success of well-behaved and misbehaved users in each slot can be derived as follows. Let X_i and Y_i be the event that slot ith contains exactly one packet of well-behaved and misbehaved users, respectively. The probability of event X_i and Y_i occurring are given by:

$$P(X_i) = N_1 \left((1-p)^{i-1} p \right) \left(1 - (1-p)^{i-1} p \right)^{N_1 - 1} \left(1 - (1-p_m)^{i-1} p_m \right)^{N_2} \quad (10)$$

and

$$P(Y_i) = N_2 \left(1 - (1-p)^{i-1} p \right)^{N_1} \left((1-p_m)^{i-1} p_m \right) \left(1 - (1-p_m)^{i-1} p_m \right)^{N_2 - 1}. \quad (11)$$

The sum of success probability of all contention slots, i.e., $\sum_{i=1}^{M} P(X_i)$ and $\sum_{i=1}^{M} P(Y_i)$ are identical to the mean number of successes, i.e., $\sum_{k_1=0}^{N_1} k_1 \, P[k_1, k_2 | M, N_1, N_2, p, p_m]$ and $\sum_{k_2=0}^{N_2} k_2 \, P[k_1, k_2 | M, N_1, N_2, p, p_m]$ respectively. Therefore, the probabilities of success of well-behaved and misbehaved users respectively are given by:

$$S_w = \sum_{i=1}^{M} \left((1-p)^{i-1} p \right) \left(1 - (1-p)^{i-1} p \right)^{N_1 - 1} \left(1 - (1-p_m)^{i-1} p_m \right)^{N_2} \quad (12)$$

and

$$S_m = \sum_{i=1}^{M} \left(1 - (1-p)^{i-1} p \right)^{N_1} \left((1-p_m)^{i-1} p_m \right) \left(1 - (1-p_m)^{i-1} p_m \right)^{N_2 - 1}. \quad (13)$$

3.2 Scenario II: Changing the Permission Probability with Multi- Token Mechanism

In the scenario II, misbehaved users not only change their permission probability in the same way as in the scenario I but also attempt to access more than once in each frame. Since giving users more chances of making reservations should enable them to achieve greater success, it is expected that the misbehaved users will gain more share of the available bandwidth. This strategy is referred to here as *changing permission probability with multi-token mechanism*, where the number of tokens represents the maximum number of access attempts to make reservation per frame.

Let T_i be the number of tokens for misbehaved user i, $1 \leq i \leq N_2$. Let B_i be the flag bit that represents whether misbehaved user i has succeeded yet. If $B_i = 1$ means misbehaved user i has already succeeded and $B_i = 0$ means misbehaved user i has not succeeded yet. R is the number of remaining misbehaved users in the system.

$$R = N_2 - (\text{the number of } T_i\text{'s that are zero}). \quad (14)$$

The probability that exactly k_1 out of N_1 users and k_2 out of N_2 users succeed in contention at the end of each frame, where misbehaved user i has T_i remaining tokens and its success status is B_i as in the following recursive formula.

$$\begin{aligned} &P[k_1, k_2 | M, N_1, T_1, T_2, \ldots, T_{N_2}, B_1, B_2, \ldots, B_{N_2}] \\ &= \binom{N_1}{0} (1-p)^{N_1} (1-p_m)^R P_A + \binom{N_1}{1} (1-p)^{N_1 - 1} p (1-p_m)^R P_B \\ &+ \binom{N_1}{0} (1-p)^{N_1} p_m (1-p_m)^{R-1} P_C + \sum_{i_1=2}^{N_1} \binom{N_1}{i_1} \\ &\quad \left((1-p)^{N_1 - i_1} p^{i_1} \right) (1-p_m)^R P_D \\ &+ \sum_{i_2=2}^{R} \binom{N_1}{0} (1-p)^{N_1} p_m^{i_2} (1-p_m)^{R-i_2} G_{i_2} \\ &+ \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{R} \binom{N_1}{i_1} \left((1-p)^{N_1 - i_1} p^{i_1} \right) \left((1-p_m)^{R-i_2} p_m^{i_2} \right) H_{i_2} \end{aligned} \quad (15)$$

where

$$P_A = P[k_1, k_2 | M-1, N_1, T_1, T_2, \ldots, T_{N_2}, B_1, B_2, \ldots, B_{N_2}]$$

$$\begin{aligned} P_B = P[&k_1 - 1, k_2 | M-1, N_1 - 1, T_1, T_2, \ldots, T_{N_2}, B_1, \\ &B_2, \ldots, B_{N_2}] \end{aligned}$$

$$\begin{aligned} P_C = \sum_{\substack{i_2=1 \\ T_{i_2} \neq 0}}^{N_2} &P[k_1, k_2 - \delta(B_{i_2}) | M-1, N_1, T_1, \ldots, T_{i_2 - 1}, \\ &T_{i_2} - 1, T_{i_2+1}, \ldots, T_{N_2}, B_1, \ldots, B_{i_2 - 1}, 1, B_{i_2+1}, \ldots, B_{N_2}] \end{aligned}$$

$$\delta(x) = \begin{cases} 1, & x = 0; \quad \text{new success} \\ 0, & x \neq 0; \quad \text{repeated success} \end{cases}$$

$$P_D = P[k_1, k_2 | M-1, N_1 - i_1, T_1, \ldots, T_{N_2}, B_1, \ldots, B_{N_2}]$$

$$\begin{aligned} G_2 = \sum_{\substack{j<j' \\ T_j, T_{j'} \neq 0}} &P[k_1, k_2 | M-1, N_1, T_1, \ldots, T_{j-1}, T_j - 1, T_{j+1}, \\ &\ldots, T_{j'-1}, T_{j'} - 1, T_{j'+1}, \ldots, T_{N_2}, B_1, \ldots, B_{N_2}] \end{aligned}$$

$$\begin{aligned} G_i = \sum_{\substack{j_1 < j_2 < \cdots < j_i \\ T_{j_1}, T_{j_2}, \ldots, T_{j_i} \neq 0}} &P[k_1, k_2 | M-1, N_1, T_1, \ldots, T_{j_1 - 1}, T_{j_1} - 1, \\ &T_{j_1+1}, \ldots, T_{j_2 - 1}, T_{j_2} - 1, T_{j_2+1}, \ldots, \end{aligned}$$

$$
\begin{aligned}
&T_{j_i-1}, T_{j_i}-1, T_{j_i+1}, \ldots, T_{N_2}, B_1, \ldots, B_{N_2}],\\
&2 \le i \le R\\
H_1 = &\sum_{j, T_j \neq 0} P[k_1, k_2 | M-1, N_1-1, T_1, \ldots, T_{j-1}, T_j-1,\\
&T_{j+1}, \ldots, T_{N_2}, B_1, \ldots, B_{N_2}]\\
H_i = &\sum_{\substack{j_1<j_2<\cdots<j_i\\ T_{j_1}, T_{j_2}, \ldots, T_{j_i} \neq 0}} P[k_1, k_2 | M-1, N_1-i_1, T_1, \ldots, T_{j_1-1}, T_{j_1}-1,\\
&T_{j_1+1}, \ldots, T_{j_2-1}, T_{j_2}-1,\\
&T_{j_2+1}, \ldots, T_{j_i-1}, T_{j_i}-1, T_{j_i+1}, \ldots, T_{N_2},\\
&B_1, \ldots, B_{N_2}], \quad 2 \le i \le R
\end{aligned}
$$

and the boundary condition is

$$
P[k_1, k_2 | m, n_1, T_1, \ldots, T_{n_2}, B_1, \ldots, B_{n_2}]
= \begin{cases}
0, k_1 < 0 \text{ or } k_2 < 0, n_1 + T_i \ge 0, B_i \ge 0, m \ge 0\\
0, k_1 + k_2 > m, n_1 + T_i \ge 0, B_i \ge 0, m \ge 0\\
0, k_1 > n_1 \text{ or } k_2 > n_2, n_1 + T_i \ge 0, B_i \ge 0, m \ge 0\\
1, k_1 + k_2 = 0, n_1 + T_i = 0, B_i \ge 0, m \ge 0\\
1, k_1 + k_2 = 0, n_1 + T_i \ge 0, B_i \ge 0, m = 0.
\end{cases} \tag{16}
$$

Thus, the probabilities of success for well-behaved and misbehaved users are respectively given by:

$$
S_w = \frac{1}{N_1} \sum_{k_1=0}^{N_1} k_1 \sum_{k_2=0}^{N_2} P[k_1, k_2 | M, N_1, T_1, T_2, \ldots, T_{N_2}, B_1, B_2, \ldots, B_{N_2}] \tag{17}
$$

and

$$
S_w = \frac{1}{N_1} \sum_{k_1=0}^{N_1} k_1 \sum_{k_2=0}^{N_2} P[k_1, k_2 | M, N_1, T_1, T_2, \ldots, T_{N_2}, B_1, B_2, \ldots, B_{N_2}] \tag{18}
$$

3.3 Scenario III: Changing the Permission Probability with Shifted Reservation Time

The misbehaving strategy of scenario III is extended from the scenario I. That is, misbehaved users will not commence their reservation attempts at the first slot in the same fashion as what other well-behaved users would do. Instead they delay or shift their first attempt till later slots in order to avoid high contention which usually occurs in early slots of a frame. It is interesting to examine how long these misbehaved users should shift their first attempt to achieve the maximum advantage. This scenario is called *changing the permission probability with shifted reservation time*.

Let l be interpreted as the number of remaining reservation slots plus one (the current slot). The probability that exactly k_1 out of N_1 users and k_2 out of N_2 users succeed in contention at the end of each frame.

$$
P[k_1, k_2 | l, N_1, N_2]
= \begin{cases}
\binom{N_1}{0} (1-p)^{N_1} P[k_1, k_2 | l-1, N_1, N_2]\\
+ \binom{N_1}{1} \left((1-p)^{N_1-1} p\right) P[k_1-1, k_2 | l-1, N_1-1, N_2]\\
+ \sum_{i_1=2}^{N_1} \binom{N_1}{i_1} \left((1-p)^{N_1-i_1} p^{i_1}\right) P[k_1, k_2 | l-1, N_1-i_1, N_2],\\
\qquad N_1 > 0, \ \ l > M-D\\
P[k_1, k_2 | l-1, N_1, N_2], \quad N_1 = 0, \ \ l > M-D
\end{cases} \tag{19}
$$

and

$$
\begin{aligned}
&P[k_1, k_2 | l, N_1, N_2]\\
&= \binom{N_1}{0} (1-p)^{N_1} \binom{N_2}{0} (1-p_m)^{N_2} P[k_1, k_2 | l-1, N_1, N_2]\\
&+ \binom{N_1}{1} \left((1-p)^{N_1-1} p\right) \binom{N_2}{0} (1-p_m)^{N_2} P[k_1-1, k_2 | l-1, N_1-1, N_2]\\
&+ \binom{N_1}{0} (1-p)^{N_1} \binom{N_2}{1} \left((1-p_m)^{N_2-1} p_m\right) P[k_1, k_2-1 | l-1, N_1, N_2-1]\\
&+ \sum_{i_1=2}^{N_1} \binom{N_1}{i_1} \left((1-p)^{N_1-i_1} p^{i_1}\right) \binom{N_2}{0} (1-p_m)^{N_2} P[k_1, k_2 | l-1, N_1-i_1, N_2]\\
&+ \sum_{i_2=2}^{N_2} \binom{N_1}{0} (1-p)^{N_1} \binom{N_2}{i_2} \left((1-p_m)^{N_2-i_2} p_m^{i_2}\right) P[k_1, k_2 | l-1, N_1, N_2-i_2]\\
&+ \sum_{i_1=1}^{N_1} \sum_{i_2=1}^{N_2} \binom{N_1}{i_1} \left((1-p)^{N_1-i_1} p^{i_1}\right) \binom{N_2}{i_2} \left((1-p_m)^{N_2-i_2} p_m^{i_2}\right)\\
&\qquad P[k_1, k_2 | l-1, N_1-i_1, N_2-i_2], \quad l \le M-D
\end{aligned} \tag{20}
$$

where D is the number of time slots that the misbehaved users shift their reservation attempts. The calculation of $P[k_1, k_2 | l, N_1, N_2]$ is separated into two parts, i.e., (19) and (20). The first part is relevant to the time duration where there is only the reservation attempt of the well-behaved users but no reservation attempt of the misbehaved users and the second part corresponds to the later duration where both the well-behaved and misbehaved users perform the reservation. For the sake of compact notation, we will not show the variable D in the probability $P[k_1, k_2 | l, N_1, N_2]$. The boundary condition for the above recursive formula is

$$
P[k_1, k_2 | l, n_1, n_2, p, p_m]
= \begin{cases}
0, \ \ k_1 < 0 \text{ or } k_2 < 0, n_1 + n_2 \ge 0, l \ge 0\\
0, \ \ k_1 + k_2 > m, \ n_1 + n_2 \ge 0, l \ge 0\\
0, \ \ k_1 > n_1 \text{ or } k_2 > n_2, n_1 + n_2 \ge 0, l \ge 0\\
1, \ \ k_1 + k_2 = 0, n_1 + n_2 \ge 0, l = 0\\
1, \ \ k_1 + k_2 = 0, n_1 + n_2 = 0, l \ge 0.
\end{cases} \tag{21}
$$

Therefore, the probabilities of success for well-behaved and misbehaved users are respectively given by:

$$
S_w = \sum_{k_1=0}^{N_1} k_1 \sum_{k_2=0}^{N_2} P[k_1, k_2 | l = M, N_1, N_2] \tag{22}
$$

or alternatively

$$S_w = \frac{1}{N_1}\left(\begin{array}{l}\sum\limits_{i=1}^{D}\left(p(1-p)^{i-1}\left(1-p(1-p)^{i-1}\right)^{N_1-1}\right)\\ +\sum\limits_{i=D+1}^{M}\left(p(1-p)^{i-1}\left(1-p(1-p)^{i-1}\right)^{N_1-1}\right.\\ \left.\quad\left(1-p_m(1-p_m)^{i-D}\right)^{N_2}\right)\end{array}\right) \tag{23}$$

and

$$S_m = \sum_{k_1=0}^{N_1}\sum_{k_2=0}^{N_2} k_2 P[k_1,k_2|l = M, N_1, N_2] \tag{24}$$

or alternatively

$$S_m = \frac{1}{N_2}\sum_{i=D+1}^{M}\left(\left(1-p(1-p)^{i-1}\right)^{N_1} p_m(1-p_m)^{i-D}\right.$$
$$\left.\left(1-p_m(1-p_m)^{i-D}\right)^{N_2-1}\right). \tag{25}$$

3.4 The Probability Ratio and the Fairness Index

In addition to the probabilities of success described before, other useful performance metrics are defined. The ratio between the average number of successes of the system with and without misbehaved users is defined as

$$\text{Probability ratio} = \frac{(N_1 S_w + N_2 S_m)}{NS}. \tag{26}$$

This probability ratio can show how much effect is caused by the misbehaved user to the whole system performance. Furthermore, the existence of misbehaved user will result in an unfair share of the resources so the well known Jain's fairness index (J) [37] is adopted to measure the equality of opportunity in channel access as follows:

$$J = \frac{(N_1 S_w + N_2 S_m)^2}{N\left(N_1 S_w^2 + N_2 S_m^2\right)}. \tag{27}$$

The range of this fairness measure lies between 0 and 1. If the well-behaved and misbehaved users share the bandwidth fairly, the fairness index equals to 1. It will decrease as the misbehaved user gain more unfair share of bandwidth from the system.

4. Numerical Results and Discussion

In this section, the performance of all scenarios is numerically evaluated by using the mathematical formulations described in the previous section. These results are also validated and confirmed with computer simulations. In each scenario, we consider the system performance in terms of the probabilities of success per user defined as S_w and S_m for well-behaved and misbehaved users, respectively, under various different system parameters such as the number of slots (M), the number of tokens (T), the number of shifted time slots (D) and the values of permission probabilities (p).

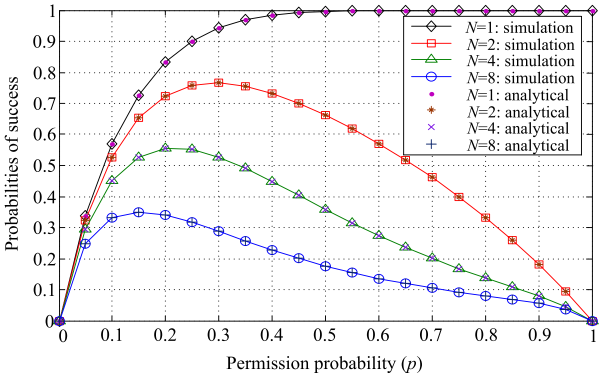


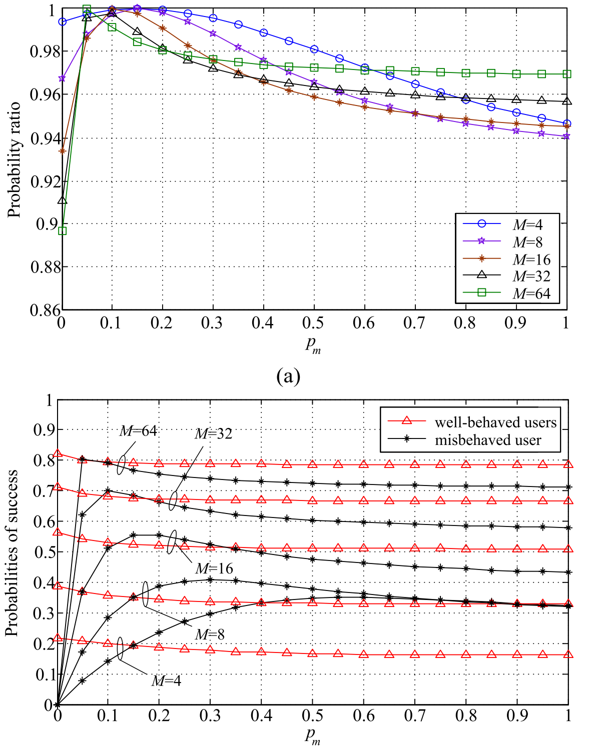
Fig. 2 Performance of the reservation-based MAC protocol.

4.1 Performance Evaluation of the Reservation-Based MAC Protocols

Figure 2 shows the comparison between the probabilities of success of the reservation-based MAC protocols obtained via simulation and the mathematical formulations provided in the previous section. We consider the number of overall users (N) at 1, 2, 4, and 8. The number of contention slots (M) is set at 8 while the permission probability (p) is varied from 0 to 1. First, we consider the case of $N = 1$ (there is no collision), the probabilities of success increase with p and quickly converge to 1 at $p = 1$. Obviously, when there is only one user in the system, the user should always send its request packet. Second, we consider the case of multiple users, $N = 2$, 4 and 8. For small values of p, the probabilities of success clearly increase with p. When p increases up to a certain value, the maximum probability of success is reached, and the value of p at this point will be referred to as the appropriate permission probability. When p further increases, the probability of success begins to decline and eventually reaches zero when $p = 1$ (there are always collisions). Note that the appropriate values of permission probabilities for $N = 1$, 2, 4 and 8 are 1, 0.294, 0.217 and 0.15 respectively. It can be seen that the simulation results accurately agree with the calculated probabilities of success. That is, our mathematical formulation for the probabilities of success of the reservation-based MAC protocols is valid and accurate.

4.2 Performance Evaluation of the Scenario I

To demonstrate how much the misbehaved user in the scenario I can have an effect on the well-behaved users and also on the system performance as a whole, we present some numerical results obtained from the mathematical formulations in (8) and (9), or alternatively (12) and (13), based on the following system configuration. The total number of contending users is fixed at 8 and one of them is a misbehaved user. Since the misbehaved user in scenario I tries to gain unfair share of bandwidth by choosing the value of permission probability other than the appropriate one, we then



(a)

(b)

Fig. 3 Performance of the scenario I: (a) the ratio of the average number of successes between systems with and without the misbehaved user and (b) probabilities of success as a function of p_m.

varies its permission probability from 0 to 1. The number of contention slots is also varied as M = 4, 8, 16, 32 and 64, to cover various different contention situation.

Figure 3(a) illustrates the ratios of the average number of successes between systems with and without the misbehaved user, as a function of the permission probability used by the misbehaved user (p_m). It can be seen that when the misbehaved user increases its permission probability from the appropriate value, the probability ratio falls below 1 for all system configurations, i.e., M = 4, 8, 16, 32 and 64, which means that the overall system performance drops due to the user misbehaviour. However, the overall system performance drops by no more than 6% compared to that of system working in normal condition. Thus, in this scenario the existence of one misbehaved user has a slightly negative impact on the overall system performance. The drops in the overall performance can be explored further by examining the probabilities of success of well-behaved and misbehaved users, which is discussed in the sequel.

The probabilities of success of well-behaved and misbehaved users are compared in Fig. 3(b). For M = 4, the misbehaved user can achieve higher probabilities of success than the well-behaved users by using the permission probabilities greater than that of the well-behaved users. For example, the probabilities of success can be increased from 0.19 (no misbehaviour) to the maximum achievable value of 0.35 by increasing p_m from the agreed value of 0.15 to 0.60, nearly double the advantage. This is achieved at a small expense of those well behaved users; in the worst case, the probabilities of success of the well-behaved users degrade from 0.19 to 0.16.

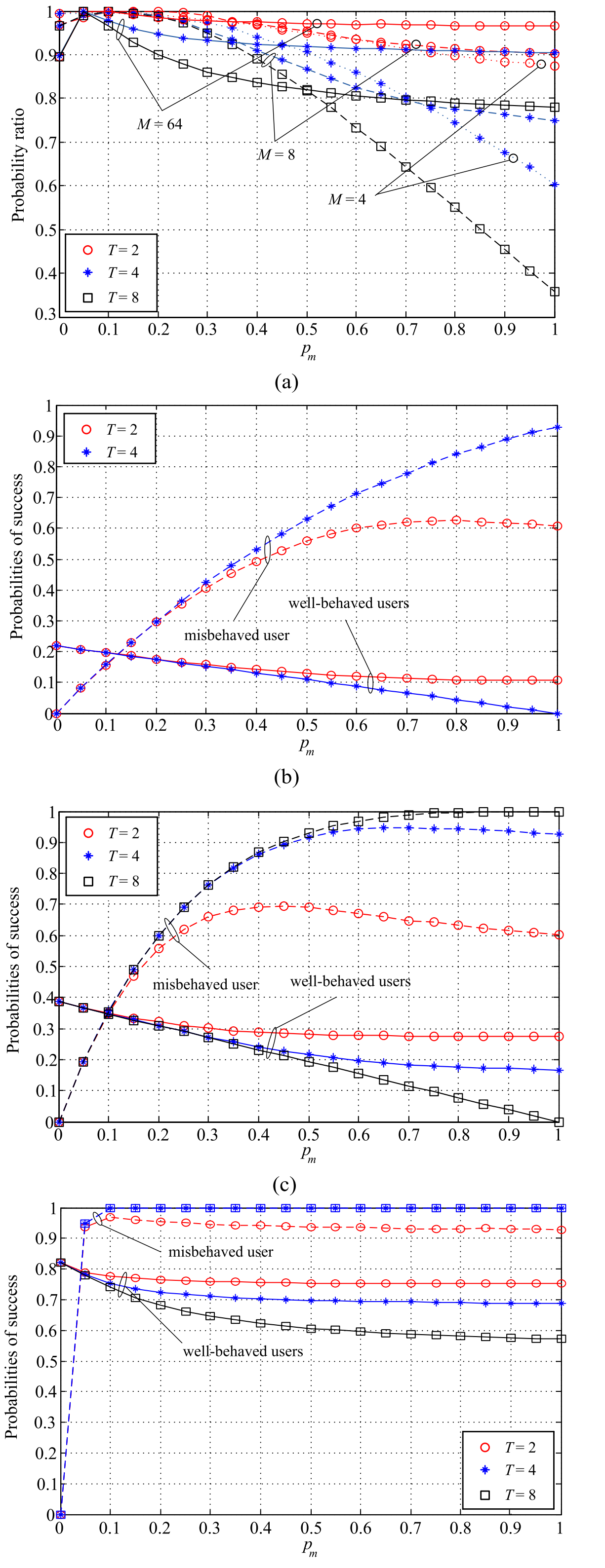
When the number of contention slots is increased to M = 8, 16, and 32, similar results to that of M = 4 are observed. The misbehaved user is still able to achieve better probabilities of success than the well-behaved users by accessing the slots with greater probability than the agreed value. However, the range of the permission probabilities that the misbehaved user can adopt to gain better access becomes narrower than the previous case with M = 4. In fact, this range gets smaller with the increase of the number of contention slots. As M = 64, as shown in Fig. 3(b), the range becomes almost zero which means that the misbehaved user hardly accomplish better access than well-behaved users no matter which value of permission probability is used. These results indicate that the misbehaved user will not gain much benefit by increasing the permission probability alone, especially when the number of contention slots is large.

4.3 Performance Evaluation of the Scenario II

In the scenario II, the misbehaved user violates the agreed rule by not only changing its permission probability as in scenario I but also using more than one token. To evaluate the performance of the scenario II, we set the total number of contending users and misbehaved user as the same as in the scenario I. The number of contention slots available is set at M = 4, 8, and 64 whereas the number of tokens is varied as T = 2, 4, and 8.

Figure 4(a) illustrates the ratios of the average number of successes between systems with and without the misbehaved user with different number of tokens. It can be seen that the effect of this misbehaviour to the overall system performance is not so substantial when the misbehaved user uses a relatively small number of tokens compared to the number of slots such as T = 2, M = 8 or T = 2, M = 64. However, when the number of tokens used by the misbehaved user is comparable to the number of contention slots such as T = 4, M = 4 or T = 8, M = 8, the probability ratio declines considerably especially when the value of p_m is close to one. This is because most of the available slots will be occupied by the misbehaved user and hence less chance for the well-behaved user to succeed.

Figures 4(b)–(d) show the probabilities of success of well-behaved and misbehaved users as a function of the permission probability of the misbehaved user (p_m). Consider Fig. 4(b) where M = 4, it can be seen that the misbehaved user gains significant advantages when it combines the use of multi-token and the increase of permission probability. The gains are also more substantial with greater number of tokens; the maximum probabilities of success of the misbehaved user of 0.62 and 0.93 can be reached with T = 2 and T = 4 respectively. Since the introduced multi-token mechanism causes more severe contention in each slot, the probabilities of success of the well-behaved users drop and



(a)

(b)

(c)

(d)

Fig. 4 Performance of the scenario II: (a) the ratio of the average number of successes between systems with and without the misbehaved user and (b)–(d) probabilities of success for M = 4, 8, and 64, respectively, as a function of p_m.

in the extreme cases the probabilities of success of the well-behaved users reach zero.

Consider Figs. 4(c)–(d) where the number of slots is increased to 8 and 64 respectively, as expected, with more number of contention slots available, both the misbehaved user and all other well-behaved users have higher probabilities of success compared to when $M = 4$. The misbehaved user can achieve significant gain on the probabilities of success by increasing its permission probabilities and number of tokens at the cost of lower probabilities of success of well-behaved users. For $M = 8$, the maximum probability of success of 1 is reached with $T = 8$ and $p_m > 0.8$ whereas for $M = 64$, the same maximum is reached with $T = 4$, 8 and much smaller values of p_m.

4.4 Performance Evaluation of the Scenario III

Figure 5(a) shows the ratios of the average number of successes under three different time shifts (D), i.e., $M/4$, $M/2$, and $3M/4$ as the permission probability (p_m) varies from 0 to 1. This figure depicts the impact of the misbehaved user to the system performance when M is varied as 4, 8, and 64 slots. It can be seen that most curves show the values of probability ratio more than one. This means that shifting the reservation by the misbehaved user is actually not only benefit for misbehaved user itself but also for the well-behaved users, especially in the case of $D = 3M/4$, which provides the highest probability ratio among three different time shifts. As a result, this shifting action will in most cases improve the performance of the whole system.

Figures 5(b)–(d) compare the probabilities of success for well-behaved and misbehaved users for three different time shifts, i.e., $M/4$, $M/2$, and $3M/4$, when the number of the contention slots is set to 4, 8, and 64 respectively. The well-behaved users apply the agreed contention probability, whereas the misbehaved user varies the permission probability from 0 to 1 and begins the access at slot $D + 1$. From the results, it can be seen that the shift of reservation time together with the increase of the permission probability to a certain value can help increase the access gain of the misbehaved user while causing small effect to the well-behaved users. This may be explained as follows. In the normal situation, each user applies a fixed permission probability from the first to the last slot with only a single attempt allowed. As a result, the contention in later slots is normally less severe than previous slots, i.e., later slots are more frequently idle, the misbehaved user can increase its chance of success by increasing the permission probability without much disturbance to the well-behaved users.

When comparing these performance curves with respect to different time shifts of $M/4$, $M/2$, and $3M/4$, we can see that with short time shift, as in the case of $D = M/4$, the misbehaved user can obtain the maximum advantages by increasing its permission probability to a certain value (further increase beyond this value will result in the reverse effect) whereas with longer time shift, as in the case $D = 3M/4$, greater advantage can be gained by applying even

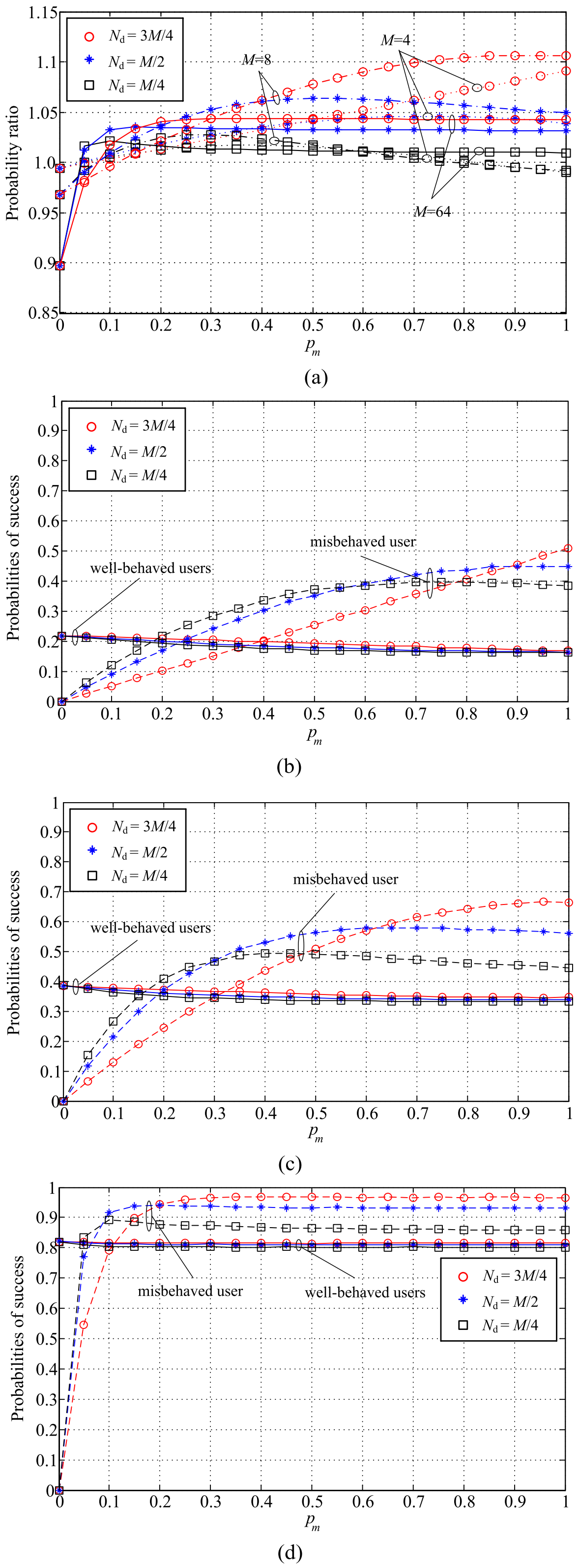


Fig. 5 Performance of the scenario III: (a) the ratio of the average number of successes between systems with and without the misbehaved user and (b)–(d) probabilities of success for M = 4, 8, and 64, respectively, as a function of p_m.

higher values of permission probability. This is conceivable, as with longer time shift, the misbehaved user has fewer opportunities to make reservations and there is less contention in those later slots, when it increases its permission probability, the probabilities of success can be improved. These results suggest that the probability of success for the misbehaved user can be maximized by shifting the first reservation attempt together with the increase of the access probability as much as possible.

4.5 Maximum Achievable Advantage and Fairness Index

Since misbehaviours aim to achieve more benefit from the system, we shall now present the maximum achievable advantage which can be acquired by the misbehaved user for each scenario. With several parameter settings, the maximum values of S_m for scenarios I, II and III are shown in Table 1 together with percent gain, S_m/S_w ratio and Jain's fairness index (J).

By comparing the results from these three scenarios, we can see that the scenario II gives the highest benefit to the misbehaved user with maximum percent gain equals 378% which is obtained when $M = 4$ with $T = 4$. This condition also results in infinity for S_m/S_w meaning that the well-behaved users do not succeed in reservation and suffer very much from this scenario. This is also reflected by the value of the fairness index which falls to 0.125. Small negative impact to the well-behaved users and high fairness index can be achieved when the misbehaved user adopts either scenario I or III. However, the higher values of S_m are obtained by scenario III than that of scenario I. In scenario III, the worst condition occurs when the number of available slots and the time shift are small ($M = 4, D = 1$). The percent gain of 164.2% and $J = 0.774$ are obtained with $D = 3$. For all scenarios, the negative impact of this selfish behaviour is

Table 1 Maximum values of S_m, percent gain, S_m/S_w ratio and fairness index (J).

	M	S_m	$\frac{(S_m-S)}{S}\%$	S_m/S_w	J
Scenario I	4	0.350	81.4	2.131	0.903
	8	0.408	16.6	1.213	0.995
	16	0.556	5.1	1.065	0.999
	32	0.700	2.2	1.028	0.999
	64	0.809	1.1	1.013	0.999

	M	T	S_m	$\frac{(S_m-S)}{S}\%$	S_m/S_w	J
Scenario II	4	2	0.626	224.4	5.689	0.511
		3	0.816	323	14.972	0.262
		4	0.923	378	Inf.	0.125
	8	2	0.692	97.8	2.446	0.859
		4	0.949	171.2	5.267	0.541
		6	0.997	184.9	10.787	0.320
		8	1	185.7	Inf.	0.125
	64	4	1	24.8	1.364	0.987
		8	1	24.8	1.454	0.980
		16	1	24.8	1.473	0.979
		32	1	24.8	1.486	0.978
		48	1	24.8	1.493	0.977
		56	1	24.8	1.504	0.976
		64	1	24.8	1.513	0.975

	M	D	S_m	$\frac{(S_m-S)}{S}\%$	S_m/S_w	J
Scenario III	4	1	0.399	106.7	2.435	0.861
		2	0.453	134.6	2.743	0.817
		3	0.510	164.2	3.049	0.774
	8	1	0.451	28.7	1.340	0.988
		2	0.494	41.1	1.465	0.979
		3	0.538	53.6	1.587	0.968
		4	0.581	65.9	1.704	0.956
		5	0.623	78.1	1.815	0.944
		6	0.666	90.3	1.920	0.931
		7	0.708	102.3	2.019	0.918
	64	1	0.816	1.9	1.020	0.999
		4	0.834	4.1	1.041	0.999
		8	0.855	6.8	1.065	0.999
		16	0.892	11.4	1.105	0.999
		24	0.920	14.9	1.135	0.998
		32	0.942	17.6	1.158	0.997
		40	0.958	19.6	1.175	0.997
		48	0.970	21.1	1.187	0.996
		56	0.979	22.2	1.196	0.996
		63	0.984	22.9	1.202	0.996

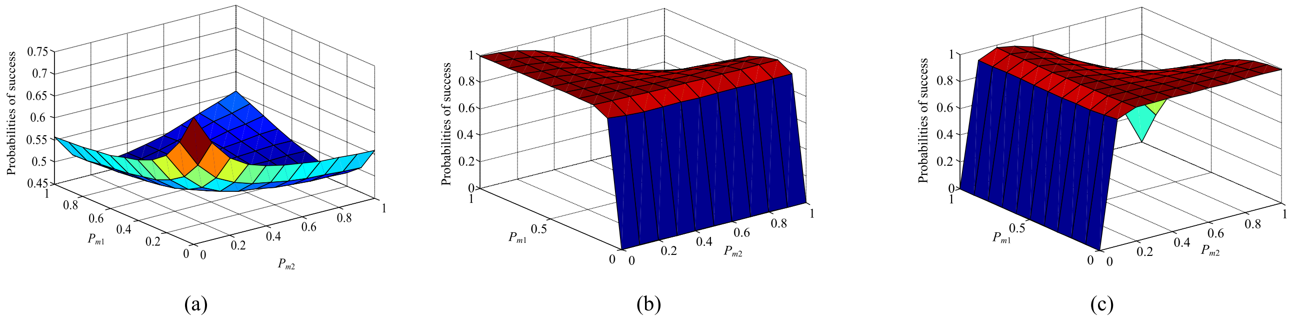


Fig. 6 Probabilities of success of well-behaved, first misbehaved and second misbehaved users success for the first case: (a) S_w, (b) S_{m1}, and (c) S_{m2}.

much less significant and the fairness of the system is still maintained when the number of available slots is large.

4.6 Performance Evaluation of Two Misbehaved Users

In the previous section, we have presented the study of misbehaviours separately for each misbehaving scenario to illustrate how each misbehaving strategy affects the well-behaved users and determine how much benefit the misbehaved user can gain. In this section, the study is extended to cover more general cases where there is more than one misbehaved user who may apply the same or different misbehaving strategies. Different mixes of misbehaved users should reveal another interesting aspect of this study such as the interaction between misbehaved users. Since there are many possible mixes of misbehaved users, and each may apply different misbehaving strategies, it is not possible to cover all cases. Therefore, three different mixes of two misbehaved users are selected to explain the key characteristic; details are as follows.

In the first case, both misbehaved users use the same misbehaving strategy, which is the multi-token mechanism. In the second case, both misbehaved users use the strategy of shifting the reservation time. In the third case, the first misbehaved user applies the multi-token strategy while the second misbehaved user applies shifting the reservation time strategy. In all cases, the first and second misbehaved users also change their permission probabilities, denoted as p_{m1} and p_{m2}, respectively.

Figures 6(a)–(c) show numerical results of the first case in terms of the probabilities of success of well-behaved users, the first misbehaved user and the second misbehaved user respectively, when the number of tokens of both misbehaved users is set to T = 4. The number of the contention slots is set to M = 32. Note that some numerical results that cannot be seen in Fig. 6 are shown in Table 2. When the first and second misbehaved users adopt small values of permission probabilities, the well-behaved users can obtain high probabilities of success, see Fig. 6(a). For example, when p_{m1} = 0.05 and p_{m2} = 0.05, we obtain S_w = 0.65. As the first misbehaved user increases its permission probability, its probabilities of success rise sharply due to the effect of multi-token mechanism while the well-behaved users become more and more affected and in the extreme case the probability of success is down to 0.53 for p_{m1} =1 and p_{m2} = 0.05. If the second misbehaved user also increases its permission probability, the effect on well-behaved users becomes more severe, because of more contention from the second misbehaved user. For example, the probability of success is down to 0.47 for p_{m1} = 1 and p_{m2} = 0.3. However, further increase of p_{m2} results in reversed effect; the probabilities of success of well-behaved users improve. This is because request packets from the two misbehaved users will collide against each other in the first few slots, leaving the remaining slots to become freer from contention. In an extreme case, where p_{m1} = 1 and p_{m2} = 1, we obtain S_w = 0.56. This behaviour agrees with numerical results of Figs. 6(b)–(c); the probabilities of success of both misbehaved users decrease with the increase of both p_{m1} and p_{m2} and converge to zero as both of them increase the permission probabilities toward one. This is because they will compete and affect each other when they use high permission probabilities.

Table 2 Details of the probabilities of success of well-behaved (S_w), first misbehaved (S_{m1}) and second misbehaved (S_{m2}) users for Figs. 6 and 7.

	p_{m1}	p_{m2}	S_{w}	S_{m1}	S_{m2}		p_{m1}	p_{m2}	S_{w}	S_{m1}	S_{m2}
The results of figure 6	0.4	0.4	0.4886	0.9532	0.9532	The results of figure 7	0.4	0.4	0.7080	0.6668	0.6668
	0.4	0.6	0.4823	0.9325	0.9206		0.4	0.6	0.7081	0.6080	0.6025
	0.4	0.8	0.4802	0.9213	0.8979		0.4	0.8	0.7092	0.5677	0.5585
	0.4	1.0	0.4775	0.9165	0.8844		0.4	1.0	0.7085	0.5370	0.5257
	0.6	0.4	0.4823	0.9206	0.9325		0.6	0.4	0.7081	0.6025	0.6080
	0.6	0.6	0.4903	0.8574	0.8574		0.6	0.6	0.7096	0.5044	0.5044
	0.6	0.8	0.4963	0.8004	0.7828		0.6	0.8	0.7116	0.4233	0.4202
	0.6	1.0	0.4984	0.7591	0.7236		0.6	1.0	0.7133	0.3546	0.3497
	0.8	0.4	0.4802	0.8979	0.9213		0.8	0.4	0.7092	0.5585	0.5677
	0.8	0.6	0.4963	0.7828	0.8004		0.8	0.6	0.7116	0.4202	0.4233
	0.8	0.8	0.5145	0.6340	0.6340		0.8	0.8	0.7135	0.2934	0.2934
	0.8	1.0	0.5262	0.4698	0.4437		0.8	1.0	0.7138	0.1768	0.1747
	1.0	0.4	0.4775	0.8844	0.9165		1.0	0.4	0.7085	0.5257	0.5370
	1.0	0.6	0.4984	0.7232	0.7571		1.0	0.6	0.7133	0.3497	0.3546
	1.0	0.8	0.5262	0.4437	0.4698		1.0	0.8	0.7138	0.1747	0.1768
	1.0	1.0	0.5570	0	0		1.0	1.0	0.7099	0	0

For the second case, where both misbehaved users shift their contention time, the probabilities of success of well-behaved users, the first misbehaved user and the second misbehaved user are shown in Figs. 7(a)–(c), respectively, when we set the shifted contention time for both misbehaved

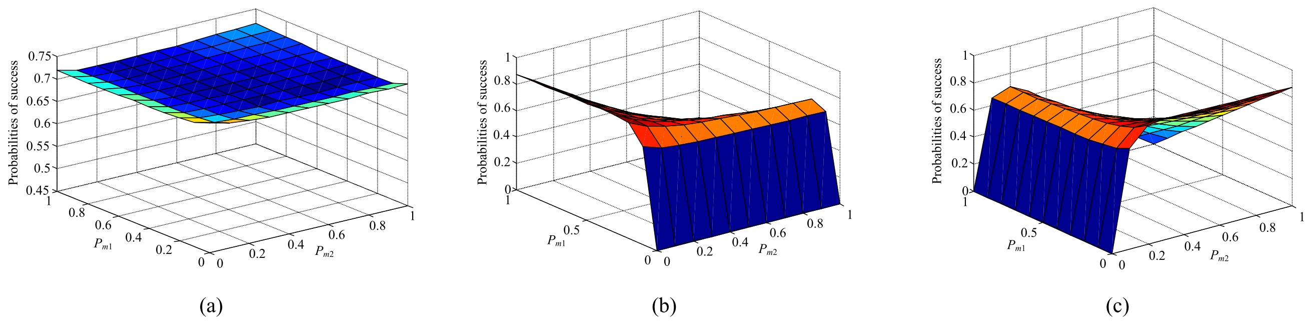


Fig. 7 Probabilities of success of well-behaved, first misbehaved and second misbehaved users success for the second case: (a) S_w, (b) S_{m1}, and (c)S_{m2}.

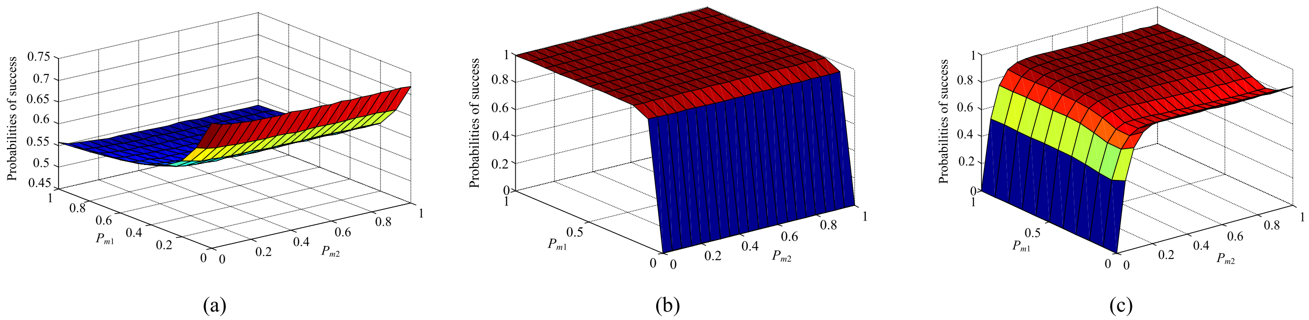


Fig. 8 Probabilities of success of well-behaved, first misbehaved and second misbehaved users success for the third case: (a) S_w, (b) S_{m1}, and (c) S_{m2}.

users as $D = M/2$, where $M = 32$. Figure 7(a) shows that this misbehaviour case does not exhibit much impact to the probabilities of success of the well-behaved users regardless of permission probabilities used by the misbehaved users. This is because the amount of contention is reduced by the two misbehaved users in the early contention slots such that there more chance for well-behaved users to obtain successful reservations as much as 0.72. On the other hand, the probabilities of success of the misbehaved users drop considerably as both of them adopt high values of permission probabilities. This two misbehaved users contend against each other in the later contention slots and suffer from collisions. The larger values of permission probabilities they use the more they suffer and their probabilities of success will reach zero in the extreme case when they both adopt permission probability as one as shown in Figs. 7(b)–(c). Note that some numerical results that cannot be seen in Fig. 7 are shown in Table 2.

Lastly for the third case when the two misbehaved users use different strategies. In this case, the first misbehaved user uses multi-token strategy with $T = 4$ and the second misbehaved user shifts its contention time by $D = M/2$, where $M = 32$. Figures 8(a)–(c) illustrate the probabilities of success of well-behaved users, the first misbehaved user and the second misbehaved user, respectively. Figure 8(a) shows that the existence of the first misbehaved user will cause significant effect to the performance of the well-behaved users. The impacts will be more significant when the greater value of p_{m1} is adopted. In contrast, the second misbehaved user does not cause performance degradation to the well-behaved users whichever value of p_{m2} used. As shown in Fig. 8(b), with $T = 4$, the first misbehaved user can maximize their probabilities of success as high as 1 by using the permission probabilities at least 0.2. The second misbehaved user also achieves good benefit by shifting its contention time, the probability of success of the second misbehaved user can be as high as 0.88. Note that there is a slight drop in the probabilities of success of the second misbehaved user when p_{m1} is between 0.1–0.3. This is because with these values of p_{m1}, the first misbehaved user tends to access in the later contention slots, where it interferes with the second misbehaved user. These results reveal that unlike the first two cases, when the misbehaved users apply different misbehaving strategies, they both can gain substantial advantages, as they exploit the available bandwidth differently such that contentions between them are less likely to occur.

5. Conclusions

In this paper, we have investigated the problem of user misbehaviours in reservation-based MAC protocols by focusing on how a selfish user may cheat on the contention resolution scheme to gain higher success than the other users. We first indentified and explained key misbehaving strategies that may arise, which include: i) the changes of the permission probabilities, ii) the use of multi-token, and iii) the shift of reservation time. We then present three different misbehaving scenarios based on the combinations of these misbehaving strategies, which enable us to systematically evaluate the extent in which the presence of misbehaviours affects those well-behaved users through comprehensive mathematical analyses. Next, we determine the maximum probabilities of success achievable by the misbehaved user and measure the fairness of the system by applying Jain's fairness index.

Results show that when only one misbehaved user exists and the user applies the misbehaving strategy of increasing the permission probability, the misbehaved user will gain only a small advantage over the well-behaved users while impacting them only slightly. In contrast, a significant gain is achieved by the misbehaved user while causing a severe impact to the well-behaved users when the strategies of increasing permission probability and using larger number of tokens are adopted together. Moderate benefit can also be achieved by the misbehaved user without causing severe negative impact to the well-behaved users by increasing its permission probability and shifting its first attempt. For the case of more than one misbehaved users, it appears that when the misbehaved users apply the same misbehaving strategies with high values of permission probabilities, they tend to compete against each other for channel accesses, causing negative impact upon themselves as well as those well-behaved users. However, when they apply different misbehaving strategies, it is possible that the misbehaved users become less interfering to each other, thus permitting them to take advantages of the available bandwidth better than when the same misbehaving strategy is employed.

Acknowledgments

The authors wish to thank the Commission on Higher Education of Thailand, the Department of Electrical Engineering, Burapha University, and AUN/SEED-Net, for financial support. We also sincerely thank Assoc. Prof. Hiroaki Morino at Shibaura Institute of Technology and Asst. Prof. Pongsatorn Sedtheetorn at Mahidol University for their valuable comments and suggestions.

References

[1] L. Guang, C.M. Assi, and A. Benslimane, "Enhancing IEEE 802.11 random backoff in selfish environments," IEEE Trans. Veh. Technol., vol.57, no.3, pp.1806–1822, May 2008.

[2] M. Raya, I. Aad, J.-P. Hubaux, and A.E. Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," IEEE Trans. Mobile Comput., vol.5, no.12, pp.1691–1705, Dec. 2006.

[3] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA Networks," Proc. IEEE INFOCOM, vol.4, pp.2513–2524, March 2005.

[4] P. Kyasanur and N.H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," IEEE Trans. Mobile Comput., vol.4, no.5, pp.502–516, Sept./Oct. 2005.

[5] Z. Lu, W. Wang, and C. Wang, "On order gain of backoff misbehaving nodes in CSMA/CA-based wireless networks," Proc. IEEE INFOCOM, pp.1–9, March 2010.

[6] IEEE standard for wireless LAN-medium access control and physical layer specification, P802.11, 1999.

[7] Y. Jin and G. Kesidis, "Distributed contention window control for selfish users in IEEE 802.11 wireless LANs," IEEE J. Sel. Areas Commun., vol.25, no.6, pp.1113–1123, Aug. 2007.

[8] M. Raya, J.-P. Hubaux, and I. Aad, "DOMINO: A system to detect greedy behavior on IEEE 802.11 hotspots," Proc. ACM MobiSys, pp.84–97, June 2004.

[9] W. Wang and X.-Y. Li, "Low-cost routing in selfish and rational wireless ad hoc networks," IEEE Trans. Mobile Comput., vol.5, no.5, pp.596–607, May 2006.

[10] S. Eidenbenz, G. Resta, and P. Santi, "The commit protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," IEEE Trans. Mobile Comput., vol.7, no.1, pp.19–33, Jan. 2008.

[11] P.P.C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G wireless networks," Proc. IEEE INFOCOM, pp.1289–1297, May 2007.

[12] P.P.C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," ELSEVIER Computer Networks, vol.53, pp.2601–2616, May 2009.

[13] S. Radosavac, A. Cárdenas, J.S. Baras, and G.V. Moustakides, "Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers," J. Computer Security, vol.15, no.1, pp.103–128, Jan. 2007.

[14] S. Dehnie and S. Tomasin, "Detection of selfish nodes in networks using coopMAC protocol with ARQ," IEEE Trans. Wireless Commun., vol.9, no.7, pp.2328–2337, July 2010.

[15] A.L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," IEEE Trans. Inf. Fore. and Sec., vol.3, no.3, pp.347–358, Sept. 2008.

[16] P. Serrano, A. Banchs, V. Targon, and J.F. Kukielka, "Detecting selfish configurations in 802.11 WLANs," IEEE Commun. Lett., vol.14, no.2, pp.142–144, Feb. 2010.

[17] C. Liu, Y. Shu, M. Li, and O.W.W. Yang, "A new mechanism to detect selfish behavior in IEEE 802.11 ad hoc networks," Proc. IEEE ICC, pp.1–5, June 2009.

[18] J. Konorski, "A game-theoretic study of CSMA/CA under a backoff attack," IEEE/ACM Trans. Netw., vol.14, no.6, pp.1167–1178, Dec. 2006.

[19] H. Inaltekin and S.B. Wicker, "The analysis of Nash Equilibria of the one-shot random-access game for wireless networks and the behavior of selfish nodes," IEEE/ACM Trans. Netw., vol.16, no.5, pp.1094–1107, Oct. 2008.

[20] B.G. Chun, K. Chaudhuri, et al., "Selfish caching in distributed systems: A game-theoretic analysis," Proc. Principles of Distributed Computing (PODC), pp.21–30, July 2004.

[21] S. Tasaka, K. Hayashi, and Y. Ishibashi, "Integrated video and data transmission in the TDD ALOHA-reservation wireless LAN," Proc. IEEE ICC, vol.3, pp.1387–1393, June 1995.

[22] J.-F. Frigon, V. Leung, and H. Chan, "Dynamic reservation TDMA protocol for wireless ATM networks," IEEE J. Sel. Areas Commun., vol.19, no.2, pp.370–383, Feb. 2001.

[23] X. Qiu, V.O.K. Li, and J.-H. Ju, "A multiple access scheme for multimedia traffic in wireless ATM," J. Mobile Networks and Applications, vol.1, no.3, pp.259–272, Dec. 1996.

[24] D. Raychaudhuri and N.D. Wilson, "ATM-based transport architecture for multiservices wireless personal communication networks," IEEE J. Sel. Areas Commun., vol.12, no.8, pp.1401–1414, Oct. 1994.

[25] N. Amitay and L.J. Greenstein, "Resource auction multiple access (RAMA) in the cellular environment," IEEE Trans. Veh. Technol., vol.43, no.4, pp.1101–1111, Nov. 1994.

[26] D.J. Goodman, R.A. Valenzuela, K.T. Gayliard, and B. Ramamurthi, "Packet reservation multiple access for local wireless communications," IEEE Trans. Commun., vol.37, no.8, pp.885–890, Aug. 1989.

[27] W. Srichavengsup, N. Sivamok, A. Suriya, and L. Wuttisttikulkij, "A design and performance evaluation of a class of channel reservation techniques for medium access control protocols in high bit-rate wireless communications," IEICE Trans. Fundamental, vol.E88-A, no.7, pp.1824–1835, July 2005.

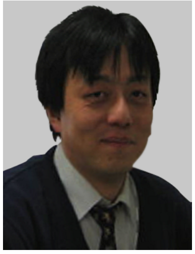
[28] IEEE Standard 802.16-2005, "IEEE standard for local and metropolitan area networks — Part 16: Air interface for fixed and mobile broadband wireless access systems," Dec. 2005.
[29] J. He, K. Guild, K. Yang, and H. Chen, "Modeling contention based bandwidth request scheme for IEEE 802.16 networks," IEEE Commun. Lett., vol.11, no.8, pp.698–700, Aug. 2007.
[30] Y. Fallah, F. Agharebparast, et al., "Analytical modeling of contention-based bandwidth request mechanism in IEEE 802.16 wireless networks," IEEE Trans. Veh. Technol., vol.57, no.5, pp.3094–3107, Sept. 2008.
[31] D. Bertsekas and R. Gallager, Data Networks. Prentice Hall, 1992.
[32] L. Kleinrock, "On queueing problems in random-access communications," IEEE Trans. Inf. Theory, vol.IT-31, no.2, pp.166–175, March 1985.
[33] A.S. Tanenbaum, Computer Networks, Third ed., Prentice Hall, 1996.
[34] T. Kim, J. Park, and B. Choi, "Throughput analysis of split-channel MAC with *p*-Persistent CSMA on the control channel and reservation scheme," Proc. ICT 2008, pp.1–5, June 2008.
[35] J. Deng, Y. Han, and Z. Haas, "Analyzing split channel medium access control schemes," IEEE Trans. Wireless Commun., vol.5, no.5, pp.967–971, May 2006.
[36] C. Chanasong, A. Suriya, W. Srichavengsup, and L. Wuttisittikulkij, "Channel reservation techniques under misbehaved users in high bit-rate wireless communications systems," Proc. IEEE TENCON, vol.3, pp.17–20, Nov. 2004.
[37] R. Jain, D. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," Digital Equip. Corp., Littleton, MA, DEC Rep., DEC-TR-301, Sept. 1984.

Norrarat Wattanamongkhol received the B.Eng. degree from Khon Kaen Uiversity and M.Eng. degree from King Mongkut's University of Technology Thonburi in Electrical Engineering in 2002 and 2006, respectively, in Thailand. He is currently pursuing the Ph.D. degree in electrical engineering, Chulalongkorn University, Thailand. His research interests include MAC protocols in wireless access networks, IEEE 802.11 and IEEE 802.16 standards.

Warakorn Srichavengsup received the B.Eng., M.Eng. and Ph.D. degree in Electrical Engineering from Chulalongkorn University, Bangkok, Thailand, in 1998, 2003 and 2009, respectively. He is currently a lecturer with the Department of Computer Engineering at Thai-Nichi Institute of Technology (TNI), Bangkok, Thailand. Prior to joining TNI, he was a visiting research student during 2008 with the Laboratory for Information and Decision Systems (LIDS) at the Massachusetts Institute of Technology (MIT). His main research interests are MAC protocol for high speed wireless local area networks.

Pisit Vanichchanunt received the B.Eng. degree (with Honors) in Telecommunication Engineering from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 1991. He received the M.Eng. and Ph.D. degrees in Electrical Engineering from Chulalongkorn University, Bangkok, Thailand, in 2001 and 2008, respectively. Now he is with the Department of Electrical and Computer Engineering, King Mongkut's University of Technology North Bangkok, Thailand. His main research interests are iterative decoding/demodulation, space-time codes, and signal processing for communications.

Robithoh Annur received the B.Eng. and M.Eng. degrees from Gadjah Mada University, Yogyakarta, Indonesia and National University of Singapore, Singapore, respectively. She is currently a Ph.D. student in the Department of Electrical Engineering, Chulalongkorn University, Thailand.



Jun-ichi Takada received B.E. and D.E. degrees from Tokyo Institute of Technology in 1987 and 1992, respectively. He was a Research Associate at Chiba University in 1992–1994, and an Associate Professor at Tokyo Institute of Technology in 1994–2006. He has been a Professor in Tokyo Institute of Technology since 2006. In 2003–2007, he was also a Researcher in National Institute of Information and Communications Technology. His current interests include the radiowave propagation and channel modeling for various wireless systems, and reguratory issues of spectrum sharing. He is a senior member of IEEE.

Lunchakorn Wuttisittikulkij received the B.Eng. degree from Chulalongkorn University Bangkok Thailand, the M.Sc. degree in Telecommunication and Information Systems and the Ph.D. in Telecommunications from the University of Essex, the United Kingdom. His research interests are multiple access control protocols for broadband wireless networks. In 1997, he joined the Department of Electrical Engineering the Faculty of Engineering Chulalongkorn University. He is presently an Associated Professor of Electrical Engineering. He has published over 60 papers internationally and authored 12 books (in Thai) in the field of telecommunications.