Kuwait J. Sci. **45** (**1**) pp 70-78, 2018

An analysis framework for the performance of collocated heterogeneous wireless networks with negative acknowledgements

Bilal khan[1,*], Jong-Suk Ahn[1], Eun-Chan Park[2]

[1]*Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea*

[2]*Dept. of Information and Communication Engineering, Dongguk University, Seoul, Korea*

**Corresponding author: bilalkhan83@hotmail.com*

Abstract

This paper proposes an analytical framework for evaluating the performance of coexistent heterogeneous wireless networks configured with different transmission powers and carrier sense thresholds. Two models, M-INF and M-MAC, are developed based on two-dimensional Markov chain. M-INF evaluates the effect of asymmetric channel access and interference among heterogeneous wireless networks, whereas M-MAC evaluates the effectiveness of a negative acknowledgement (NACK) mechanism. Results obtained from simulations are compared with those obtained from our proposed M-INF as well as conventional models, e.g., CHAM and HSM. It was found that simulations match our proposed models more closely than the conventional models. In addition, results obtained from M-MAC suggest that using NACK improves network performance by 40%.

Keywords: Binary exponential backoff; coexistence; heterogeneous; IEEE802.11; interference.

1. Introduction

Recently, there have been considerable research activities to precisely estimate and efficiently overcome severe performance degradation caused by frequent interferences among collocated heterogeneous wireless networks. This research area tends to attract attention since more heterogeneous wireless networks continue to be redundantly deployed in a small area with an aim of supporting an abundant number of wireless devices running a variety of applications. In these densely overlapped heterogeneous networks, nodes are forced to contend with others in the same network and simultaneously with nodes in their neighboring but different networks, which may run the same or different medium access control (MAC) protocols.

Several studies have proposed analytical models to analyze the effect of interference caused by one wireless network to another sharing the same frequency band. Park & Rim (2011) proposed the conventional heterogeneous analysis model (CHAM) for performance analysis of heterogeneous wireless networks and derived per-network throughput, when heterogeneous networks with different transmission powers coexist. However, CHAM does not consider the binary exponential backoff (BEB) algorithm (IEEE 802.11; 1999),and assumes that the size of contention window (CW) is fixed. Furthermore, CHAM uses negative acknowledgement (NACK) as a notification mechanism for transmission failure caused by inter-network collision assuming that NACK is never impaired, which is incorrect. Note that NACK was previously proposed by Pang *et al.* (2006)to notify the transmitter of transmission failure caused by erroneous channel.

In contrast to CHAM, the hidden station model (HSM) includes precise BEB behavior to measure the effect of transmissions from hidden nodes (Hung & Marsic, 2010). However, HSM does not suitably model interference among wireless networks, since it ignores the asymmetric aspect of inter-network interference that occurs when transmissions overlap in time but only one is successful while the other is unsuccessful. In the context of wireless sensor and actor network (WSAN), Ranga *et al.* (2016) proposed mechanisms to minimize the overlapped area in the acting region. The authors, however, ignored the effect of hidden sensors in the network on calculating the overlapped region.

The analytical model proposed in this paper considers variable CW size according to the BEB algorithm and also considers the effect of asymmetric interference due to disparate power levels of collocated networks. Moreover, heterogeneous wireless networks considered in this paper are assumed to be running the same IEEE 802.11 MAC protocol, but have different transmission powers and carrier sense thresholds. We also assume that these networks operate in the same channel because in unlicensed band, wireless networks are usually deployed in an unplanned manner. Therefore, as the density of network deployment increases, the chances that these networks may occupy the same channel of the same frequency band become very high.

Khan & Ahn (2013; 2014) presented preliminary versions of our proposed analytical model. However, their first model (Khan & Ahn, 2013) was limited to the evaluation of only two collocated networks and was not validated by simulations. Their latter work (Khan & Ahn, 2014) extended the previous model to evaluate N collocated networks, but it was still primitive since it did not provide an integrated framework to assess the effectiveness of NACK mechanism.

The aforementioned limitations in the research of Khan & Ahn (2013; 2014) are specifically addressed and eliminated in this paper. The current research broadens its application by incorporating the effects of various network parameters, such as payload sizes, data rates and network size, on interference. It proposes an analytical framework that hierarchically organizes two models. The first model is developed for infrastructure of heterogeneous wireless networks (M-INF) and second model incorporates NACK in individual wireless network (M-MAC). M-INF aims at discriminately abstracting both collision and interference within heterogeneous wireless networks. And M-MAC evaluates the effect of NACK in heterogeneous networks by incorporating NACK algorithm into Markov chains presented for M-INF. According to M-MAC, a transmitter receives NACK in the event of a transmission failure due to interference and does not increase its CW.

Results obtained from the proposed analytical framework were compared with simulation as well as conventional models. In contrast to conventional models, our proposed analytical framework was in close agreement with the simulation results. In addition, it was found that using NACK in heterogeneous wireless networks significantly improves performance. The following section describes the details of the proposed models.

2. Model for infrastructure of heterogeneous wireless networks (M-INF)

Figure 1 shows M-INF, which is based on Markov chain that is widely used for performance analysis of IEEE 802.11 MAC (Bianchi 2000).Each node state is identified by its backoff counter and backoff stage, which are modeled as two-dimensional discrete-time Markov process. Each state of the Markov chain is represented as $b_{i,c}$, which is the probability of a node to be in state (i, c), where $i \in [0,m]$, $c \in [0,W_i - 1]$, and W_i and m are the CW size at backoff stage i and the node retry limit, respectively. However, unlike the Markov chain model presented in Bianchi (2000), our proposed model considers the effect of asymmetric interference, which is not a straightforward extension of the former. M-INF classifies networks from N_1 to N_N into three types in terms of transmission power: weakest (N_1), middle (N_K), and strongest (N_N), as shown in Figure 1. The network N_K is overpowered by the stronger networks from N_{K+1} to N_N, while it dominates the remaining weaker networks from N_1 to N_{K-1}. Hence, when a node in the N_K networks ends a frame, all nodes in N_1, N_2,…, N_{K-1} networks can sense the channel busy and refrain transmission, but for nodes in N_{K+1}, N_{K+2},..., N_N networks due to their high carrier sensing thresholds the channel is still idle and may attempt transmission. M-INF focuses on predicting the upper and lower bounds on the performance that can be achieved by the strong and weak networks, respectively, when the strong network overwhelms weak networks.

The Markov chain for weakest network shown in Figure1(a) considers interference probability $p_{1,e}$, unlike the Markov chain presented by Bianchi (2000). For example, the successful transmission probability, $p_{1,s}$, of a given frame transmitted by a node in N_1 is $p_{1,s} = (1 - p_{1,c})(1 - p_{1,e})$, where $p_{1,c}$ and $p_{1,e}$ denote the intra-network collision and inter-network interference probabilities, respectively, of a given frame from N_1.

The Markov chain for the middle network N_K is shown in Figure 1(b). It includes *k-1* dotted boxes consisting of a set of N_K's states, which lead to interfering the ongoing transmission of its *k-1* weaker networks once N_K's backoff counter reaches 0 inside one of the boxes. For example, when network N_i $(i<k)$, transmits a frame and at the same time N_K enters dotted box, then thetransmission will be inevitably interfered.$\tau_{k,i}$ around box $I_{k,i}$ in Figure1(b) represents the probability that N_i is interfered by N_K. $V_{k,i}$ represents vulnerable period and is equivalent to the transmission time of one data frame of N_i during which its transmission is vulnerable to interference by N_K transmission. Since N_K itself is also prone to interference from stronger networks, i.e., N_j where $j \in [k+1, N]$,, its vulnerable period is scattered over Markov chain of N_j.

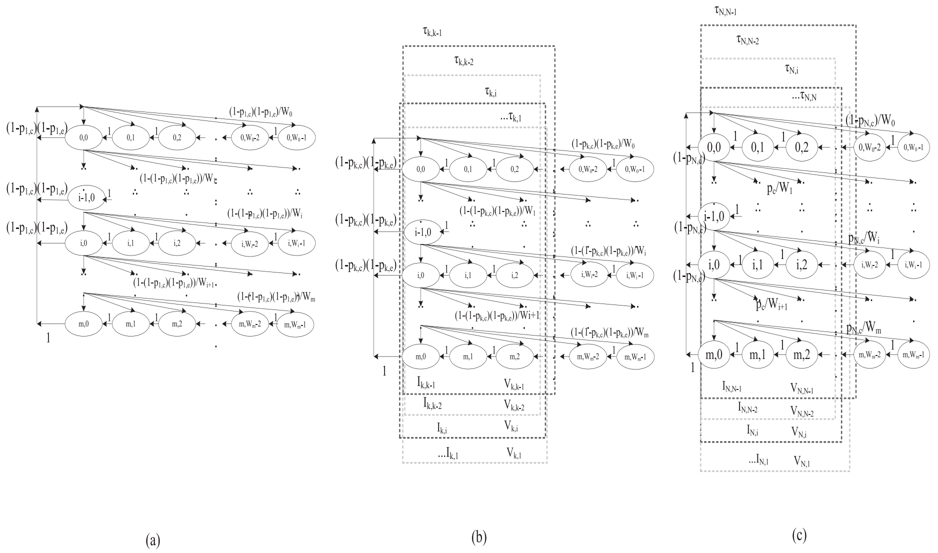

Fig. 1. Two-dimensional Markov chains for nodes from (a) weakest network,N_1; (b) middle networks,N_k(1 <*k*<*N*); and (c) strongest network, N_N.

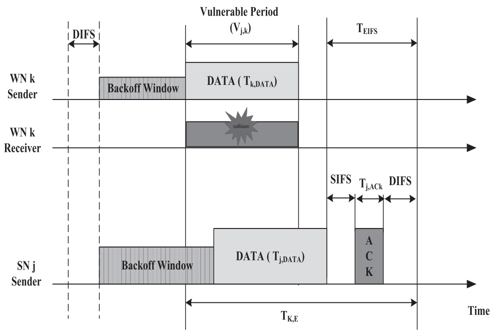

Fig. 2. Inter-network interference between weak network (WN) N_k and strong network (SN) N_j transmissions.

Figure 2 shows $V_{j,k}$, the transmission time of one data frame of N_K vulnerable to interference by N_j transmission .

Figure1(c) finally shows Markov chain for strongest network, N_N, containing (N-1) dotted boxes each of which represents a set of states resulting in interfering with the corresponding weak network's transmission.

2.1. Throughput derivation of N_k

In this subsection, we derive throughput equation for N_k. We consider only basic DCF as a channel access mechanism since the use of RTS/CTS (Request to Send / Clear to Send) has been proved ineffective when the interference range is larger than the transmission range, which is a common phenomenon in our work (Xu *et al*., 2003).From Figure 1(b) the transmission failure probability $p_{k,f}$ of a given transmission in N_k is

$$p_{k,f} = 1-(1-p_{k,c})(1-p_{k,e}) \tag{1}$$

where, $p_{k,c}$ and $p_{k,e}$ denote the probabilities of intra-network collision and inter-network interference, respectively, in N_k $p_{k,c}$ can be determined as

$$p_{k,c} = 1-(1-\xi_k)^{n_k-1} \tag{2}$$

wheren_k is the total number of nodes in N_k, and ξ_k is the probability that a node transmits a frame in a randomly chosen time slot, which can be derived by adding all state probabilities, $b_{i,0}$, when the remaining backoff counter reaches zero (Wu *et al*., 2002),

$$\xi_k = \sum_{i=0}^{m} b_{i,0} = b_{0,0}\frac{1-p_{k,f}^{m+1}}{1-p_{k,f}} \tag{3}$$

Here *m* is the maximum number of retransmissions. $b_{0,0}$ is the state probability when both backoff stage and remaining backoff counter are zero; and can be determined from Equation (4). In Equation (4), *m*'(≤ *m*) is the number of backoffs at which CW reaches maximum size, CW_{max}, and W_0 represents minimum CW size, CW_{mix}. Now $p_{k,e}$ is obtained as

$$p_{k,e} = 1-\prod_{j=k+1}^{N}(1-\tau_{j,k})^{n_j} \tag{5}$$

where n_j is the total number of nodes in N_j(*k*< *j* ≤ *N*), and $\tau_{j,k}$ is the probability that N_J transmits when N_k has already occupied the channel.

$\tau_{j,k}$ is derived in Equation (6)and is calculated by summing all the state probabilities, whose states are contained invulnerable box $I_{j,k}$ on the N_j Markov chain. X is the earliest backoff stage at which the CW of N_j is larger than $V_{j,k}$. As shown in Figure 2, N_j interferes the transmission of N_k, when the backoff stage X of the former is chosen such that $W_{x-1} < V_{j,k} \leq W_x$, where W_{x-1} and W_x are the CW sizes at backoff stages *X-1* and *X*, respectively. Equations (1)–(6) become a set of non-linear equations that can be solved using numerical methods (Karakaya etal., 2016).

Finally, throughput of N_k is

$$TH_k = \frac{P_{k,S} L_k}{P_{k,I} T_{k,I} + P_{k,S} T_{k,S} + P_{k,C} T_{k,C} + P_{k,E} T_{k,E}} \quad (7)$$

where L_k is the payload size, and $P_{k,s}$, $P_{k,I}$, $P_{k,C}$, and $P_{k,E}$ are the probabilities of successful transmission, idle channel, collision, and interference in a given time slot for N_k, respectively. These probabilities are derived in Equation (8).

$$\begin{cases} P_{k,S} = n_k \xi_k (1 - \xi_k)^{n_k - 1} (1 - p_{k,e}) \\ P_{k,I} = \prod_{i=k}^{N} (1 - \xi_i)^{n_i} \\ P_{k,E} = n_k \xi_k (1 - \xi_k)^{n_k - 1} p_{k,e} \\ P_{k,C} = 1 - P_{k,S} - P_{k,I} - P_{k,E} \end{cases} \quad (8)$$

$$b_{0,0} = \begin{cases} \dfrac{2(1-p_{k,f})(1-2p_{k,f})}{W_0(1-p_{k,f})(1-(2p_{k,f})^{m+1}) + (1-p_{k,f}^{m+1})(1-2p_{k,f})} & \text{when } m \le m' \\ \dfrac{2(1-p_{k,f})(1-2p_{k,f})}{W_0(1-p_{k,f})(1-(2p_{k,f})^{m'+1}) + (1-p_{k,f}^{m+1})(1-2p_{k,f}) + W_0 2^{m'} p_{k,f}^{m'+1}(1-p_{k,f}^{m-m'})(1-2p_{k,f})} & \text{when } m > m' \end{cases} \quad (4)$$

$$\tau_{j,k} = \sum_{i=0}^{m} \sum_{c=0}^{V_{j,k}} b_{i,c}$$

$$= \begin{cases} b_{0,0} \cdot \left(\left(\dfrac{W_0}{2}\right) \dfrac{1-(2p_{k,f})^X}{1-2p_{k,f}} + \left(\dfrac{1}{2}\right) \dfrac{1-p_{k,f}^X}{1-p_{k,f}} + (V_{j,k}+1) \dfrac{p_{k,f}^X - p_{k,f}^{m+1}}{1-p_{k,f}} - \dfrac{V_{j,k}(V_{j,k}+1)}{2W_0} \dfrac{\left(\dfrac{p_{k,f}}{2}\right)^X - \left(\dfrac{p_{k,f}}{2}\right)^{m+1}}{1-\dfrac{p_{k,f}}{2}} \right) & \text{when } 0 \le V_{j,k} \le W_{m'} \text{ and } 0 \le X \le m' \\ 1 & \text{when } V_{j,k} > W_{m'} \end{cases} \quad (6)$$

$P_{k,c}$ in Equation (7) differs from $P_{k,c}$ in Equation (2)in that the former is the probability that a given time slot in N_k is wasted due to collision,while the latter refers to the probability that a given frame sent from N_k is collided. $P_{k,E}$ in Equation (7) differs similarly from $p_{k,e}$ in Equation (5).

The four time intervals $T_{k,S}$, $T_{k,I}$, $T_{k,C}$, and $T_{k,E}$ in Equation (7) are the time slots consumed for successful transmission, idle channel, collision, and interference, respectively. In Equation(9), σ refers to the basic time unit stipulated in IEEE 802.11 standard; $T_{k,DATA}$ and $T_{k,ACK}$ refer to the transmission time of a data and acknowledgement (ACK) frame including the physical layer (PHY) and MAC headers, respectively; other intervals account for various inter-frame spaces defined in the IEEE 802.11 standard; $V_{j,k}/_2$ is the average number of time slots wasted by the interfered transmission; $T_{j,DATA}$ is the transmission time of a data frame, as shown in Figure 2.

$$\begin{cases} T_{k,I} = \sigma \\ T_{k,S} = T_{k,DATA} + 2\delta + T_{SIFS} + T_{k,ACK} + T_{DIFS} \\ T_{k,C} = T_{k,DATA} + \delta + T_{EIFS} \\ T_{k,E} = \dfrac{V_{j,k}}{2} \sigma + T_{j,DATA} + \delta + T_{EIFS} \end{cases} \quad (9)$$

where T_{EIFS} is the extended inter-frame N_j space and is equivalent to $T_{SIFS} + T_{j,ACK} + \delta + T_{DIFS}$.

3. Model for an individual wireless network with nack (M-MAC)

Now we develop M-MAC by incorporating the NACK mechanism into M-INF, as shown in Figure 3. The purpose of using NACK is to let the sender node know the cause of transmission failure. NACK is transmitted by intended receiver to sender, if a transmission failure is caused by interference otherwise neither ACK nor NACK is sent. When the sender node receives, NACK it refrains from increasing the size of its CW to prevent channel bandwidth being wasted. For more on using NACK, the reader is referred to Park & Lim (2011) and Pang *et al*. (2006).

To evaluate the effect of NACK in collocated heterogeneous networks, the Markov chains for each network in Figure 1 must be replaced with that shown in Figure 3. In M-MAC a node remains in the same backoff stage after receiving NACK with probability $p_{k,intf}$. However, when neither ACK nor NACK is received, the CW size is doubled with probability $p_{k,coll}$. Due to interference, a NACK frame is not guaranteed to be delivered. Upon successful transmission, CW is set to with probability 1-$p_{k,coll}$ - $p_{k,intf}$.

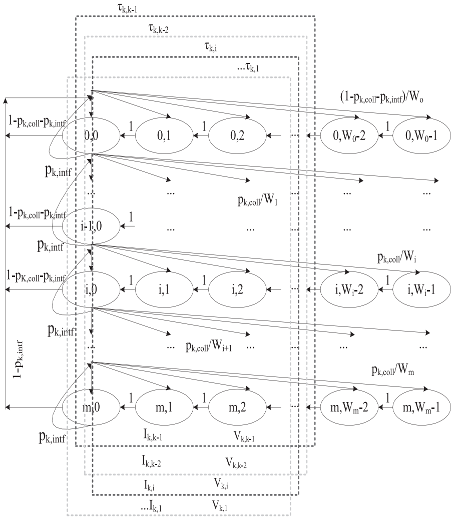

Fig. 3. Model for an individual wireless network with NACK.

$p_{k,intf}$ obtained from Equation (10), is the probability that only frame body is interfered, whereas frame header and its NACK are intact. Frame header is rarely interfered due to its small size. Therefore, when receiver receives only frame header correctly and not frame body it declares interference and feeds back a NACK based on the source address in the frame header of data frame.

On the other hand, $p_{k,coll}$ obtained from Equation (11) is the probability of transmission failure due to frame collision, frame header interference, NACK interference or ACK interference.

$$p_{k,intf} = (1 - p_{k,c})(1 - p_{k,H}) p_{k,B} (1 - p_{k,NACK}) \tag{10}$$

$$p_{k,coll} = \begin{cases} p_{k,c} + (1 - p_{k,c}) p_{e,H} + (1 - p_{k,c})(1 - p_{k,H}) p_{k,B} p_{k,NACK} \\ +(1 - p_{k,c})(1 - p_{k,H})(1 - p_{k,B}) p_{k,NACK} \end{cases} \tag{11}$$

In Equations (10) and (11) $p_{k,H}$, $p_{k,B}$, $p_{k,ACK}$, and $p_{k,NACK}$ are the probabilities of interference of frame header, frame body, ACK frame, and NACK frame for N_k , respectively, and can be calculated from Equation (5) by putting values of $V_{j,k}$ in Equation (6)according to the transmission duration of frame header, frame body, ACK, and NACK, respectively.

Let us define $p_{k,f}$ as the probability of transmission failure obtained from Figure (3) as

$$p_{k,f} = p_{k,coll} / (1 - p_{k,intf}) \tag{12}$$

Now we substitute the newly derived $p_{k,f}$ from Equation (12) into Equation (4) to obtain $b_{0,0}$ for M-MAC. M-MAC throughput can be calculated from Equation (7) by exchanging the four probabilities in Equation (8) with the corresponding ones in Equation (13) whereas, several time intervals $T_{k,S}$, $T_{k,I}$, $T_{k,C}$, and $T_{k,E}$ for M-MAC are same as in Equation (9).Table 1 summarizes and describes notations used in M-INF and M-MAC.

$$\begin{cases} P_{k,S} = n_k \xi_k (1 - \xi_k)^{n_k - 1} (1 - p_{k,H})(1 - p_{k,B})(1 - p_{k,ACK}) \\ P_{k,I} = \prod_{i=k}^{N} (1 - \xi_i)^{n_i} \\ P_{k,E} = n_k \xi_k (1 - \xi_k)^{n_k - 1} (1 - p_{k,H})((1 - p_{k,B}) p_{k,ACK} + p_{k,B} p_{k,NACK}) \\ P_{k,C} = 1 - P_{k,S} - P_{k,I} - P_{k,E} \end{cases} \tag{13}$$

4. Experiments

This section evaluates M-INFand M-MAC prediction accuracy by comparing their results with simulations. For experiment, heterogeneous wireless networks were virtually emulated in network simulator (ns-2) by grouping nodes into distinct networks depending on transmission power, distance between networks, carrier sensing threshold, and receiver sensitivity. The values of these parameters are shown in Table 2 (IEEE 802.11a 1999) and were carefully determined such that the transmission of a node could be sensed by all nodes in the same and weaker networks, but could not be sensed by nodes in the stronger networks.

Table 1. Reference index table for notations used in analysis model.

Notation	Description
N_k	k^{th}network.
ξ_k	Transmission probability of network N_k in a randomly chosen time slot.
$\tau_{j,k}$	Transmission probability of stronger network N_j into the vulnerable period $V_{j,k}$ of networkN_k.
$V_{j,k}$	Transmission time of a frame from networkN_k vulnerable to interference from stronger network N_j.
$p_{k,f}$	Probability of transmission failure of network N_k either due to collision or interference.
$p_{k,c}$	Probability that a transmission of network N_k is collided using M-INT.
$p_{k,e}$	Probability that a transmission of network N_k is suffered interference using M-INT.
$p_{k,coll}$	Probability that a transmission of network N_k is collided using M-MAC.
$p_{k,intf}$	Probability that a transmission of network N_k is suffered interference using M-MAC
$P_{k,S}$	Probability that the time slot is consumed due to successful transmission by network N_k.
$P_{k,C}$	Probability that the time slot is consumed due to collision by network N_k's transmission.
$P_{k,E}$	Probability that the time slot is consumed by interference of network N_k's transmission.
$P_{k,I}$	Probability that channel slot is idle.

Table 2. Parameters for experiments.

Parameters	Values	Parameters	Values
Data Rate	54 Mbps	SN Carrier Sensing Threshold	-40 dBm
Control Rate	24 Mbps	SN Receiver Sensitivity (RxTh)	-45 dBm
PHY Header	20 us	Capture Threshold (T_H)	10 dB
MAC Header	272 bits	ACK Frame	112 bits
WN Transmission Power	0 dBm	Payload	200 bytes
WN Carrier Sensing Threshold	-90 dBm	DIFS	34 µs
WN Receiver Sensitivity (RxTh)	-90 dBm	SIFS	16 µs
MN Transmission Power	17 dBm	Slot Time (σ)	9 us
MN Carrier Sensing Threshold	-64 dBm	Propagation Delay (δ)	1 us
MN Receiver Sensitivity (RxTh)	-70 dBm	CW_{min} (W_0)	15
SN Transmission Power	30 dBm	Retransmission Limit (m)	5

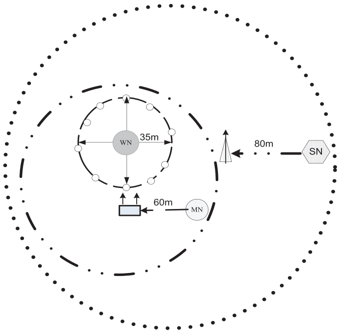

Fig. 4. Simulation topology of three coexistent heterogeneous wireless networks.

Figure 4 shows the experimental topology that assumes the collocation of three wireless networks; residential, indoor small and indoor large hotspots, denoted as weak (WN), middle (MN) and strong (SN) network, respectively. Three receivers were deployed, each at the center of their respective network, and transmitters were deployed at the perimeter of the circles. Transmission ranges of SN, MN and WN are shown in Figure 4 as the outermost pure-dotted circle, dashed-dotted circle and pure-dashed circle, respectively.

4.1. Evaluating M-INF accuracy

We first evaluate M-INF accuracy by comparing simulation with M-INF as well as CHAM and HSM, as shown in Figure 5. The observations from Figure 5 are summarized as follows.

- The proposed M-INF more accurately estimates WN throughput since simulation matches M-INF more closely than CHAM and HSM.
- Both CHAM and HSM remarkably overestimate WN throughput as compared to simulation by more than 3 times, i.e., CHAM and HSM produce significant modeling error.
- CHAM estimation error mainly results from the unrealistic assumption of constant CW size, without considering the BEB algorithm. This highlights that the BEB algorithm should be included in modeling interactions among heterogeneous networks.
- HSM estimation error is largely due to the fact that HSM only considers the symmetric interference, i.e., it assumes that all transmitted frames are lost, when they overlap whether fully or partially.

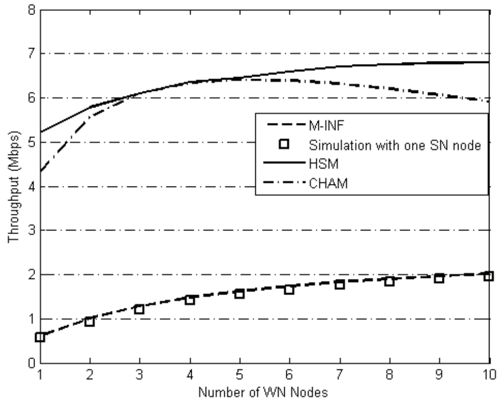

Fig. 5. Performance comparison among M-INF, CHAM, and HSM.

4.2. Performance evaluation of M-INF in heterogeneous networks

We investigate the performance of coexisting heterogeneous networks in various aspects including the throughput of strong and weak network, inter-network interference probability, effect of number of nodes, payload size, data rate, and ACK failure.

Figure 6 comparesWN throughput when it coexists with, (i) one SN node, (ii) two SN nodes, and (iii) one SN and one MN node.

When a WN consisting of 10 nodes coexists with one SN node, WN achieves throughput of approximately 2.0 Mbps. WN throughput drops to 0.75 Mbps as the number of coexisting SN nodes increases to 2.

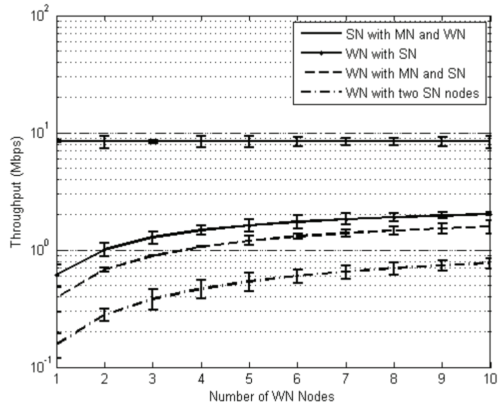

Fig. 6. Weak (WN) and strong (SN) network performances in the presence of each other and medium network (MN).

Furthermore, Figure 6 shows interesting results that the presence of a MN node and a SN node do not significantly reduce WN performance compared to the case, when there are two SN nodes. This is because the MN node does not get enough transmission opportunity in the presence of a SN node, causing less interference to WN. Finally, Figure 6 confirms that the SN throughput is not affected in the presence of MN and WN, and remains 8.3 Mbps regardless of the number of nodes in MN and WN. These results show significant throughput unfairness between SN and WN.

Figure 7 compares WN throughput for two cases: when ACKs are not interfered and interfered, indicated as 'invulnerable ACKs 'and 'vulnerable ACKs', respectively. Note that the results in Figures 5 and 6 were obtained under the assumption of invulnerable ACK.

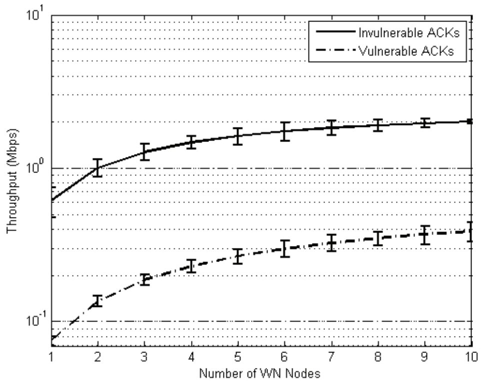

Fig. 7. Effect of acknowledgement (ACK) vulnerability on weak network (WN) performance.

WN throughput with vulnerable ACK is almost 1 /5 the case with invulnerable ACK. This is because ACK transmission is susceptible to interference, since it is transmitted by the receivers after a short inter-frame space (SIFS) without performing carrier sensing and, therefore, makes the previous long transmission of its data frame futile.

Figure 8 shows inter-network interference probability increases with respect to WN frame size and the number of interferers. For example, inter-network interference probability approaches 90% when WN transmits a frame having payload size 500 bytes, since the larger frame size expands the vulnerable period almost enough to cover the all the states in the SN's Markov chain. Interference probability is further increased, when the number of SN nodes increases to two. However, interference probability does not significantly increase in the presence of one MN and one SN node compared to the case of only one SN node since MN node does not get enough transmission opportunity in the presence of SN.

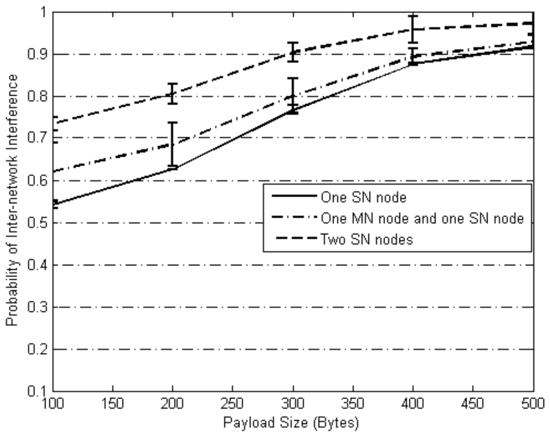

Fig. 8. Effect of payload size on interference probability.

Figure 9 shows that interference probability decreases, when the data rate increases, since transmitting a data frame with higher data rate reduces its transmission time, making WN transmission less vulnerable to interference from SN transmission. However, WN interference probability is high for all data rates, when there are two nodes in the collocated SN.

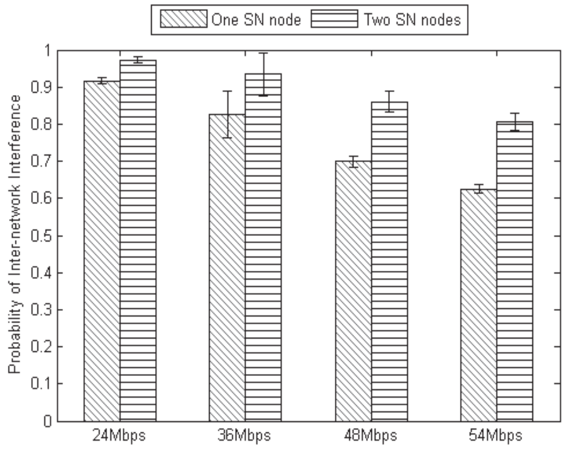

Fig. 9. Effect of data rate on interference probability.

4.3. Performance evaluation of M-MAC

In this subsection, we compare WN throughput with and without the NACK mechanism. Figure 10 shows that M-MAC estimated throughput closely matches simulation throughput, within the error-bar. The use of NACK improves WN throughput by over 40% when one SN node coexists with 10 WN nodes. Figure 10 also confirms that NACK still improves WN performance by more than 10% in the presence of two SN nodes. In the latter case, more than 70% of NACKs are disrupted by two SN nodes in contrast to less than 50%,when there is one node in SN. Figure 10 also compares WN throughput with and without NACK in the presence of one MN and one SN node.

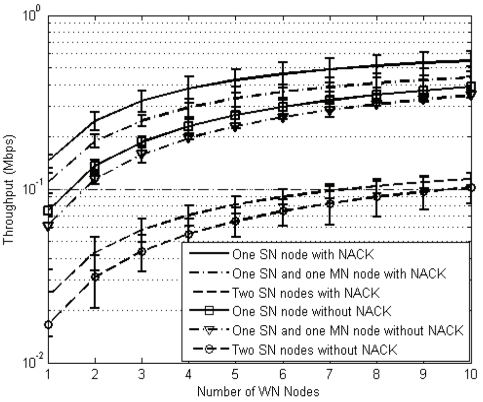

Fig. 10. WN performance with and without NACK.

5. Conclusion

We proposed an analytical framework to evaluate the interaction among contention based MAC protocols running in heterogeneous wireless networks. The framework was divided into two models: M-INF for interference, and M-MAC implementing an interference resistant algorithm, i.e., NACK.

We verified the effectiveness of the proposed models, showing that M-INF significantly improves prediction accuracy compared to the conventional (CHAM and HSM) by precisely abstracting the BEB algorithm and asymmetric aspects of heterogeneous wireless networks. The proposed M-MAC model was shown to accurately measure NACK effectiveness.

6. Acknowledgements

This research is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2012R1A1A2020051).

References

Bianchi, G. (2000). Performance Analysis of the IEEE 802.11 Distributed Coordination Function.IEEE Journal on Selected Areas in Communications, **18**(3):535–547.

Hung, F. Y. & Marsic, I. (2010). Performance analysis of the IEEE 802.11 DCF in presence of hidden stations. The International Journal of Computer and Telecommunications Networking, **7**(4):2674–2687.

IEEE 802.11a (1999). WG Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band.

Karakaya, V., Gursoy F.&Erturk M. (2016). Some convergence and data dependence results for various fixed point iterative methods. Kuwait Journal of Science, **43**(1):112–128.

Khan, B. & Ahn J.S. (2013). A performance model for the effect of interferences among the collocated heterogeneous wireless networks.15th International Conference on Advanced Communication Technology, South Korea.

Khan, B. & Ahn J.S. (2014). Modeling the effect of interferences among n collocated heterogeneous wireless networks. In proceedings of the International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), Tunisia.

Network simulator, ns-2, [Online; Dec 2016]. Available at: http://www.isi.edu/nsnam/ns/.

Pang, Q., Leung V. C. M. & Liew S. C. (2006). Improvement of WLAN Contention Resolution by Loss Differentiation. IEEE Transactions on Wireless Communications,**5**(12):3605–3615.

Park, E. C. & Rim, M. (2011). Fair coexistence MAC protocol for contention-based heterogeneous networks. The Computer Journal, **54**(8):1382–1397.

Ranga, V., Dave M. &Verma A. K. (2016). Optimal nodes selection in wireless sensor and actor networks based on prioritized mutual exclusion approach. Kuwait Journal of Science. **43**(1):150–173.

Wu, H., Peng, Y., Long, K., Cheng, S. & Ma, J. (2002). Performance of Reliable transport protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement. IEEE INFOCOM, NY, USA.

Xu, K., Gerla, M. & Bae, S. (2003). Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. Ad Hoc Networks, **1**(1):107–123.

Submitted: 15/08/2016
Revised : 24/01/2017
Accepted : 08/03/2017

إطاراً تحليلياً لقياس أداء الشبكات اللاسلكية غير المتجانسة المُجمعة مع الإشعارات السلبية

بلال خان[1]، *، جونغ–سوك آن[1] ، إون–تشان بارك[2]

[1] قسم علوم وهندسة الحاسوب، جامعة دونغقوك، سيول، كوريا

[2]قسم هندسة المعلومات والاتصالات، جامعة دونغقوك، سيول، كوريا

* bilalkhan83@hotmail.com

خــلاصــة

يعرض هذا البحث إطاراً تحليلياً لتقييم أداء الشبكات اللاسلكية القائمة غير المتجانسة التي تم تكوينها بقدرات إرسال مختلفة وعتبات تحسس الناقل. تم تطوير نموذجين، M-INF و M-Mac استناداً إلى سلسلة ماركوف ثنائية الأبعاد. ويعمل M-INF على تقييم تأثير نفاذ وتداخل القناة غير المتماثلة بين الشبكات اللاسلكية غير المتجانسة، بينما يعمل M-Mac على تقييم فعالية آلية الإشعار السلبي (NACK). تمت مقارنة النتائج التي تم الحصول عليها من المحاكاة مع تلك التي تم الحصول عليها من M-INF المُقترحة بالإضافة إلى النماذج التقليدية، مثل: CHAM و HSM. ووُجد أن عمليات المحاكاة تطابق النماذج المُقترحة بشكل أوثق من النماذج التقليدية. وبالإضافة إلى ذلك، تشير النتائج التي تم الحصول عليها من M-MAC أن استخدام NACK يعمل على تحسين أداء الشبكة بنسبة ٪40.