Biologically Inspired Consensus-Based Spectrum Sensing in Mobile Ad Hoc Networks with Cognitive Radios

F. Richard Yu and Minyi Huang, Carleton University
Helen Tang, Defense R&D Canada

Abstract

Cognitive radios, which are capable of sensing their surrounding environment and adapting their internal parameters, have been considered in mobile ad hoc networks. Secondary users can cooperatively sense the spectrum to detect the presence of primary users. In this article we present a novel biologically inspired consensus-based cooperative spectrum sensing scheme in CR-MANETs. Our scheme is based on recent advances in consensus algorithms that have taken inspiration from self-organizing behavior of animal groups such as birds, fish, ants, honeybees, and others. Unlike the existing cooperative spectrum sensing schemes, such as the OR-rule or the 1-out-of-*N* rule, there is no need for a common receiver to do the data fusion for reaching the final decision. A secondary user needs only to set up local interactions without a centralized node in CR-MANETs. Simulation results are presented to show the effectiveness of the proposed scheme.

The trend in wireless communications is such that advances demand ever increasing, and more efficient, use of limited spectrum resources. Regulatory agencies such as the Federal Communication Commission (FCC), are considering opening up licensed (primary) bands to unlicensed (secondary) operations on a non-interference basis to licensed users. One way to realize this is to adopt the idea of cognitive radio (CR), which is capable of sensing the surrounding environment and adapting its internal states by making corresponding changes in certain operating parameters [1]. CR technologies have been considered in mobile ad hoc networks (MANETs) [2], which enable wireless devices to dynamically establish networks without necessarily using a fixed infrastructure. In such a self-organized network, each node can pass information and control packets from one neighbor to another. CR-MANETs are gaining importance with the increasing number of potential applications, such as military battlefield communications, disaster relief, and autonomous vehicular communications [2].

Since primary user networks have no requirement to change their infrastructure for spectrum sharing, the task falls to CRs as secondary users in MANETs to detect the presence of primary users through continuous spectrum sensing. Spectrum sensing by CRs can be conducted either individually or cooperatively. Recently, the efficacy of cooperative spectrum sensing has garnered a great deal of attention. There are several advantages offered by cooperative spectrum sensing over the non-cooperative methods [3].

Although some work has been done in cooperative sensing, most of it uses a centralized center to do data fusion for the final decision whether or not the primary user is present. However, a centralized center is not available in CR-MANETs. Therefore, how to perform distributed cooperative spectrum sensing in CR-MANETs merits further investigation. On the other hand, the area of security in CR-MANETs has received relatively little attention. Some distinct characteristics of CRs introduce new nontrivial security risks to CR-MANETs. For example, locally collected and exchanged spectrum sensing information is used to construct a perceived environment that will impact CR behavior. This opens opportunities to malicious attackers. Two known security threats in CRs are incumbent emulation (IE) and spectrum sensing data falsification (SSDF). In an IE attack intruders emulate signals with the characteristics of incumbent primary users to fool other secondary users. A transmitter verification scheme is proposed in [4] to identify such IE attacks. In an SSDF attack, intruders send false local spectrum sensing results in cooperative spectrum sensing, which will result in suspect spectrum sensing decisions by CRs. The authors in [5] make fine attempts by suggesting several approaches to counter SSDF attacks. However, no further development is reported.

In this article we present a novel biologically inspired consensus-based spectrum sensing scheme without using a centralized center to improve the sensing performance and counter SSDF attacks in CR-MANETs simultaneously. Recently, biologically inspired mechanisms have become important approaches to handle complex communication networks, and they also lead to the design of efficient sensor network data harvesting algorithms from the point of view of multi-agent coordination [6]. Our scheme is based on recent advances in biologically inspired consensus algorithms [7]. An important motivational background of this area is initially related to the

0890-8044/10/$25.00 © 2010 IEEE

study of complex natural phenomena including flocking of birds, schooling of fish and swarming of ants and honeybees, among others (see the survey in [7]). The investigation of such biological systems has generated fundamental insights into understanding the relation between group decision making at the higher level and the individual animals' communication at the lower level [8, 9], and in fact consensus seeking in animal colonies is vital for group survival [8]. Such collective animal behavior has motivated many effective yet simple control algorithms for the coordination of multi-agent systems in engineering. Recently, consensus problems have played a crucial role in spatial distributed control models, wireless sensor networks, and stochastic seeking with noise measurement [10]. Since these algorithms are usually constructed based on local communication of neighboring agents, they have low implimentational complexity and good robustness, and the overall system may still function when local failure occurs. Concerning our secure spectrum sensing models, the basic requirements are to collectively determine the presence of the primary user and to filter out falsified data inserted by SSDF attacks, which can be viewed as a typical multi-agent coordination situation. The distinct features of the proposed scheme include:

- The consensus-based spectrum sensing scheme is a fully distributed and scalable scheme. Unlike many existing schemes, there is no need for a centralized center to do data fusion for reaching the final decision. Since it is rare to have a centralized node in CR-MANETs, in the proposed scheme a secondary user needs only to set up local interactions without centralized information exchange.
- Unlike most decision rules, such as OR-rule or n-out-of-N, adopted in existing spectrum sensing schemes, we use consensus from secondary users. The proposed scheme has self-configuration and self-maintenance capabilities, and is robust against SSDF attacks by using consensus to differentiate the trustworthiness of the local spectrum sensing reports received from each sensing terminal.
- Since the CR paradigm imposes human-like characteristics (e.g., learning, adaptation, and cooperation) in wireless networks, the biologically inspired consensus algorithm used in this article can provide some insight into the design of future CR-MANETs.

Some simulation results illustrate the effectiveness of the proposed scheme. It is shown that the proposed scheme can have both lower missing detection probability and lower false alarm probability, and significantly improve in identifying and preventing SSDF attacks.

The rest of the article is organized as follows. The next section presents spectrum sensing and SSDF attack models. In the following section the consensus-based spectrum sensing scheme is presented. Some simulation results are then given. Finally, we conclude this study in the final section.

Spectrum Sensing in CR-MANETs

In this section we first present the spectrum sensing problem in CR-MANETs. Then we introduce the SSDF attack models.

Spectrum Sensing

For many years radio spectrum has been assigned to licensed (primary) users. Most of the time, some frequency bands in the radio spectrum remain largely unoccupied by primary users. Spectrum usage measurements by the FCC show that at any given time and location, most of the spectrum is actually idle. That is, the spectrum shortage results from the spectrum management policy instead of the actual physical scarcity of usable spectrum. CR is considered an enabling technology that allows unlicensed (secondary) users to operate in the licensed spectrum bands. One important application of CR is spectrum overlay dynamic spectrum access (DSA), where secondary users operate in the licensed band while limiting interference with primary users. Spectrum opportunities are detected and used by secondary users in the time and frequency domain [1]. Three kinds of methods are widely used for spectrum sensing. Matched filter is optimal theoretically, but it needs prior knowledge of the primary system, which means higher complexity and cost to develop adaptive sensing circuits for different primary wireless systems. Energy detection is suboptimal, but it is simple to implement and does not have too much requirement on the position of primary users. Cyclostationary feature detection can detect signals with very low signal-to-noise ratio (SNR), but it still requires some prior knowledge of the primary user. In this article we consider the scenario where there is no prior knowledge of the primary user. In this case an energy detection spectrum sensing method [3] is a popular approach. The output of the energy detector is compared with a threshold to decide whether the primary user signal is present or not.

SSDF Attack Models in Cooperative Spectrum Sensing

In cooperative spectrum sensing a group of secondary users perform spectrum sensing by collaboratively exchanging locally collected information. Malicious secondary users may take advantage of cooperative spectrum sensing and launch SSDF attacks by sending false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision. Three attack models are presented as follows.

In the first attack model a malicious secondary user sends out a relatively high primary user energy to indicate the presence of primary users, although there is no primary user and its sensed energy is low. In this case other secondary users make a wrong decision that primary users are present and will not use the spectrum. The intention of the malicious secondary user is to gain exclusive access to the target spectrum. We call this kind of attack on selfish SSDF.

In the second attack model a malicious secondary user sends out a relatively low primary user energy to indicate the absence of primary users, although there are primary users and its sensed energy is high. In this case other secondary users make a wrong decision that there is no primary user and will use the spectrum. The intention of the malicious secondary user is to give interference to primary users. We call this kind of attack on interference SSDF.

In the third attack model a malicious secondary user sends out a random primary user energy during the process of cooperative spectrum sensing. That is, sometimes it sends out correct primary user energy; sometimes it sends out a false value. The intention of the malicious secondary user is to make other secondary users confused, so no consensus can be reached among secondary users. We call this kind of attack confusing SSDF.

Consensus-Based Spectrum Sensing Scheme

In this section we present the biologically inspired consensus-based spectrum sensing scheme without using a centralized center to improve sensing performance and counter SSDF attacks in CR-MANETs simultaneously. The scheme consists of three stages as follows.

In the first stage all the secondary users individually sense the target spectrum band based on the spectrum sensing models. We denote for user i, its measurement Y_i at time instant $k = 0$ by $x_i(0) = Y_i$.

In the second stage all the users establish the wireless communication links with their neighbors, and then locally exchange estimated energy levels among them. This process is done in iterations. The state update of the consensus variable for each secondary user occurs at discrete time instant $k = 0, 1, 2, \ldots$, which is associated with a given sampling period. In each time instant k, once receiving the updated estimated energy level $x_j(k)$ from neighbors, each user i first identifies the neighbor with the maximum deviation from the mean value to exclude a neighbor that is more likely to be an attacker. In turn, this procedure generates a subset of neighbors whose date will be used in updating the state $x_i(k + 1)$. Those iterations are done repeatedly until all of the individual states $x_i(k)$ converge toward a common value x^*. From $k = 0, 1, 2, \ldots$, the iterative form of the consensus algorithm can be stated as follows:

$$x_i(k+1) = x_i(k) + \varepsilon \sum_j \left(x_j(k) - x_i(k) \right), \quad (1)$$

where $0 < \varepsilon < \Delta^{-1}$, and Δ is called the maximum degree of the network.

Finally, by comparing the average consensus result x^* with a predefined threshold λ, every secondary user i gets the final data fusion locally: If $x^* > \lambda$, the primary user is present; otherwise, the primary user is absent.

If there is no attacker and we choose ε such that $0 < \varepsilon < 1/\Delta$, an average consensus will be ensured in that all the agents' states will converge to a common value x^* as the average of the initial state values. It can be further shown that the above algorithm can achieve an exponential convergence rate. By this averaging mechanism, some agents may reduce the uncertainty level of their information.

However, when an attacker is present, the basic consensus algorithm may not ensure-reliable decision since the attacker can persistently misguide one or more authentic agents, which may further spread wrong information to even more authentic agents. Consequently, it is necessary to modify the procedure involved in the original algorithm. Specifically, the neighborhood of each authentic user must be determined online according to the information it has received so that the user most likely to be an attacker is rejected. This step will give the network some ability to filter out wrong information. One method to identify an attacker is to find the neighbor with the maximum deviation from the mean value. Simulation results presented in the next section will show that this method is effective in countering SSDF attacks.

So far, we have assumed that any two neighboring nodes can reliably exchange data at all times. Hence, the network topology remains unchanged during the overall time period of interest. However, in real CR-MANETs signal fading can result in link failures. In this situation we can model the network as a random graph, and the proposed consensus-based spectrum sensing scheme can still converge. Please refer to [11] for details.

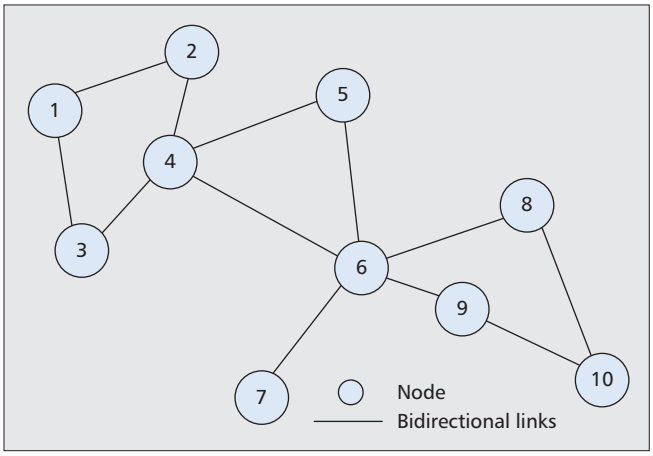

Figure 1. *A 10-node network without malicious attack.*

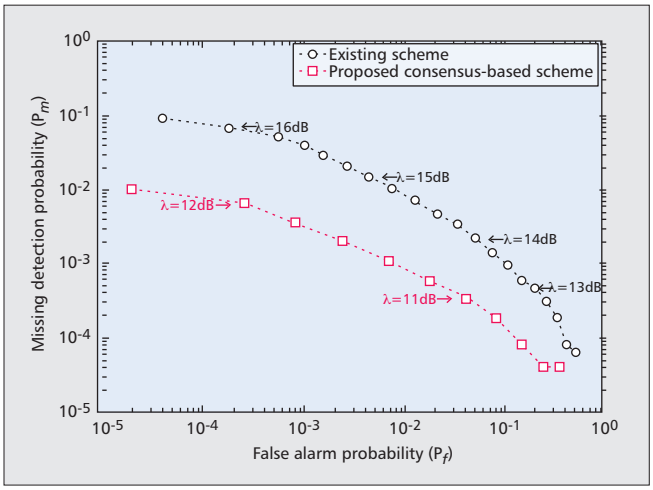

Figure 2. *Missing detection probability (P_m) vs. false alarm probability (P_f) in the 10-node network without malicious attack.*

Simulation Results and Discussions

In the simulations all secondary users are experiencing (i.i.d.) Rayleigh fading without spatial correlation. An energy detector is used by each secondary user. Each user has the same average $SNR(\overline{\gamma})$. The relevant information of primary users, such as position, moving direction, and moving velocity, is unknown to the secondary users. We consider two simulation scenarios: a 10-node network without malicious attack in Fig. 1 and a 17-node network with malicious attacks in Fig. 3. We compare the performance of the proposed scheme with that of an existing OR-rule cooperative sensing scheme [12], which is better than AND-rule and MAJORITY-rule in many cases of practical interest. In the OR-rule cooperative sensing scheme, each secondary user makes a local spectrum sensing decision, which is a binary variable — a *one* denotes the presence of a primary user, and a *zero* denotes its absence. Then all of the local decisions are sent to a data collector to sum up all local decision values. If the sum is greater than or equal to one, a primary user is believed to be present.

Before presenting the simulation results, we discuss briefly the relationship between P_m (probability of missing detection) $= 1 - P_d$ (probability of detection) and P_f (probability of false alarm). The fundamental trade-off between P_m and P_f has different implications in the context of dynamic spectrum sharing. A high P_m will result in the missing detection of primary users with high probability, which in turn increases the interference to primary users. On the other hand, a high P_f will result in low spectrum utilization since false alarms increase the number of missed opportunities (white spaces).

Figure 2 shows P_f vs. P_m in the 10-node network without malicious attack. We can see that the proposed scheme has better performance than the existing OR-rule cooperative sensing scheme. The numbers beside the curves are the corresponding thresholds λ in dB. In Fig. 2, if the threshold λ is in

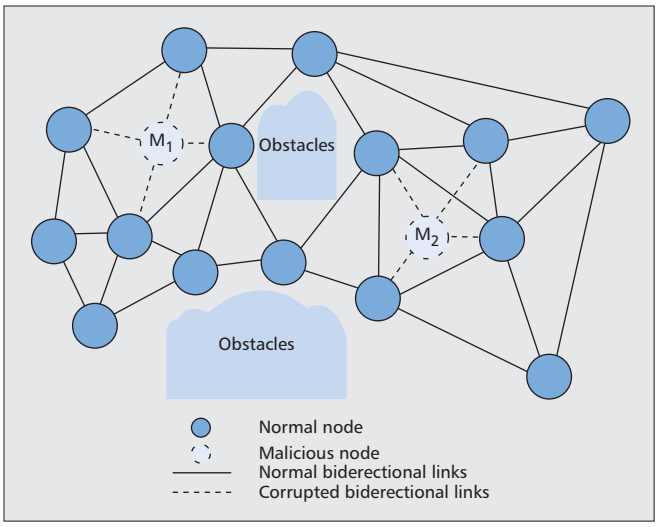

Figure 3. *A 17-node MANET with two malicious SSDF attacks.*

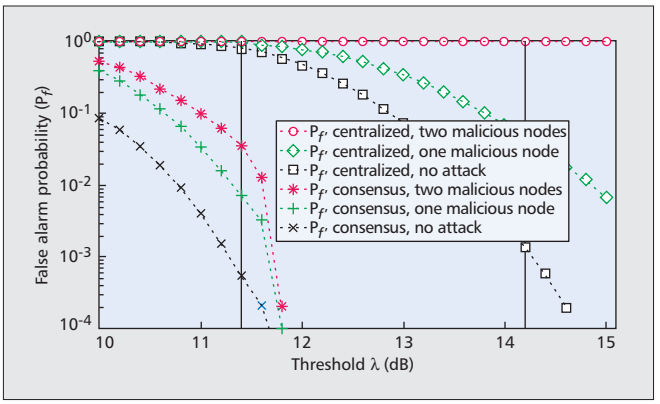

Figure 4. *False alarm probability comparison between the centralized decision fusion scheme and the consensus-based scheme.*

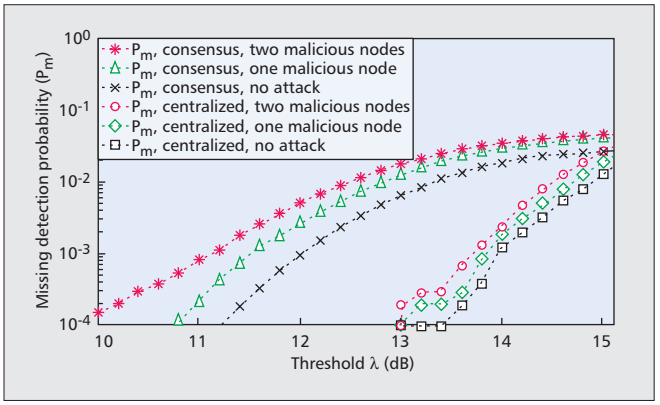

Figure 5. *Missing detection probability comparison between the centralized decision fusion scheme and the consensus-based scheme.*

the range of 11.4 to 12 dB, both P_f and P_m can simultaneously drop below the probability of 10^{-2} for the proposed consensus-based algorithm. In comparison, to reach the same goal, the existing OR-rule method must set λ to be around 14.8 dB, which has far worse P_m (10^{-2} vs. 10^{-3}) with regard to the same P_f level (10^{-2}).

Two selfish SSDF attacks are conducted in the 17-node network in Fig. 3. In the first attack user M_1 is compromised and sends out falsified data 20. In the second attack both users M_1 and M_2 are compromised; they send out falsified data 20 and 15, respectively. Figure 4 shows the results in terms of false alarm probabilities, and Fig. 5 shows the results in terms of missing detection probabilities. From Fig. 4, we can see that the consensus-based scheme is more robust than the existing centralized fusion scheme. When λ = 11.4 dB, the false alarm probability in the consensus-based scheme is lower than that in the centralized scheme in all of the following three cases: no attack, one attack, and two attacks. The centralized scheme is very vulnerable to selfish SSDF attacks, particularly in the two attacks case, where the false alarm probability is 1. This will result in severe performance degradation of the MANET. The spectrum utilization will be very low since false alarms increase the number of missed opportunities (white space). When the false alarm probability is 1, the MANET with CRs cannot find any spectrum opportunity under two malicious attacks. From Fig. 5, we can see that the missing detection probability is low in the centralized fusion scheme, even with two malicious attacks. This is because the centralized fusion scheme is a conservative scheme. That is, whenever there are some terminals (including selfish SSDF attacks) sensing the presence of primary users, it will not access the spectrum band, resulting in a low missing detection probability. Nevertheless, the consensus-based scheme has lower missing detection probabilities compared to the centralized scheme in all of the three different cases, which means that the consensus-based scheme can decrease the interference to primary users.

Conclusions and Future Work

In this article we have presented a distributed spectrum sensing scheme in CR-MANETs based on recent advances in biologically inspired consensus algorithms. Cooperative spectrum sensing is modeled as a multi-agent coordination problem. Secondary users can cooperatively sense the spectrum to detect the presence of primary users based on only local information exchange without a centralized receiver. We have also considered the SSDF attacks in CR-MANETs. Simulation results were presented to illustrate the effectiveness of the proposed scheme. It is shown that both missing detection probability and false alarm probability can be significantly reduced in the proposed scheme compared to those in an existing scheme. In addition, it is shown that the proposed scheme can differentiate the trustworthiness of spectrum sensing terminals, which makes it robust against SSDF attacks.

Future work is in progress to use other bio-inspired algorithms, such as those in [13], to improve the quality of service and security in MANETs with CRs.

References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE JSAC*, vol. 23, Feb. 2005, pp. 201–20.
[2] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive Radio Ad Hoc Networks," *Ad Hoc Net.*, vol. 7, July 2009, pp. 810–36.
[3] Y.-C. Liang *et al.*, "Sensing-Throughput Trade-off for Cognitive Radio Networks," *IEEE Trans. Wireless Commun.*, vol. 7, Apr. 2008, pp. 1326–37.
[4] R. Chen, J.-M. Park, and J. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE JSAC*, vol. 26, Jan. 2008, pp. 25–37.
[5] R. Chen *et al.*, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Commun. Mag.*, vol. 46, Apr. 2008, pp. 50–55.
[6] U. Lee *et al.*, "Bio-Inspired Multi-Agent Data Harvesting in a Proactive Urban Monitoring Environment," *Ad Hoc Net.*, vol. 7, no. 4, 2008, pp. 725–41.
[7] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and Cooperation in Networked Multi-Agent Systems," *Proc. IEEE*, vol. 95, Jan. 2007, pp. 215–33.
[8] P. K. Visscher, "How Self-Organization Evolves," *Nature*, vol. 421, Feb. 2003, pp. 799–800.
[9] I. D. Couzin, "Collective Cognition in Animal Groups," *Trends Cog. Sci.*, vol. 13, Dec. 2008, pp. 36–43.

[10] M. Huang and J. Manton, "Stochastic Consensus Seeking with Measurement Noise: Convergence and Asymptotic Normality," *Proc. Amer. Control Conf. '08*, Seattle, WA, June 2008.
[11] Z. Li, F. R. Yu, and M. Huang, "A Distributed Consensus-Based Cooperative Spectrum Sensing in Cognitive Radios," *IEEE Trans. Vehic. Tech.*, vol. 59, no. 1, Jan. 2010, pp. 383–93.
[12] K. B. Letaief and W. Zhang, "Cooperative Communications for Cognitive Radio Networks," *Proc. IEEE*, vol. 97, May 2009, pp. 878–93.
[13] F. Dressler, O. B. Akan, and A. Ngom, "Guest Editorial — Special Issue on Biological and Biologically-Inspired Communication," *Springer Trans. Comp. Sys. Biology*, vol. LNBI 5410, Dec. 2008.

Biographies

F. RICHARD YU [S'00, M'04, SM'08] (richard_yu@carleton.ca) received his Ph.D. degree in electrical engineering from the University of British Columbia in 2003. From 2002 to 2004 he was with Ericsson, Lund, Sweden, where he worked on the research and development of 3G cellular networks. From 2005 to 2006 he was with a startup in California, where he worked on research and development in the areas of advanced wireless communication technologies and new standards. He joined Carleton School of Information Technology and the Department of Systems and Computer Engineering at Carleton University in 2007, where he is currently an assistant professor. He received the Leadership Opportunity Fund Award from the Canada Foundation of Innovation in 2009 and best paper awards at IEEE/IFIP TrustCom 2009 and International Conference on Networking 2005. His research interests include cross-layer design, security, and QoS provisioning in wireless networks. He serves on the editorial boards of several journals, including *IEEE Communications Surveys & Tutorials*, *Wiley Journal on Security and Communication Networks*, and *International Journal of Wireless Communications and Networking*. He has served on the Technical Program Committees of numerous conferences and as the Co-Chair of ICUMT-CWCN '09, TPC Co-Chair of IEEE INFOCOM-CWCN '10, IEEE IWCMC '09, VTC-Fall '08 Track 4, and WiN-ITS '07.

MINYI HUANG [S'01, M'04] (mhuang@math.carleton.ca) received his B.Sc. degree from Shandong University, Jinan, China, in 1995, his M.Sc. degree from the Institute of Systems Science, Chinese Academy of Sciences, Beijing, China, in 1998, and his Ph.D. degree from the Department of Electrical and Computer Engineering, McGill University, Montreal, Canada, in 2003, all in the area of systems and control. From February 2004 to March 2006 he was a Research Fellow with the Department of Electrical and Electronic Engineering, University of Melbourne, Victoria, Australia. From April 2006 to June 2007 he was a research fellow with the Department of Information Engineering, Research School of Information Sciences and Engineering, Australian National University, Canberra. He joined Carleton University, Ottawa, Ontario, Canada, in July 2007, where he is an assistant professor in the School of Mathematics and Statistics. His research interests include stochastic control and game theory, cooperative multiagent stochastic systems, stochastic algorithms, and wireless networks.

HELEN TANG [M] (helen.tang@drdc-rddc.gc.ca) received her Ph.D. degree from the Department of System and Computer Engineering at Carleton University in 2005. From 1999 to 2005, she had worked in a few R&D organizations in Canada and the United States including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. In October 2005 she joined the Network Information Operations Section of Defence R&D Canada as a defence scientist. She has published more than 20 research papers in international journals and conferences including *IEEE Transactions on Wireless Communications*, *Journal of Security and Communication Networks*, IEEE ICC, IEEE VTC, IEEE MILCOM, and IEEE GLOBECOM. She has served as reviewer, session chair, and technical committee member for various conferences. Her research interests include ad hoc and sensor networks, wireless network security, communication protocols, and performance analysis.