

# Using Agents to Improve International Maritime Transport Security

Michal Jakob, Ondřej Vaněk, and Michal Pěchouček, Czech Technical University

**T**he recent surge in maritime piracy presents a serious threat to the international maritime transport system. Over the past few years, insurance rates have increased more than tenfold for vessels transiting known pirate waters, and the overall costs of piracy in the Pacific and Indian Oceans alone were estimated at up to US\$16 billion in 2008 and continue to rise.<sup>1</sup> To combat this problem, researchers have explored various measures for getting piracy back under control and for mitigating the risks it entails.

Inspired by the recent successful applications of the multiagent approach to other traffic and transportation domains,<sup>2,3</sup> we have developed a testbed for prototyping and evaluating agent-based techniques for understanding, detecting, anticipating, and eventually suppressing piracy and possibly other categories of maritime crime. Building on that testbed, we have investigated a range of specific coordination and planning methods for tackling the problem. The multitude of objectives, priorities, constraints, and complex scheduling dependencies, together with the necessity of transporters and ship operators to both cooperate and compete, makes maritime security a particularly good fit for applying agent-based techniques, which have been tackling many of these issues in a principled, well-founded way. To our best knowledge, our work is the first integrated attempt at employing agents in this domain.

## Agent-Based Simulation of Maritime Traffic

Agent-based simulation is a fundamental pillar of our approach. It provides a controlled environment for systematic experimentation with all the developed techniques. It also helps to overcome the lack of real-world data in certain areas (such

as good-quality traces of illegal vessels) by letting us supplement real-world data with synthetic data generated by the agent-based model. Although simulation has long been used for naval warfare purposes, there is little work on modeling civilian maritime traffic. The Matrics project,<sup>4</sup> which modeled the behavior of transport ships near the Canadian shore, seems to be the only case. The model used in Matrics is based on fluid mechanics and therefore has difficulties capturing vessel interactions and other more complex structures in maritime traffic. In contrast, numerous mature (agent-based) simulations are available for other traffic and transportation domains, such as air and road traffic.

## Vessel Agents

We focus on modeling three types of behavior: long-haul shipping, piracy, and patrolling. The *long-haul shipping behavior*, typically associated with large to very large vessels, consists of transporting cargo between two or more geographically distant locations. Except for the areas affected by piracy, long-haul shipping vessel movement is straightforward, following a route minimizing travel time and costs. The security of the passage, however, becomes an additional, major factor that must be accounted for when transiting pirate waters.

The *piracy behavior* contrasts strongly with the largely direct and predictable nature of long-haul shipping. Typically associated with small- to medium-sized vessels, pirate behavior aims at discovering, approaching, and attacking another vessel and—in the event of successful attack—hijacking the vessel and escorting it to one of the pirate home ports. Depending on their equipment and level of sophistication, pirates can use strategies ranging from simple uninformed roaming of high seas to

**Table 1. Implemented pirate strategies.**

Behavior	Description
Uninformed	Pirate vessel roaming the sea relying fully on direct observations within a limited range of sight
Radar	Pirate vessel equipped with radar significantly extending its observation range
Automated Identification System (AIS)	Pirate vessel monitoring AIS broadcasts revealing the exact position of broadcasting vessels
Mother ship with radar	Radar-equipped pirate vessel employing a mother ship with speed boats to significantly increase operational range
Mother ship with AIS	AIS broadcast-aware pirate vessel employing a mother ship with speed boats
Adaptive	Pirate vessel employing reinforcement learning to acquire knowledge from past successful attacks

employing radars, Automated Identification System (AIS) data monitoring, and the use of mother ships. Table 1 gives a list of implemented piracy behaviors.

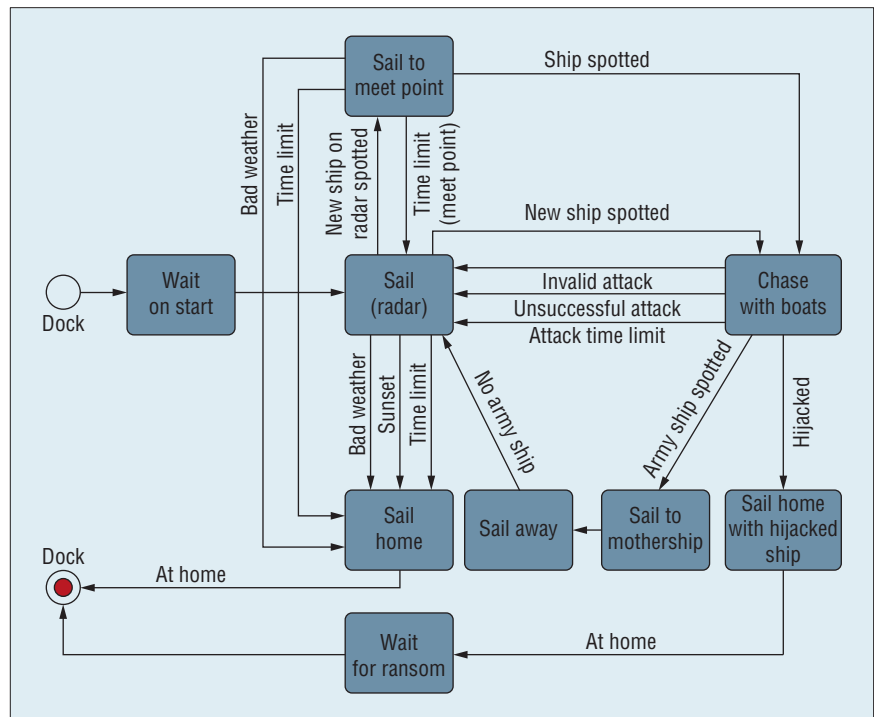
Finally, we implemented *patrolling behavior*. Used by security forces, this behavior is currently limited to patrolling the Gulf of Aden to maximize deterrence and minimize the risk of pirate attacks. In addition, we have implemented simple models of local traffic and fishing.

Each vessel behavior is represented using a finite-state machine. Despite its simplicity, the representation provides sufficient power to capture even the more complex behaviors, such as the pirate mother-ship strategy (see Figure 1).

**Data Sources**

The models we constructed and the overall simulation are based on real-world data, broadly distinguishable into these three categories:

- *Environmental data* describe the static and dynamic conditions of the environment in which the vessels operate—in particular coast-line, ports, transport corridors, weather, sea conditions, daytime, and season. These data are easy to obtain from public sources.
- *Vessel operational characteristics* describe the vessels’ physical properties such as vessel construction type, beam width, length, tonnage, and max speed. We obtained these data from vessel tracking servers



**Figure 1. Finite-state machine representing the pirate mother-ship strategy. The pirate vessel might use a mother ship with radar to significantly increase its operational range.**

- (such as VesselTracker.com) and use them to provide realistic parameters for simulated vessels.
- *Behavioral data* provide information about vessel behavior. This information can be either behavior-independent (such as observed vessel traces) or specific to a particular vessel behavior type (such as piracy strategies). We obtained the information from several specialized data sources, including vessel tracking servers and institutions working in the area of maritime security (such as the Maritime

Security Centre, Horn of Africa, [www.mschoa.eu](http://www.mschoa.eu)).

Collectively, these data sources let us construct more realistic and accurate models of maritime traffic.

**User Interface**

We use a Google Earth-based front end (see Figure 2) to interactively visualize the simulation’s output as well as all geographical and environmental data. An important feature of the front end is the ability to present structured data on varying levels of detail.

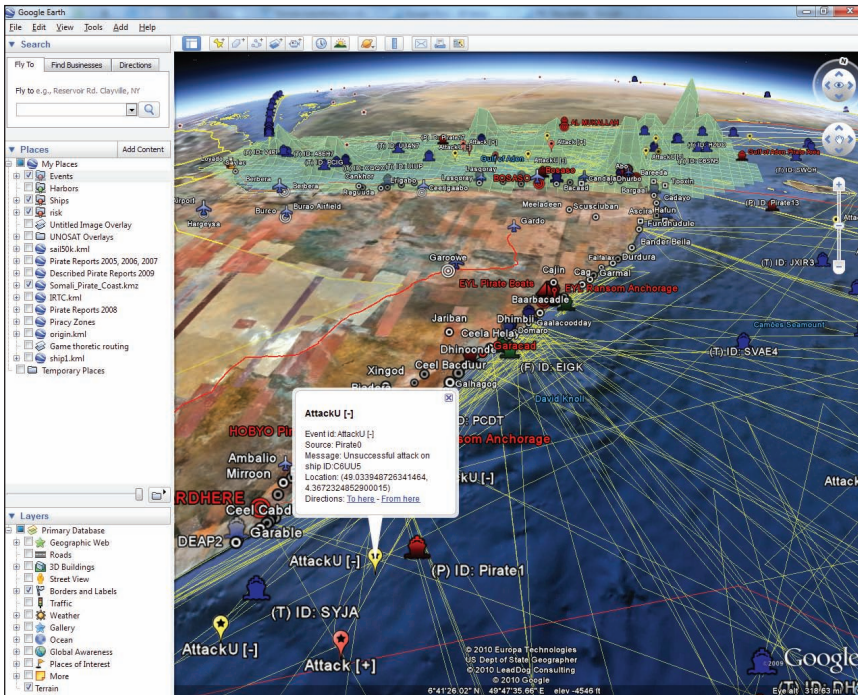


Figure 2. Google Earth-based front end to the maritime simulation platform. The interface shows vessels, their past trajectories, and important events, such as pirate incidents.

The layer-based interface lets us select different information layers and compose a picture with the aspects and the level of detail fit for the specific user's need.

We integrated Google Earth via dynamically created Keyhole Markup Language (KML) files served by an HTTP server running inside the platform. The KML files are periodically fed into the Google Earth application using its HTTP data-link feature and automatically refreshed. Using this innovative approach, we can display dynamic data (such as moving vessels) in Google Earth, turning it into a powerful base on which to build geographically enabled simulation interfaces.

### Strategic Transit Routing

Pirates are known for their ability to quickly adapt to new antipiracy measures and sustain their ability to carry out successful attacks. A case in point is the speed with which the pirates adapted to the introduction,

and subsequent alternation, of the international recommended transit corridor (IRTC) for vessels transiting the Gulf of Aden. The original intention was to narrow the area through which the vessels move to help protect them. However, the pirates took advantage of the predictability of their victims' movement and continued their attacks. Moreover, in wide, open areas with many different transit routes, such as the Indian Ocean, establishing transit corridors is even less effective.

Inspired by recent work in the area of security games, we have therefore investigated whether we can reduce the pirates' capacities by instilling a level of unpredictability into the route-selection process. Using a game theoretical framework, we came up with optimum randomization of the route selection process and generated risk-minimizing routes for vessels traversing known pirate waters. (A detailed technical discussion of our approach is available elsewhere.<sup>5</sup>)

We have formalized the problem of a vessel transiting a piracy-infested area as a zero-sum game, termed *transit game*, between two players: the *transporter* and the *attacker*. The transporter repeatedly traverses a rectangular area from an origin to a destination—that is, entry and exit points of the Gulf of Aden. The area is roamed by an attacker, which aims to determine an optimum ambush route starting and ending in its base and attack the transporter. The strategy set for the transporter is a set of all paths from the origin to the destination, and the attacker's strategy set is the set of all possible bounded-length closed walks from its base. Following their chosen routes, if the attacker and the transporter happen to be at the same position throughout its whole route, then the transporter wins. We defined the payoff to reflect the resource expenditure on the attacker's side and the chance of a rescue on the transporter's side. The payoff decreases (for the attacker) monotonously with the distance of the attack location from the nearest pirate base.

The solution of the game (for the transporter) is a probability distribution over possible routes representing the optimum randomization of transporter's route selection—that is, the selection strategy with the lowest expected payoff for the attacker. This selection strategy corresponds to a mixed Nash equilibrium of the transit game.

Unfortunately, the sizes of the strategy spaces for both players grow exponentially with the size of the game graph, making the search for a Nash equilibrium for even moderate graph sizes (tens of nodes) intractable. To mitigate this problem, we used two complexity reduction techniques.

The first technique utilizes an alternative, compact flow-based representation of the transporter's route selection strategies. The second technique employs the iterative single- and double-oracle algorithms for finding Nash equilibria.<sup>6</sup> Together, the techniques significantly enlarge the set of games for which a solution can be found in a reasonable time. Figure 3 depicts an example route selection strategy.

### Patrol Deployment

Due to the size of piracy-affected areas and the relatively small number of patrol resources, efficient planning and coordination of patrols is essential. We investigated algorithms for near-optimum placement of patrol vessels with respect to their deterrence potential. The input to the algorithm is the set of patrol vessels and the risk map (see Figure 4), representing the likelihood that a pirate attack might take place in a particular area. The algorithm output is the set of routes for each patrol vessel collectively maximizing deterrence and thus minimizing the risk of ambush in the target area.

The techniques we developed represent the first step in solving what in full is a complex multiagent planning and coordination problem. Individual patrol vessels belong to different countries and/or alliances and therefore have different objectives. The same is true for the transiting vessels, which might also form convoys to facilitate protection. Fundamentally, all this takes place in international waters with no single central authority and where measures can mostly only be recommended and not forced. Mediating interaction between different parties and brokering a solution that satisfies the different stakeholders' preferences and constraints in a balanced way is an area

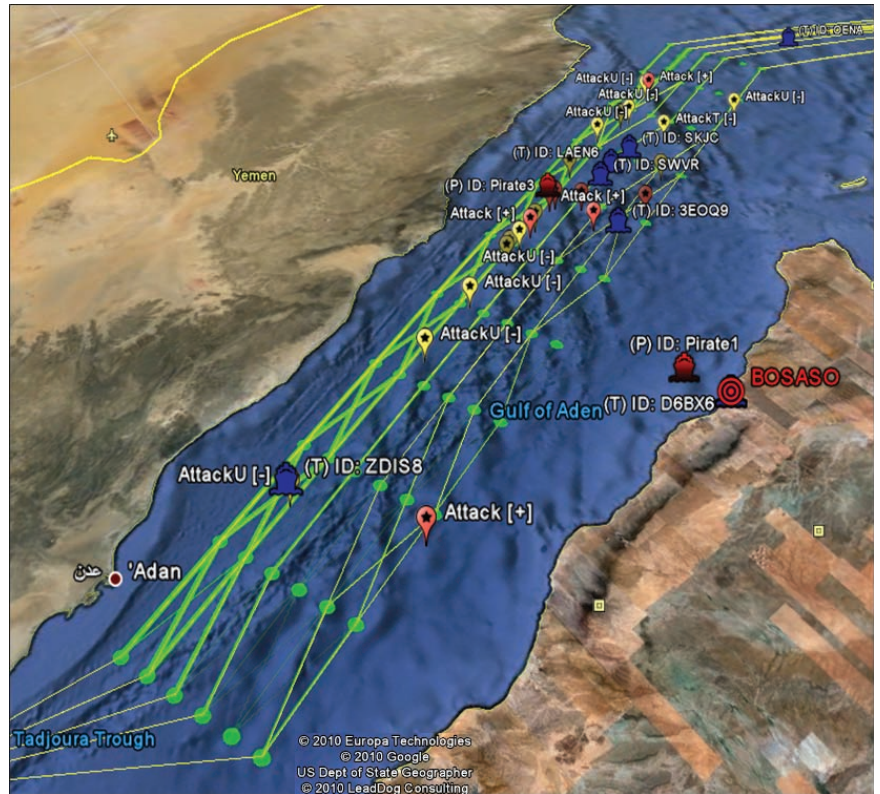


Figure 3. Strategic transit planning. The underlying graph represents a possible randomized route selection strategy (edge width corresponds to transition probability). The place marks represent successful and attempted attacks registered when the strategy was evaluated against simulated pirate vessels.

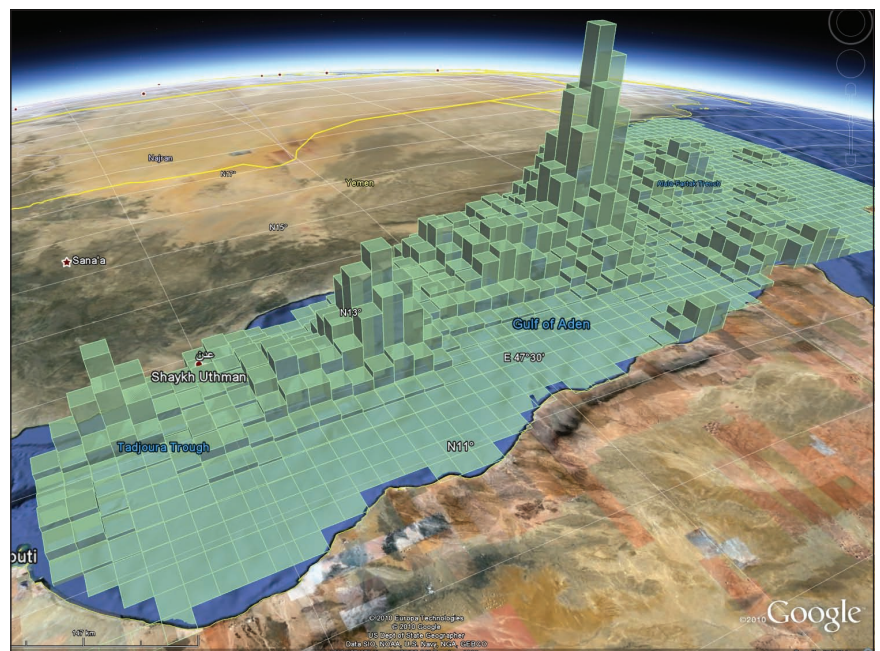
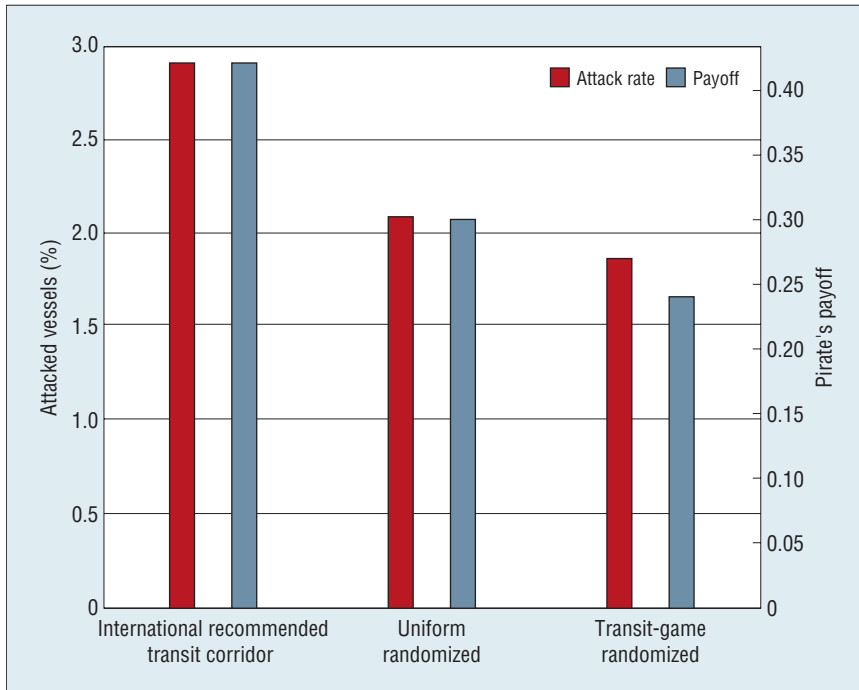


Figure 4. Pirate attack risk map created from historical data on piracy incidents and up-to-date transit vessel maps. The high map levels indicate a higher likelihood of a pirate attack.



**Figure 5. Percentage of attacked vessels and the accumulated payoff of pirates when using different gulf transit routing strategies. The transit-game randomized strategy yields superior results.**

with huge potential for agent-based techniques.

### Evaluation

To evaluate our approach, we must first evaluate the agent-based model to ensure sufficient correlation to real-world behavior. For long-haul shipping traffic, we did this by comparing real-world vessel traces with the traces generated by the simulation. Unfortunately, no such traces are available for pirate vessels; consequently, the only validation utilizing hard evidence possible was the comparison of generated pirate attack distribution with those observed in reality.

Second, we need to evaluate the individual planning and coordination methods. To test the validity of the transit game model and assess its usefulness in practice, we have evaluated the game-theoretic route selection algorithm on the simulation. We did not assume the pirates employ game theory to determine the

optimum way to roam the sea (although in theory they could, without any impact on the results presented). We assume that the pirates go to the sea repeatedly and learn from their previous experience. In the simulation, we emulate pirates' learning capability using a simple reinforcement learning scheme based on an arm-acquiring variant of the multiarmed bandit problem.

Figure 5 shows results comparing the overall number of attacks and total attacker's payoff for the original fixed, IRTC-based routing strategy, and the uniformly randomized and transit-game randomized route selection strategies. The results demonstrate the superiority of the randomized game-theoretic strategy, especially when we consider payoffs, and not just raw attack numbers.

**A**gent-based techniques have the potential to improve the security

of international maritime transport threatened by a steep rise of maritime piracy. We have demonstrated that a randomized route-selection strategy resulting from a normal two-player game formulation of the transit problem can decrease the number of attacks and the payoff accumulated by pirates. Coordinating the movement of patrol and transit vessels without a central authority requires techniques for semi-cooperative planning and coalition formation.

With regard to existing applications of agent-based techniques, the maritime domain seems currently underrepresented compared to other traffic and transportation domains. This work is a first step in addressing the situation and bringing this important domain into the focus of researchers in the multiagent systems field. ■

### Acknowledgments

This work is supported by the Office for Naval Research project number N00014-09-1-0537 and by the Czech Ministry of Education, Youth, and Sports under Research Program number MSM6840770038: Decision Making and Control for Manufacturing III.

### References

1. R. Gilpin, "Counting the Costs of Somali Piracy," working paper, US Inst. of Peace, 2009.
2. M. Jain et al., "Software Assistants for Randomized Patrol Planning for the LAX Airport Police and the Federal Air Marshal Service," *Interfaces*, vol. 40, no. 4, 2010, pp. 267–290.
3. M. Pěchouček and D. Šišlák, "Agent-Based Approach to Free-Flight Planning, Control, and Simulation," *IEEE Intelligent Systems*, vol. 24, no. 1, 2009, pp. 14–17.
4. S. Burton, Y. Gauthier, and J. Greiss, *MATRICES: A Maritime Traffic Simulation*, tech. report, Defense

R&D Canada, Center for Operational Research and Analysis, 2007.

5. O. Vaněk et al., “Transiting Areas Patrolled by a Mobile Adversary,” *Proc. IEEE Conf. Computational Intelligence and Games*, IEEE Press, 2010, pp. 9–16.
6. H.B. McMahan, G.J. Gordon, and A. Blum, “Planning in the Presence of Cost Functions Controlled by an Adversary,” *Proc. 20th Int’l Conf. Machine*

*Learning* (ICML), AAAI Press, 2003, pp. 536–543.

---

**Michal Jakob** is a senior researcher at the Czech Technical University. Contact him at [jakob@agents.felk.cvut.cz](mailto:jakob@agents.felk.cvut.cz).

---

**Ondřej Vaněk** is a researcher at the Czech Technical University. Contact him at [vanek@agents.felk.cvut.cz](mailto:vanek@agents.felk.cvut.cz).

---

**Michal Pěchouček** is a full professor and the head of Agent Technology Center at the Czech Technical University. Contact him at [pechoucek@fel.cvut.cz](mailto:pechoucek@fel.cvut.cz).

---

**cn** Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

“All writers are vain,  
selfish and lazy.”

—George Orwell, “Why I Write” (1947)

(except ours!)



The world-renowned IEEE Computer Society Press is currently seeking authors. The CS Press publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. It offers authors the prestige of the IEEE Computer Society imprint, combined with the worldwide sales and marketing power of our partner, the scientific and technical publisher Wiley & Sons.

For more information contact Kate Guillemette, Product Development Editor, at [kguillemette@computer.org](mailto:kguillemette@computer.org).

 **IEEE  
CSPress**  
[www.computer.org/cspress](http://www.computer.org/cspress)

Why

YOU



belong as a Member of  
**IEEE Computer  
Society**

**Need to keep up with developments in computing and IT?**

**Looking to enhance your knowledge and skills?**

**Want to shape the future of your profession?**

If you answered “yes” to any of these questions, IEEE Computer Society membership is definitely for you! With benefits that include:

- **Access to 600 titles from Safari® Books Online**, featuring the top technical and business online books from leading publishers such as O’Reilly Media.
- **Access to 3,500 online technical and professional development online courses**, provided by Element K.
- **Access to the newest emerging technologies** through your monthly subscription to COMPUTER magazine.
- **Access to conferences, publications, and certification credentials** at exclusive member-only savings.

Discover even more benefits and become an **IEEE Computer Society** Member today at

[www.computer.org](http://www.computer.org)

