On Modeling of Adversary Behavior and Defense for Survivability of Military MANET Applications

Ing-Ray Chen[†], Robert Mitchell[‡], and Jin-Hee Cho*

[†]Virginia Tech
Department of Computer Science
irchen@vt.edu

[‡]Sandia National Labs
Cybersecurity Department
rrmitch@sandia.gov

*U.S. Army Research Laboratory
Computational and Information Sciences Directorate
jinhee.cho@us.army.mil

Abstract— **In this paper we develop a methodology and report preliminary results for modeling attack/defense behaviors for achieving high survivability of military mobile ad hoc networks (MANETs). Our methodology consists of 3 steps. The first step is to model adversary behavior of capture attackers and inside attackers which can dynamically and adaptively trigger the best attack strategies while avoiding detection and eviction. The second step is to model defense behavior of defenders utilizing intrusion detection and tolerance strategies to reactively and proactively counter dynamic adversary behavior. We leverage game theory to model attack/defense dynamics with the players being the attackers/defenders, the actions being the attack/defense strategies identified, and the payoff for each outcome being related to system survivability. The 3rd and final step is to identify and apply proper solution techniques that can effectively and efficiently analyze attack/defense dynamics as modeled by game theory for guiding the creation of effective defense strategies for assuring high survivability in military MANETs. The end product is a tool that is capable of analyzing a myriad of attacker behaviors and seeing the effectiveness of countering adaptive defense strategies which incorporate attack/defense dynamics.**

Keywords*— *mobile ad hoc networks, reliability, adversary modeling, defense behavior modeling, survivability.

1. INTRODUCTION

In this paper we address the survivability issue of a military mobile ad hoc network (MANET) typically comprising sensor-carried human actors, vehicles, or robots assembled together for executing a specific mission. Our primary objective is to develop analytical models and performance metrics capturing the dynamics between adversary behavior and defense for high survivability of military MANETs. The end product is a tool that is capable of analyzing a myriad of attacker behaviors and seeing the effectiveness of countering adaptive defense strategies which incorporate attack/defense dynamics modeled by game theory with the players being the attackers/defenders, the actions being the attack/defense strategies identified in the paper, and the payoff for each outcome being related to system survivability.

The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 discusses adversary behavior modeling and defense behavior modeling. Section 4 discusses attack/defense dynamics modeling based on game theory. Section 5 presents performance analysis results. Finally Section 6 summarizes the paper and outlines future research areas.

2. RELATED WORK

While the importance of survivability of military MANET applications against malicious attacks is well recognized, the literature is thin in modeling and analysis of attack and defense strategies. To date, there are two lines of research in modeling and analysis. The first line of work focused on a formal process or framework to formalize safety and functional requirements utilizing formal modeling and analysis tools and then perform rigorous model verification [18]. The second line of work focused on a mathematical model for analyzing the system's response behavior in the presence of malicious nodes performing various attacks [3]. The basic idea is to develop a state-based stochastic process to model a system equipped with an intrusion detection system (IDS) presented with various types of attacks, with the objective to improve IDS designs so as to prolong the system lifetime. In this paper, we follow the second line of research work with the primary objective to capture the dynamics between adversary behavior and defense for survivability. We leverage our preliminary research experience on survivability of cyber physical systems [1, 2, 4, 5, 11] and wireless sensor networks [8, 12, 33] to model adversary behavior for survivability of military MANETs. We also leverage our research experiences in trust/reputation management for MANETs [14-16] and Internet of Things [34-36], and mechanism design [17] for modeling the attack/defense dynamics and the associated reputation-based payoff functions.

TABLE 1: SYSTEM FAILURE CONDITIONS.

Type	Meaning
Byzantine failure	Byzantine failure occurs when one-third or more of the nodes are compromised. The reason is that once the system contains more than 1/3 compromised nodes, it is impossible to reach a consensus, hence inducing a security failure.
Attrition failure	Attrition failure occurs when the MANET application does not have enough nodes to accomplish its intended functions.
Exfiltration failure	Exfiltration failure occurs when the aggressor secretes enough data to achieve an intelligence victory or leaks enough surveillance data to instrument a devastating attack.
Resource depletion failure	Resource depletion failure occurs when system resources (e.g., energy) are depleted to be able to accomplish the mission.

3. Attack/Defense Behavior Modeling

In this Section, we discuss adversary behavior modeling and defense behavior modeling. Later in Section 4 we will model attack/defense dynamics.

3.1 Adversary Behavior Modeling

For military MANETs, adversary behavior comes in two forms:

The 1st form of attacker behavior derives from capture attacker strategies to compromise nodes, i.e., to turn healthy nodes into compromised nodes. We consider the following capture attacker strategies:

- Random capture: capture attacks are random.
- Selective capture: capture attacks are selective and strategic so that "critical" nodes are targets of capture.
- Stuxnet-style capture: capture attacks grow exponentially with the number of compromised nodes who act as capture attackers.

The 2nd form of attacker behavior derives from inside attacker strategies to break the functionality of the system. We consider the following inside attacker strategies:

- Persistent: An inside attacker attacks recklessly.
- Random: An inside attacker attacks randomly to evade detection and to increase its chance of eventually damaging the system without being caught and evicted.
- Opportunistic: An inside attacker attacks opportunistically depending on what the environment is giving it, especially when there is high noise or high detection error due to incomplete information or low observability.
- Insidious: insidious nodes are hidden; they wait for a critical mass of bad nodes being formed to perform "all-in" attacks to break the system all at once.

While our list of attack strategies can expand, we initially consider random capture, selective capture, and Stuxnet-style capture to model capture attacker strategies in the 1st form of attack, and persistent, random, opportunistic and insidious to model inside attacker strategies in the 2nd form of attack. The adversary behavior of a capture attacker or an inside attacker will be dynamic and adaptive, triggering the best attack strategies while avoiding detection and eviction. For this, we will explore adversarial reasoning leveraging game theory to provide a means to model adversarial dynamic behavior. The detail will be described in Section 4.

3.2 Defense Behavior Modeling

We model defense behavior given a combination of intrusion detection and tolerance strategies being applied to reactively and proactively counter dynamic adversary behavior. Specifically, we investigate the use of behavior rule based monitoring [4, 5] for host-level intrusion detection system (host IDS) reactive strategies, i.e., each node acts actively as a monitoring node for its neighbors, and the use of dynamic voting [6, 7] for system-level intrusion detection system (system IDS) proactive strategies, i.e., a number of nodes is dynamically formed in the neighborhood of a target node acting as verifiers to perform voting to determine whether the target node is compromised.

In addition, a military MANET will have its basic functionality to fulfill. We consider a set of strategies for intrusion tolerance so that the basic functionality can be maintained albeit in degraded mode in the presence of attackers. We investigate the use of secure multipath routing [8, 12] to maintain connectivity as one strategy for fault tolerance. We also investigate moving targets for reduced observability against attacks as another possible intrusion tolerance strategy. The defense behavior generated by host IDS, system IDS and system intrusion tolerance strategies is manifested by a number of design parameters controlling the intrusion detection and tolerance strength as follows:

- At the host IDS level (i.e., based on reactive behavior rule monitoring), the detection strength is controlled by a "compliance degree" threshold parameter. A high threshold reduces the probability of missing a bad node (i.e., low false negatives) but increases the probability of misidentifying a good node as a bad node (i.e., high false positives). A defense adaptive behavior is to increase the compliance degree threshold to counter increasing adversary strength without hurting survivability due to excessive false positives.
- At the system IDS level (i.e., based on proactive dynamic voting), the detection strength is controlled by the number of verifiers and how often intrusion detection is performed to best tradeoff security gain vs. resource consumption especial in energy which is considered important for system survivability for rapidly deployed military MANETs without energy replenishment. A defense adaptive behavior is to control intrusion detection strength to counter increasing adversary

TABLE 2: ATTACK/DEFENSE STRATEGIES STUDIED.

Attack Strategies		Defense Strategies		
Capture attack strategies	Inside attack strategies	Host intrusion detection strategies	System intrusion detection strategies	System intrusion tolerance strategies
Random	Persistent	Controlling the increment of the “compliance degree” parameter to reduce false negative rate	Controlling the “number of verifiers” parameter for majority voting	Controlling the “number of disjoint paths” parameter for secure routing
Selective	Random	Controlling the decrement of the “compliance degree” parameter to reduce false positive rate	Controlling the “detection interval” parameter for detection strength tuning	Controlling the “number of versions” parameter for moving targets
				Controlling the “frequency of moves” parameter for moving targets
Stuxnet-style	Opportunistic			
	Insidious			

strength without hurting survivability due to excessive energy consumption, which is critical for mobile nodes often executing in a military MANET application without energy replenishment.

- At the system intrusion tolerance level (e.g., based on reactive secure multipath routing or based on moving targets), we model the defense behavior derived from controlling the amount of redundancy used (i.e., the number of disjoint paths in secure multipath routing and the number/frequency of versions/moves in moving targets against attacks) to counter adversary behavior without hurting system survivability due to excessive resource consumption.

The smart defense behavior will be dynamic and adaptive, triggering the best defense strategies in response to attack behavior. For this, we will explore defense reasoning leveraging game theory to provide a means to model defense dynamic behavior, described below in Section 4.

3.2 System Failure Conditions

We consider the following failure conditions which can possibly cause a military MANET application to fail:

- Byzantine failure occurs when one-third or more of the nodes are compromised. The reason is that once the system contains more than 1/3 compromised nodes, it is impossible to reach a consensus, hence inducing a security failure.
- Attrition failure occurs when the MANET application does not have enough nodes to accomplish its intended functions.
- Exfiltration failure occurs when the aggressor secretes enough data to achieve an intelligence victory or leaks enough surveillance data to instrument a devastating attack.
- Resource depletion failure occurs when system resources (e.g., energy) are depleted to be able to accomplish the mission.

Table 1 lists these system failure conditions.

4. Attack/Defense Dynamics Modeling

We apply game theory principles to model attack/defense dynamics. The players are attackers/defenders, the actions are the attack/defense strategies, and the payoffs for each outcome are related to system survivability. The objective of defenders is to bring up the survivability probability, while the objective of attackers is to bring it down.

The attack/defense strategies to be studied are listed in Table 2. A central piece of our approach is the payoff function which takes in a combination of attack/defense strategies as input and outputs a payoff for each player representing the extent to which the system survivability is improved (for a defender) or reduced (for an attacker). While there exist many forms for the payoff function, in this paper we consider the instantaneous system reliability $R(t)$ at time t to implement the payoff function. More specifically, each player (an attacker or a defender) is described by a separate continuous-time semi-Markov process, faithfully modeling its attack/defense behavior as prescribed by an attack/defense strategy chosen at time t. All players therefore interact with each other through these own continuous-time semi-Markov processes as time progresses. By utilizing SPNP [9] to implement these continuous-time semi-Markov processes, we can compute $R(t)$, given a set of failure conditions properly defined for a military MANET application (see Table 1). The payoff to a player is $R(t) - R(t\text{-}\Delta t)$ where Δt is the time epoch when the system reliability was last calculated by a player. Here we note that the system reliability calculation is performed by each player separately and independently using its own view (i.e., its own process) and interaction experiences with other players (through their processes). Also we note that collusion behavior is modeled through capture/insider attack behavior modeling for the worst case scenario that attackers know each other and will collude to perform the most opportunistic and insidious attacks to break down the system.

Here we notice that an inside attacker as a member of the MANET team is forced to play intrusion detection/tolerance defense strategies, or this uncooperative behavior will be detected and it will be labeled as a malicious node for eviction. A malicious insider, however, has the choice of whether to play intrusion detection/tolerance defense strategies faithfully (to avoid detection) or maliciously (to attack such as bad-mouthing a well-behaved node during voting in a system IDS execution). The intrusion detection/tolerance strategies nevertheless are essential "mechanisms" that must be played by every member of a military MANET team. Therefore, another design we consider to cope with inside attackers is based on mechanism design theory [13]. Mechanism design (also called reverse game theory) is a field of game theory. The main idea behind it is to construct mechanisms that provide the users the incentive to act in the way so as to further the interest of the designer. We consider the use of "reputation" as the incentive. That is, a node is awarded with reputation gain if it complies with defense protocol execution, and penalized with reputation loss if it deviates from defense protocol execution. Then a node is labeled as malicious for eviction when its reputation score falls below a system-defined threshold.

5. EVALUATION

We use a continuous-time semi-Markov stochastic process to describe each node's specific attack/defense behavior. This mathematical model formulation can take attack/defense dynamics modeled by game theory as input, and analyze the effect of attack/defense strategies for assuring high survivability of military MANETs. Specifically, we utilize stochastic Petri modeling techniques [9, 19-32] to define a continuous-time semi-Markov process describing the behavior of a node as time progresses, including the location of the node, its bad/good status, its attack behavior if it is a bad node, its defense behavior if it is a good node, its capability status for performing its intended functions including routing, host IDS and system IDS functions, and intrusion tolerance functions, and its energy status, thus providing information regarding whether a node is encountering with another node, whether it is compromised and is performing attacks, whether it is not compromised and is performing defense, whether it is competent to perform system functions at time *t*, etc. Conceptually, a node with its own stochastic process will go from one state to another, depending on its interactions (e.g., attack/defense strategies applied) with other nodes having their own continuous-time semi-Markov processes. This requires an iterative computational procedure be applied so that all semi-Markov stochastic processes converge, thus properly reflecting attack/defense dynamics with each other.

With this mathematical model formulation, we then study the effect of attack/defense behavior on system survivability, as a result of adaptively and dynamically applying attack/defense strategies. The output essentially is the system reliability or the probability of the MANET system survives over a mission period. We test a range of failure conditions applicable to military MANET applications, including attrition failure, exfiltration failure, Byzantine failure [10] and resource depletion failure. We also analyze the effect of incorporating game theory principles as discussed in Section 4 for effecting attack/defense dynamics on system survivability.

Below we report preliminary results of applying the proposed methodology to analyze the survivability of a MANET application with the following environment conditions and attack/defense strategies:

- There are n mobile nodes in an operational area. All are benign at the beginning.
- The attack strategies comprise "random" captures and "persistent" attacks (see Table 2). That is, all nodes have equal chance to be captured and then will be compromised into malicious nodes. Assume the per-node capture rate is λ. Also a compromised node will attack persistently in order to fail the system in the fastest pace.
- The defense strategies comprise (see Table 2):
  a) A host-level anomaly-based intrusion detection system with a false negative probability P_{fn} and a false positive probability P_{fp}. The reason is that a detection system often is not perfect. So it can misidentify a bad node as a good node with a false negative probability P_{fn} and conversely can misidentify a good node as a bad node with a false positive probability $P_{fp.}$ The knowledge of P_{fn} and P_{fp} can be obtained after thoroughly testing the anomaly detection technique.
  b) A system-level majority-voting based intrusion detection system with m being the number of verifiers used to perform majority voting (toward a target node) and T_{IDS}being the invocation interval to best balance energy conservation versus intrusion strength for achieving high survivability. Each invocation will cause a percentage P_e of the battery life to be drained. When the battery of a node is used up, it fails.
- There is no intrusion tolerance strategy used in the system to tolerate compromised attackers. When a node (good or bad) is diagnosed as compromised (through the system-level majority-voting based intrusion detection system), it is evicted.
- Without loss of generality we consider Byzantine failure and resource depletion failure conditions (see Table 1) for this MANET application.

TABLE 3: ATTACK/DEFENSE PARAMETERS FOR A MILITARY MANET APPLICATION.

Parameter	Meaning
n	Number of nodes
P_{fn}	False negative probability (host-level)
P_{fp}	False positive probability (host-level)
λ	per-node capture rate
m	Number of voters
T_{IDS}	Intrusion detection interval
P_e	Percentage energy spent per invocation

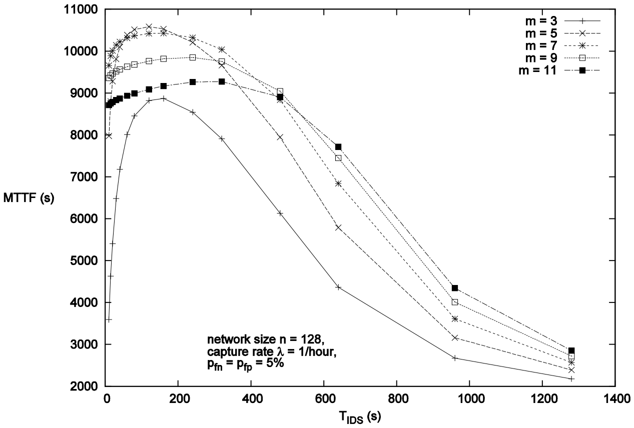

Figure 1: Analyzing the Effect of Attack/Defense Strategies on Survivability of a Military MANET Application with the Attack/Defense Parameters Listed in Table 3.

Table 3 List the attack/defense strategy parameters for this military MANET application. The performance metric is system survivability, measured by the mean time to failure (MTTF). Our methodology allows the defense parameter settings to be identified to maximize the MTTF.

Figure 1 shows the system survivability (in terms of MTTF) vs. T_{IDS} for the military MANET application for which n = 128, P_{fn}=P_{fp}=5%, λ = 1/hour, P_e= 0.01%, and the number of voters (m) in majority voting based intrusion detection varies from 3 to 11 in increments of 2 to test its effect. We first observe that an optimal T_{IDS} exists at which the MTTF is maximized to best trade energy consumption for intrusion detection strength. When T_{IDS} is too small, the system performs intrusion detection too frequently and quickly exhausts its energy, resulting in a small lifetime. As T_{IDS} increases, the system saves more energy and its lifetime increases. Finally when T_{IDS} is too large, even although the system can save more energy, it fails to catch bad nodes often enough, resulting in the system having many bad nodes. When the system has 1/3 or more bad nodes out of the total population, a Byzantine failure occurs.

We also observe that the optimal T_{IDS} is sensitive to the number of voters (m). As m decreases, the optimal T_{IDS} decreases because the system has to compensate less vigorous intrusion detection (i.e., a smaller m) by a higher invocation frequency (i.e., a smaller T_{IDS}) to prevent Byzantine failures. We see that m = 5 is optimal to maximize MTTF because too many voters would induce resource depletion failure, while too few voters would induce Byzantine failure. Using m = 5 can best balance resource depletion failure versus Byzantine failure for high survivability.

6. CONCLUSION

In this paper, we proposed a methodology for attack/defense behavior modeling with the goal to achieve high survivability of military MANET applications. Our methodology allows a full set of attack/defense strategies and environment/failure conditions to be specified and analyzed, including node mobility patterns (random is considered in this work), capture strategies, attack strategies, defense strategies, game playing mechanisms based on game theory principles, control mechanisms based on control theory principles, resources, initial energy, and role-based energy consumption rate. We exemplified the methodology with a simple yet practical military MANET application and demonstrated that there exist optimal defense parameter settings under which the system survivability in terms of the MTTF is maximized.

At this point we have not fully analyzed the effect of incorporating game theory principles for effecting attack/defense dynamics. It is a future research area.

ACKNOWLEDGMENT

This work is supported in part by the U.S. Army Research Office under contract number W911NF-12-1-0445.

REFERENCES

[1] R. Mitchell, and I.R. Chen, “Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems,” *IEEE Transactions on Reliability,* vol. 62, no. 1, March 2013, pp. 199-210.

[2] R. Mitchell, and I.R. Chen, “On Survivability of Mobile Cyber Physical Systems with Intrusion Detection,” *Wireless Personal Communications*, Elsevier, vol. 68, no. 4, 2013, pp. 1377-1391.

[3] R. Mitchell and I.R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications,” *Computer Communications*, vol. 42, 2014, pp. 1–23.

[4] R. Mitchell, and I.R. Chen, “Behavior Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications,” *IEEE Transactions on Smart Grid*, vol. 4, no. 3, Sept. 2013, pp. 1254 - 1263.

[5] R. Mitchell, and I.R. Chen, “Adaptive Intrusion Detection for Unmanned Aircraft Systems based on Behavior Rule Specification,” *IEEE Transactions on Systems, Man and Cybernetics,* vol. 44, no. 5, 2014, pp. 593-604.

[6] J.H. Cho and I.R. Chen, “Performance Analysis of Hierarchical Group Key Management Integrated with Adaptive Intrusion Detection in Mobile Ad Hoc Networks,” *Performance Evaluation*, Vol. 68, No. 1, 2011, pp. 58-75.

[7] J.H. Cho, I.R. Chen and P.G. Feng, “Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks,” *IEEE Transactions on Reliability*, Vol. 59, No. 1, 2010, pp. 231-241.

[8] H. Al-Hamadi and I.R. Chen, “Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, 2013, pp. 189-203.

[9] G. Ciardo, R.M. Fricks, J.K. Muppala and K.S. Trivedi, *Stochastic Petri Net Package (SPNP)*, Department Electrical Engineering, Duke University, 1999.

[10] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, 2982, pp. 382-401.

[11] R. Mitchell, and I.R. Chen, "Modeling and Analysis of Attacks and Counter Defense Mechanisms for Cyber Physical Systems," *IEEE Transactions on Reliability*, 2015, in press.

[12] H. Al-Hamadi and I.R. Chen, "Integrated Intrusion Detection and Tolerance in Homogeneous Clustered Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 11, no. 3, March 2015, article no. 47.

[13] L. Canzian, Y. Xiao, W. Zame, M. Zorzi, and M. van der Schaar, “Intervention with private information, imperfect monitoring and costly communication,” *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3192–3205, 2013.

[14] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, 2014, pp. 1200-1210.

[15] I.R. Chen, J. Guo, F. Bao and J.H. Cho, "Trust Management in Mobile Ad Hoc Networks for Bias Minimization and Application Performance Maximization," *Ad Hoc Networks*, vol. 19, August 2014, pp. 59-74.

[16] J.H. Cho, A. Swami and I.R. Chen, "Modeling and Analysis of Trust Management with Trust Chain Optimization in Mobile Ad Hoc Networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, May 2012, pp. 1001-1012.

[17] J. Wang, I.R. Chen. "Trust-based Data Fusion Mechanism Design in Cognitive Radio Networks." *IEEE CNS Workshop on Cognitive Radio and Electromagnetic Spectrum Security*, San Francisco, CA, Oct. 2014.

[18] A. B. Sharma, F. Ivancic, A. Niculescu-Mizil, H. Chen, and G. Jiang, “Modeling and Analytics for Cyber-Physical Systems in the Age of Big Data,” *ACM Sigmetrics*, 2013.

[19] I. R. Chen and D. C. Wang, “Analyzing Dynamic Voting using Petri Nets,” *15th IEEE Symposium on Reliable Distrib-uted Systems*, Niagara Falls, Canada, 1996, pp. 44-53.

[20] I. R. Chen and D. C. Wang, “Analysis of Replicated Data with Repair Dependency,” *The Computer Journal*, vol. 39, no. 9, 1996, pp. 767-779.

[21] I. R. Chen and F. B. Bastani,, “Effect of Artificial-Intelligence Planning-Procedures on System Reliability,” *IEEE Transactions on Reliability*, vol. 40, no. 3, 1991, pp. 364–369.

[22] I. R. Chen, F. B. Bastani, and T. W. Tsao, “On the Reliability of AI Planning Software in Real-time Applications,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 7, no. 1, 1995, pp. 4–13.

[23] F. B. Bastani, I. R. Chen, and T. W. Tsao, “Reliability of Systems with Fuzzy-Failure Criterion,” *Annual Reliability and Maintainability Symposium*, Anaheim, California, USA, 1994, pp. 442–448.

[24] I. R. Chen, T. M. Chen, and C. Lee, “Performance Evaluation of Forwarding Strategies for Location Management in Mo-bile Networks,” *The Computer Journal*, vol. 41, no. 4, 1998, pp. 243–253.

[25] B. Gu and I. R. Chen, “Performance Analysis of Location-Aware Mobile Service Proxies for Reducing Network Cost in Personal Communication Systems,” *Mobile Networks and Applications*, vol. 10, no. 4, 2005, pp. 453–463.

[26] O. Yilmaz and I. R. Chen, “Utilizing Call Admission Control for Pricing Optimization of Multiple Service Classes in Wireless Cellular Networks,” *Computer Communications*, vol. 32, 2009, pp. 317-323.

[27] I. R. Chen and T. H. Hsi, “Performance Analysis of Admission Control Algorithms based on Reward Optimization for Real-Time Multimedia Servers,” *Performance Evaluation*, vol. 33, no. 2, pp. 89-112, 1998.

[28] I. R. Chen and N. Verma, “Simulation study of a class of autonomous host-centric mobility prediction algorithms for wireless cellular and ad hoc networks,” *36th annual symposium on Simulation*, 2003, pp. 65-72.

[29] I. R. Chen, T. M. Chen, and C. Lee, “Agent-based forwarding strategies for reducing location management cost in mobile networks,” *Mobile Networks and Applications*, vol. 6, no. 2, 2001, pp. 105-115.

[30] S. T. Cheng, C. M. Chen, and I. R. Chen, “Dynamic Quota-based Admission Control with Sub-Rating in Multimedia Servers,” *Multimedia Systems*, vol. 8, no. 2, 2000, pp. 83-91.

[31] I. R. Chen, O. Yilmaz, and I. L. Yen, “Admission Control Algorithms for Revenue Optimization with QoS Guarantees in Mobile Wireless Networks,” *Wireless Personal Communications*, vol. 38, no. 3, 2006, pp. 357-376.

[32] Y. Li and I. R. Chen, “Design and Performance Analysis of Mobility Management Schemes Based on Pointer Forwarding for Wireless Mesh Networks,” *IEEE Transactions on Mobile Computing*, vol. 10, no. 3, 2011, pp. 349-361.

[33] H. Al-Hamadi and I.R. Chen, "Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks," *IEEE Transactions on Network and Service Management*, June 2015, in press.

[34] F. Bao and I. R. Chen, “Dynamic Trust Management for Internet of Things Applications,” *2012 International Workshop on Self-aware Internet of Things*, San Francisco, CA, USA, Sept. 2012, pp. 1-6.

[35] I. R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Service Computing*, 2015, in press.

[36] I. R. Chen, F. Bao, and J. Guo, “Trust-based Service Management for Social Internet of Things Systems,” *IEEE Trans. on Dependable and Secure Computing*, 2015, in press.