Trust-based Service Management of Mobile Devices in Ad Hoc Networks

Yating Wang, Ing-Ray Chen
Virginia Tech
Department of Computer Science
Falls Church, VA, USA
Email: {yatingw, irchen}@vt.edu

Jin-Hee Cho
U.S. Army Research Laboratory
Computational and Information Sciences Directorate
Adelphi, MD, USA
Email: jinhee.cho@us.army.mil

***Abstract*— With the proliferation of fairly powerful mobile devices and ubiquitous wireless technology, traditional mobile ad hoc networks (MANETs) now migrate into a new era of service oriented MANETs wherein a mobile device can provide and receive service from other mobile devices it encounters and interacts with. We discuss our ongoing research efforts in trust management and trust-based algorithm design for service-oriented MANET applications to answer the challenges of MANET environments, including no centralized authority, dynamically changing topology, limited bandwidth and battery power, limited observations, unreliable communication, and the presence of malicious nodes who act to break the system functionality as well as selfish nodes who act to maximize their own gain. We also highlight key ideas and experiences learned, and provide future research directions.**

Keywords-service-oriented mobile ad hoc networks; multi-objective optimization; trust; performance analysis.

I. INTRODUCTION

An autonomous service-oriented mobile ad hoc network (MANET) is populated with service providers (SPs) and service requesters (SRs). A realization of service-oriented MANETs is a web-based peer-to-peer service system with mobile nodes providing web services and users (through their mobile devices) invoking web services. Unlike a web service system in which nodes are connected to the Internet, nodes in service-oriented MANETs are mobile and the communication between peers not within radio range is multi-hop with nodes in the system serving as routers. One can view a service-oriented MANET as an instance of Internet of Things (IoT) systems [7] with a wide range of mobile applications including smart-city, smart tourism, smart car, smart environmental monitoring, and healthcare [1]. It is particularly suitable to military applications where all nodes are mobile with multi-hop communication.

This paper discusses our ongoing research work in trust management and trust-based algorithm design for service-oriented MANETs, key ideas and experiences learned, and future research directions. Our aims are to (1) identify trust dimensions for service-oriented MANET applications; (2) develop an efficient and effective trust protocol for service-oriented MANETs; and (3) develop efficient and effective trust-based algorithms for a set of service-oriented MANET applications. The overarching principle is the design notion of adaptive control, allowing trust computation, aggregation, propagation, formation (out of multiple trust dimensions) and update decisions to be dynamically adjusted to minimize trust bias and maximize application performance. This goal is to be achieved in the presence of malicious mobile devices performing a wide range of attacks, including bad-mouthing, ballot-stuffing, packet dropping, opportunistic service, self-promotion, conflicting behavior, and on-off service attacks for personal gain.

The rest of the paper is organized as follows. Section II discusses related work. Section III discusses the threat model for service-oriented MANETs. Section IV presents our solutions toward trust management of mobile devices in service oriented MANETs. Section V presents our solutions toward trust-based service management for performance optimization of service-oriented MANET applications. Section VI summarizes key research ideas and experiences learned. Finally, Section VII concludes the paper and outlines future research directions.

II. RELATED WORK

Many existing trust models for predicting trust are based on Bayesian inference [3]. Bayesian inference treats trust as a random variable following a probability distribution (e.g., Beta distribution) with its model parameters being updated upon new observations. A shortcoming of Bayesian inference is that trust value does not reveal the uncertainty of trust since it is just a mean. For example, the same trust value can be given to two nodes despite one node was observed for just 2 times, while the other node was observed for 20 times. Belief theory or subjective logic trust models [9] have been proposed to remedy the problem mentioned above, by introducing uncertainty into trust calculation. Fuzzy logic based trust models are also well studied in the literature [12]. Instead of using a binary set, a membership function is defined indicating the degree to which a node is considered trustworthy. Relative to the works cited above based on Bayesian inference, belief theory, or fuzzy logic, we take an entirely different approach. Our root is in statistical analysis. We develop a regression-based trust model to learn the behavior pattern of a SP, taking *context* information into consideration to estimate the reliability trust of a SP that is selected by a SR to execute a service request under a particular environment context.

A significant amount of work has been done in the area of trust-based defenses against attacks in MANETs [13]-[18], [35]-[38]. A common drawback is that dynamically tuning trust parameters may perform poorly when a node

does not have enough self-observation experiences with other nodes in MANET environments and must rely on recommendations. Different from the works cited above, we advocate the use a robust statistical kernel to tolerate false recommendations to effectively achieve resiliency against recommendation attacks. Also unlike existing work, our goal is not to identify "bad" SPs, but to predict whether a SP, whether "good" or "bad," can provide good service, given a set of context variables characterizing the MANET operational environment, including dynamically changing topology, limited bandwidth, battery power, and unreliable communication. In our approach, a SR learns and predicts a SP's service behavior taking context information into consideration, instead of just judging a SP's trustworthiness from self-observations or recommendations received, as having been done in existing works.

III. Threat Model

Just like Internet-based web services, in a service-oriented MANET there are malicious SPs acting for their own gain. The common goal of malicious nodes is to increase their chance of being selected for providing service. Malicious nodes can collude to achieve this common goal. We consider the following malicious attacks in our research:

1. *Bad-mouthing attacks*: a malicious node can ruin the trust of a good node (by providing bad recommendations against it) so as to decrease the chance of that node being selected for service. This is a form of collusion recommendation attacks, i.e., a malicious node can collaborate with other malicious nodes to ruin the trust of a good node.
2. *Ballot-stuffing attacks*: a malicious node can boost the trust of another malicious node (by providing good recommendations) so as to increase the chance of that malicious node being selected as a SP. This is another form of collusion recommendation attacks, i.e., a malicious node can collaborate with other malicious nodes to boost the trust of each other.
3. *Packet-dropping attacks*: when serving as a packet relaying node, a malicious node can delay forwarding or simply drop data packets to ruin the trust of the source node.
4. *Opportunistic service attacks:* a malicious node can provide good service to gain high reputation when it senses its trust status is low, and can provide bad service when it senses its trust status is high.
5. *Self-promotion attacks:* A malicious node can boost its service quality information so as to increase its chance of being selected as a SP.
6. *Conflicting behavior attacks*: a malicious node can selectively provide satisfactory service for some SRs while unsatisfactory for others. Here, we note that a node's best service quality is dictated by the environmental and operational conditions at the time a service request is issued. Therefore, a malicious node can only perform conflicting behavior attacks with a service quality not exceeding its best service quality.
7. *On-off attacks*: instead of always performing its best service, a malicious node can perform bad service. With on-off attacks, a malicious node performs bad service on and off (or randomly) so as to avoid being labeled as a low trust node and risk itself not being selected as a SP, as well as not being able to effectively perform bad-mouthing and ballot-stuffing attacks. One can view on-off attacks as random attacks.

A malicious node may also perform data modification attacks to ruin the reputation of a good node. We assume data/source authentication techniques based on PKI can prevent such attacks. A malicious node may also jam the communication channel or perform denial of service (DoS) attacks to overwhelm a SP. We assume that standard intrusion detection techniques [8] are in place to mitigate such attacks.

IV. Trust Management

One challenge for implementing trust management in service-oriented MANETs is to reliably estimate the trust levels of SPs in a fully distributed manner, in contrast with an e-commerce system with a centralized authority for trust management. Most existing works take direct evidence for direct trust assessment and propagates its observations to other nodes as recommendations for indirect trust assessment. However, a malicious node may violate this protocol. Further, trust management of mobile devices must take "service context" information into consideration. Such service context information includes the current capability of a SP (e.g., energy status), the service environment (e.g., congested wireless traffic), the identity of the SR (e.g., a friend or a stranger), the payoff obtained (which is application-dependent), and the service cost (e.g., energy consumed). All these factors are called "context" variables based on which the service behavior of a node forms a pattern. The key to effective trust management is therefore to learn the service behavior pattern of a node toward these context variables. The behavior pattern learned can be used to assess the *reliability trust* [3] of a SP when it is selected to service a request in a particular context state characterized by these context variables.

More specifically, within a specific type of service, SR i's observation s_{ij}^t at time t of the service quality received from SP j is either "satisfactory" or "unsatisfactory." If the service quality is satisfactory, then s_{ij}^t =1 and SP j is considered *trustworthy;* otherwise, s_{ij}^t =0 and SP j is considered *untrustworthy*. Let the operational and environmental conditions at time t be characterized by a set of distinct context variables deemed appropriate for an application, denoted by a column vector $\mathbf{x}^t = [x_0^t, \ldots, x_m^t]^\top$, where x_i^t represents the ith context variable. Then, *reliability trust* or just *trust* for short is the probability that SP j is capable of providing satisfactory service under the operational and environment conditions at time t described by the context variable set $\mathbf{x}^t$.

Let k ($k \neq i$) be a recommender who had a prior service experience with SP j and is asked by SR i to provide its feedback regarding SP j. The recommendation from node k is in the form of $[\mathbf{x}^t, s_{kj}^t]$ specifying the specific operational and environmental context conditions in $\mathbf{x}^t$ under which the

observation in s_{kj}^t was made. For notational conveniences, let $\mathbf{S_{ij}} = \left[s_{ij}^{t_0}, \ldots, s_{ij}^{t_n}\right]^\top$, $i \neq j$, denote the cumulative evidence gathered by SR *i* regarding SP j's service quality over $[t_0, t_n]$ including self-observations and recommendations. Also let $\mathbf{X} = [\mathbf{x}^{t_0}, \ldots, \mathbf{x}^{t_n}]^\top$ denote the corresponding operational and environmental context conditions when the observations are made.

The problem is to learn the service behavior pattern of SP *j* by a latent variable $\boldsymbol{\beta}_j$ between $\boldsymbol{S_{ij}}$ and $\mathbf{X}$, and predict the probability that SP j is trustworthy at time t, given the context environment set at time n+1, $\mathbf{x}^{t_{n+1}}$, as input, i.e., $T_{i,j}^{t_{n+1}} = \Pr\{s_{ij}^{t_{n+1}} = 1 | \mathbf{x}^{t_{n+1}}, \boldsymbol{\beta}_j\}$. Essentially $T_{i,j}^{t_{n+1}}$ obtained above is the *reliability trust* of SP *j* at time t_{n+1} from SR *i*'s perspective. The service quality at time n+1, $\hat{s}_{ij}^{t_{n+1}}$, can be predicted by setting a trust threshold, depending on the SR's tolerance for the risk.

A common practice is to set the trust threshold as a value greater than 0.5. For example, if the trust threshold is set to be 0.6 by SR *i* then the requested service performed by SP *j* is predicted to be satisfactory when the predicted reliability trust is greater than 0.6.

In [2], we utilized *logit regression* as the behavior pattern learning mechanism to solve the above trust assessment problem, resulting in a trust management protocol which we call LogitTrust.

LogitTrust assesses each SP in terms of its service behavior patterns in response to operational and environmental changes characterized by three context variables: $[x_e^t, x_c^t, x_p^t]$ for energy, capability, and price (or reward). Energy is used to measure the cost of task execution. In a congested environment the probability of wireless channel contention and signal interference will be high, so it will cost more for a SP to execute a task because the SP needs to consume more energy in listening to the channel and repeating packet transmission. The reasons for considering the above context variables in service-oriented MANET environments are: (a) a SP is more likely to provide inferior service when the cost of servicing the task is high (b) a SP is likely to provide inferior service when it is limited in resources and capability; and (c) a profit-aware SP is more likely to provide quality service when the SR offers a higher price.

SR *i* will assess the three context variables $[x_e^t, x_c^t, x_p^t]$ while it sends a service request to SP *j* as follows: x_e^t is estimated by the number of neighbors sharing the channel as more energy is consumed for channel contention and packet retransmission when there are more nodes sharing the channel; x_c^t is estimated by the packet traffic to SP *j* as more traffic to SP *j* hinders its processing capability; x_p^t is SR *i*'s reward to SP *j* upon satisfactory service completion. When SP *j* completes the service, SR *i* will assess if the service is satisfactory (1) or not (0), and store the service outcome together with $[x_e^t, x_c^t, x_p^t]$ context information as one record in the dataset set for learning. It can also pass this experience record to another node as a recommendation. A SR in the system uses its own self-observations and recommendations received to learn the behavior pattern of a SP, and predict the reliability trust of the SP on a service request in a particular context environment.

Relying on its robust learning engine, LogitTrust is highly effective against dishonest recommendations (through bad-mouthing and ballot-stuffing attacks). It significantly outperforms existing trust computation models such as Beta reputation with belief discounting [3] and Adaptive Trust Management [4] in terms of trust accuracy because it takes context information into consideration in service behavior assessment. LogitTrust is also efficient in terms of computational complexity as it utilizes a simple linear model to model the relation between context variables and observations.

With conflicting behavior attacks, a SP can selectively provide satisfactory service for some SRs while providing unsatisfactory service for others. In general, the relation between a SR and a SP determines the SP's service attitude toward the SR. This is naturally solved by LogitTrust since LogitTrust is based on SR-SP pairing. That is, each SR evaluates each SP based on its own self-observations and filtered recommendations. If SP *j* provides bad services to a particular SR, then this evidence will be considered by this SR as it learns SP *j*'s behavior pattern (that is, $\boldsymbol{\beta}_j$) and will not trust SP *j* with its service request.

With on-off attacks, a malicious node will attack only randomly so as to evade detection and avoid being classified as a malicious node. To the system, this malicious node is not 100% of the time providing bad service, but just a percentage of time providing bad service. Therefore, SP *j* performing on-off attacks translates into SP *j* providing bad service only randomly instead of persistently, which is a pattern that can be learned by SR as LogitTrust learns SP *j*'s behavior pattern (that is, $\boldsymbol{\beta}_j$). This in effect allows each SR to cope with a particular SP's on-off attack behavior.

V. Trust-Based Algorithm Design for Application Performance Maximization

Service-oriented MANET applications are on the rise thanks to the proliferation of fairly powerful mobile devices and ubiquitous wireless technology. We aim to design and validate trust-based algorithms for application performance maximization for service-oriented MANET applications with the goal of satisfying multiple objectives with conflicting goals to achieve multi-objective optimization (MOO).

Trust-based service composition and binding (with or without MOO) has been studied in the web services domain but only a single-trust, i.e., a single dimension of trust, was considered. This largely ignores the fact that trust is multi-dimensional. Identifying proper trust components and forming the overall trust out of multiple trust components to maximize application performance is of paramount importance. We advocate the use of two key trust dimensions in service request execution, namely, *competence* and *integrity*, as the building blocks of a composite trust metric.

Below we discuss our trust-based service management

algorithm designs for solving two service-oriented MANET applications with MOO.

In [5], we investigated a trust-based dynamic task assignment algorithm for performing dynamic task-to-node service assignments to satisfy multiple objectives with conflicting goals. The results demonstrated that our trust-based solution has low complexity and yet can achieve performance comparable to that of the ideal solution with perfect knowledge of node reliability, and can significantly outperform the non-trust-based solution. We analyzed how MOO is achieved by the ideal, trust-based and non-trust-based solutions, and identified parameter settings under which the trust protocol performance in terms of MOO is optimized for the trust-based solution which can best balance multiple objectives with conflicting goals. The results obtained are useful for dynamic trust management to maximize application performance in terms of MOO in the presence of malicious attacks.

In [6], we investigated a trust-based service composition algorithm designed to satisfy mobile user service requests with multiple objectives including maximizing quality-of-service (QoS) and quality-of-information (QoI) while minimizing the service cost (e.g., pricing) with the *user satisfaction* ultimately measuring success. With a service request in hand, a SR has to first formulate a service composition plan based on the available SPs it encounters and interacts with dynamically, and then determine the best node-to-service assignment for achieving MOO. Dynamic service composition and binding is especially complicated in MANETs because of the space-time complexity of mobile devices. This issue is further compounded by the fact that the information received is often malicious, erroneous, partly trusted, uncertain and incomplete in MANET environments. Our trust-based service composition and binding algorithm based on multi-trust outperforms the non-trust-based counterpart using blacklisting, as well as a single-trust-based algorithm using a traditional beta reputation system.

Our trust-based algorithm has a linear runtime complexity and is able to achieve a solution quality approaching that generated by Integer Linear Programming without sacrificing much solution accuracy. We conducted a comparative performance analysis of single-trust vs. multi-trust protocols for peer-to-peer trust evaluation in service-oriented MANETs. We utilized trust to effectively prevent malicious nodes from disrupting the operation of a service-oriented MANET. We conducted a detailed performance analysis and demonstrated that our trust-based algorithm can effectively penalize malicious nodes performing bad-mouthing, ballot-stuffing packet dropping, self-promotion, or opportunistic service attacks, thus filtering out malicious nodes from service participation, and can ultimately lead to high user satisfaction.

VI. Key Ideas and Experiences Learned

The major difference between a service-oriented MANET and an Internet-based web service system is that the information received in MANET environments is often malicious, erroneous, partly trusted, uncertain and incomplete. In this paper we discussed key research ideas for trust-based service management of mobile devices in service-oriented MANETs wherein every node can be a service provider or a service requester.

The first key idea is to take special characteristics of service-oriented MANET environments into consideration so as to design an efficient and effective trust protocol. We discussed a novel logit regression-based trust model called LogitTrust to dynamically estimate the trust of a mobile device based on how it behaves in response to dynamically changing MANET environments characterized by a set of context variables. LogitTrust outperforms traditional approaches based on Bayesian Inference with belief discounting in terms of trust accuracy and resiliency against attacks, while maintaining a low false positive rate. It is efficient as it adopts a simple liner model for behavior learning with low computational complexity. It is effective since it reflects dynamic MANET characteristics, such as limited bandwidth and battery power, as context variables in the learning model formulation.

The 2nd key idea is to use multi-trust instead of single-trust for trust-based algorithm design, recognizing multi-dimensional trust assessment is critical for decision makings.

The 3rd key idea is that multi-trust-based algorithm design is application specific. One must apply the best trust formation tailored to the application requirements to achieve application performance maximization, especially for those applications with multi-objective optimization goals. We demonstrated that our multi-trust-based algorithm outperforms its non-trust-based and single-trust-based counterparts with multi-objective optimization over a range of service-oriented MANET applications, including node-to-service composition and binding, and node-to-task assignment MANET applications. Furthermore, we demonstrated that our multi-trust-based algorithms for solving these problems are efficient (with linear runtime complexity) and effective without compromising solution optimality, when compared with non-trust-based solutions, and other single-trust-based solutions based on Bayesian inference.

VII. Future Research Directions

There are several future research directions for trust management of mobile devices in service-oriented MANETs:

First, we plan to address the issue of runtime learning and decision making for MANET nodes with limited storage and computation resources. This may involve the use of heuristics for each resource-limited node to store most relevant trust records [10].

Second, we plan to incorporate adaptive control to the trust protocol design. A possible direction is to use a recommendation filtering mechanism to dynamically decide if a recommendation is to be taken or not. Adaptive control may be achieved by adjusting the recommender filtering threshold value based on the hostility level in the environment. When the hostility level is low (i.e., not many "bad" nodes are out there), one can set a low threshold so as to take in recommendations into the dataset, because chances are all recommendations are benign. On the other

hand, when the hostility level is high, one can set a high threshold to filter out false recommendations so as not to contaminate the dataset for effective behavior learning.

Third, although we have reflected MANET environment characteristics such as limited bandwidth and energy power as context variables in our trust model formulation, we have not considered node social behaviors which can also be treated as context information. A context variable such as "friendship" can dictate whether a node will perform good service or bad service toward another node, or if a node will perform ballot-stuffing or bad-mouthing attack toward another node. We plan to further test the resiliency of LogitTrust [2] against more complicated environmental and operational scenarios such as noisy environments, social-based service behaviors, as well as more sophisticated attack behaviors such as opportunistic, collusion and insidious attacks [11].

Lastly, we plan to leverage game theory and artificial intelligence principles [19]-[23], and stochastic Petri net modeling techniques [24]-[34] to capture the dynamics between attacker/defense behaviors [39]-[42] and reason how a service requester can perform counterattacks by adaptive trust-based service management for achieving multi-objective optimization of service quality.

ACKNOWLEDGMENT

This work is supported in part by the U. S. Army Research Laboratory and the U. S. Army Research Office under contract number W911NF-12-1-0445. This research was also partially supported by the Department of Defense (DoD) through the office of the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)). The views and opinions of the author(s) do not reflect those of the DoD or ASD (R&E).

REFERENCES

[1] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, 2014, pp. 1-31.

[2] Y. Wang, Y. C. Lu, I. R. Chen, J. H. Cho, A. Swami, and C. T. Lu, "LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks," 6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA, Dec. 2014, pp. 1-10.

[3] A. Jøsang and R. Ismail, "The Beta Reputation System," 15th Bled Electronic Commerce Conf., 2002, pp. 1-14.

[4] 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.

[5] Y. Wang, I. R. Chen, and J. H. Cho, "Trust-Based Task Assignment in Autonomous Service-Oriented Ad Hoc Networks," IEEE 12th International Symposium on Autonomous Decentralized Systems, Taichung, Taiwan, March 2015, pp. 71-77.

[6] Y. Wang, I. R. Chen, J. H. Cho, K. S. Chan, and A. Swami, "Trust-based Service Composition and Binding for Tactical Networks with Multiple Objectives," 32th IEEE Military Communications Conference (MILCOM 2013), San Diego, CA, USA, Nov. 2013, pp. 1862-1867.

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

[8] R. Mitchell and I. R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications," Computer Communications, vol. 42, April 2014, pp. 1-23.

[9] A. Jøsang, "A Logic for Uncertain Probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, vol. 9, no. 3, 2001, pp. 279-311.

[10] 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.

[11] 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, 2013, pp. 199-210.

[12] H. Xia, Z. Jia, L. Ju, and Y. Zhu, "Trust Management Model for Mobile Ad Hoc Network Based on Analytic Hierarchy Process and Fuzzy Theory," IET Wireless Sensor Systems, vol. 1, no. 4, 2011, pp. 248-266.

[13] 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.

[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] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," IFIP 6th Joint Working Conference on Communications and Multimedia Security, Portorož, Slovenia, 2002, pp. 107-121.

[16] J. H. Cho, A. Swami, and I. R. Chen, "Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks," in Int'l. Conf. Computational Science and Engineering, 2009, pp. 641-650.

[17] 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, 2012, pp. 1001-1012.

[18] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," IEEE Comm. Survey and Tutorials, vol. 14, no. 2, 2012, pp. 279-298.

[19] D. Korzhyk, V. Conitzer, and R. Parr, "Solving Stackelberg Games with Uncertain Observability," 10th International Conference on Autonomous Agents and Multiagent Systems, Taipei, Taiwan, May 2010, pp. 1013-1020.

[20] J. Wang and I. R. Chen, "Trust-based Data Fusion Mechanism Design in Cognitive Radio Networks," IEEE Conference on Communications and Network Security (CNS), San Francisco, Oct. 2014, pp. 53-59.

[21] I. R. Chen and F. B. Bastani,, "Effect of Artificial-Intelligence Planning-Procedures on System Reliability," IEEE Trans-actions 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 and D. C. Wang, “Analyzing Dynamic Voting using Petri Nets,” 15th IEEE Symposium on Reliable Distributed Systems, Niagara Falls, Canada, 1996, pp. 44-53.
[25] 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.
[26] R. Mitchell and I. R. Chen, “Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, 2015, pp. 16-30.
[27] I. R. Chen, T. M. Chen, and C. Lee, “Performance Evaluation of Forwarding Strategies for Location Management in Mobile Networks,” The Computer Journal, vol. 41, no. 4, 1998, pp. 243–253.
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] 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.
[35] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, “A Probabilistic Misbehavior Detection Scheme Towards Efficient Trust Establishment in Delay-Tolerant Networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, 2014, pp. 22-32.
[36] L. Xiong and L. Liu, “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” IEEE Trans. on Knowledge and Data Engineering, vol. 16, no. 7, 2004, pp. 843-857.
[37] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks,” 12th International Conference on World Wide Web, Budapest, Hungary, May 2003, pp. 640-651.
[38] Z. Su et al., “ServiceTrust: Trust Management in Service Provision Networks,” IEEE International Conference on Services Computing, Santa Clara, CA, 2013, pp. 272-279.
[39] 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.
[40] 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, 2015, in press.
[41] 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 preess.
[42] 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.