A Novel Coalitional Game Model for Security Issues in Wireless Networks

Xiaoqi Li Michael R. Lyu
Department of Computer Science and Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
{xqli, lyu}@cse.cuhk.edu.hk

***Abstract*—In this paper, we propose a novel coalitional game model for security issues in wireless networks. The model can be applied to not only mobile ad hoc networks but also wireless sensor networks. We define a new throughput characteristic function, on the basis of which nodes are enforced to cooperate and form coalitions. This function implies the maximal throughput and the most reliable traffic that a coalition can achieve. The fair payoff share inside the coalition is given by Shapley Value after proving the feasibility of this method. Then a set of game rules is presented to establish a threatening mechanism to all players. We then describe the coalition formation procedure and explain how to integrate this game theoretic model with available wireless routing protocols. Finally, theoretical analysis is conducted to illustrate the convergence situation and justify the correctness of the formulation.**

Keywords: Coalitional Game, Game Theory, Wireless Network Security

I. Introduction

In wireless networks, nodes scatter in different positions and move in all directions randomly every now and then. This kind of network is designed to achieve high flexibility. However, the mobility of nodes and lack of sufficient information about each other increase the risk of being compromised from either outside or inside. It is crucial to arm the whole network or the individual nodes with effective security mechanisms. The security mechanism, on one hand, must require low computation complexity and small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors and identify misbehaving nodes from normal ones.

For recent years, many researchers have tried to model the wireless network as a game. Selfish issue is the most extensive application of game theory. Because of the limit of individual power, nodes are inherently not willing to forward packets for others. This behavior will decrease the throughput level of the whole network. Several incentive mechanisms [1], [2], [3], [4], [5], [6] based on game theory have been proposed to tackle this problem. However, there is another category of problems, which are more stochastic than the selfish problem, that have not been modeled using game theory effectively. That is the security issue.

Due to the variety of malicious behaviors, it is more difficult to apply game theory to security problems than selfish issues. Malicious behaviors or attack actions may have all kinds of forms, which bring the challenges to restrict them into a safe range. However the malicious nodes still have certain behavior pattens that usually take several steps to fulfill one attack. They must be rational enough to perform harmful actions and at the same time hide themselves from being detected or denied by the network, and in that case no more harmful actions can be performed. In the premise of rational malicious nodes, we can also apply game theory into the design of incentive mechanisms and then routing protocols. Currently the security issues of wireless ad hoc networks using game theory can be modeled as non-cooperative games played between one attacker and one target [7], between one attacker and the whole network, or between two or more attackers and the rest of the network. It can also be modeled as cooperative games [8] where nodes form coalitions according to some game rules to achieve higher security and throughput level or be able to identify the malicious nodes more efficiently.

In this paper, we propose a novel coalitional game model for security issues in wireless networks. The model can be applied to not only mobile ad hoc networks (MANET) but also wireless sensor networks (WSN). Both MANET and WSN face similar security challenges and share the same cooperating characteristic among nodes. Unlike MANET most nodes in WSN are fixed which simplified the problem while on the other hand computation complexity and energy consumption should be addressed more in WSN for the sake of limited hardware resources of nodes. The main contributions of our work are:

- We define a new throughput characteristic function, on the basis of which nodes are enforced to cooperate and form coalitions. The physical meaning of the throughput characteristic function is the maximal throughput and the most reliable traffic that a coalition can achieve.
- The payoff share is given by Shapley Value after proving the feasibility of this method.
- Then a set of game rules is presented to establish a threatening mechanism to all players.
- We then describe the coalition formation procedure and the integration of this game theory model with available wireless routing protocols.
- Finally, theoretical analysis is conducted to illustrate the convergence situation and justify the correctness of the

formulation.

The rest of this paper is organized as follows. Section II summarizes related works on solving selfishness and security issues using game theory. Section III presents our proposed coalitional game model in detail. We present the coalition formation algorithm and its integration with routing protocols in Section IV. In Section V we analyze the model using game theory. We finally conclude the paper in Section VI.

II. Related Work

A. Selfishness Study

Selfishness has been studied in wireless networks in recent years. Most approaches fall into one of two main categories: approaches rewarding cooperative nodes and those punishing non-cooperative nodes.

In the first category, nodes forwarding packets get monetary incentives for their service. In Ad Hoc-VCG [1], payments are paid to nodes which forward data packets for others, consisting the actual costs incurred by forwarding data and the extra premiums. The implemented reactive routing protocol is a variation of the well-known VCG mechanism. It achieves the design objectives of truthfulness and cost-efficiency in a game-theoretic sense. But Ad Hoc-VCG is not budget-balanced. Another work [2] introduces a virtual currency called *nuglets*. The source of the packet must load it with enough nuglets to pay for the trip to the destination. Cooperation is enforced in this scheme because nodes must forward packets for others in order to build up enough nuglets to get their own packets forwarded. NUGLETS [2] is budget-balanced. Somewhat similar in scope to nuglets is SPRITE [3], which uses a Credit Clearance Service (CCS) to store the credit, as opposed to the tamper-proof module used in nuglets. However, centralized services tend to defeat the purpose of ad hoc networks. [4] designs an incentive-compatible routing and forwarding protocol integrating VCG mechanism and cryptographic technique. Payments are implemented based on VCG protocol and the application of cryptographic techniques in the design of forwarding protocol enforces the routing decision.

In the second category non-cooperative nodes are identified based on a reputation system and circumvented in the routing process. The primary goal of reputation-base schemes is to block selfish nodes from the network. In CORE [5], node cooperation is stimulated by a collaborative monitoring technique and a reputation mechanism. Each node of the network monitors the behavior of its neighbors with respect to a requested function and collects observations about the execution of that function. If the observed result and the expected result coincide, the observation will take a positive value; otherwise it will take a negative value. CONFIDANT [6] differs from CORE only in that it sends reputation values to other nodes in the network, which exposes the scheme to malicious spreading of false reputation values.

B. Security Study

In [8], the authors define a cooperative game between sensor nodes and concentrate on three fundamental factors: cooperation, reputation and quality of security. The more a node cooperates, the better its reputation is, which decreases when misbehavior is detected. When security of the network is compromised, the percentage of exposed traffic measures the quality of security of sensor nodes. By incorporating these three factors, sensor nodes are clustered where payoff is the largest possible individual gain for each sensor according to a defined utility metric. [7] is a game theoretic formulation for intrusion detection system in mobile ad hoc networks. The interaction between attacker and individual node is viewed as a two-player multistage dynamic non-cooperative game with incomplete information.

C. Trust Evaluation

This paper provides another way to represent trust relationship among nodes, in which nodes can evaluate the trustworthiness of other nodes so that trust communities are able to be established. There were a lot of work studying this issue. Liu and Issarny employ Bayesian approach to design an incentive compatible reputation system to facilitate the trustworthiness evaluation of nodes [9]. Some also use subjective logic to calculate uncertain trust so as to desgin secure routing protocols [10] or incentive reputation mechanisms [11]. Theory of semirings is also applied to evaluate trust and trust relations in [12].

III. Our Coalitional Game Model

In this work, we formulate the wireless network as playing a coalitional game by defining a throughput characteristic function and giving the payoff distribution method among the coalitional members. A set of game rules is prescribed and a threatening mechanism is established, based on which we also design a coalitional formation algorithm that can be integrated into routing protocol to make it have more traffic capacity and more reliability.

A. Basic Idea

Cooperation is the inherent nature of wireless ad hoc and sensor networks. Formulating the network as a cooperative game will not destroy this nature but make full use of it. Coalitional game is one kind of cooperative game that we think will satisfy the properties of our problem.

Our coalitional game has transferable payoff and is denoted by $\Gamma =< N, v >$, where N is the set of nodes (players), and v is the throughput characteristic function that associates with every non-empty subset S of N a real number $v(S)$. The physical meaning of v is the maximal throughput and the most trustful and reliable traffic that each coalition S can achieve. It is the foundation of the coalition forming procedure and it constrains the coalition to admit or exclude a node. Our goal is to gracefully define the throughput characteristic function and also a fair payoff distribution method among coalition members. This work is done in sections III-B and III-C. We

will then examine how coalitions are formed under the effect of this payoff function and set game rules in sections III-D and IV. In such a way, nodes are enforced to take part in coalitions and those that cannot join into any coalition are under very high suspicion of being malicious.

To make our model mainly focus on the problem formulation, we give the following assumptions: 1) we assume that there is a Watchdog [13] mechanism in each node, by which it can detect whether its neighbors are forwarding data packets for it or not; 2) we also assume that a time synchronization mechanism has been implemented in the system so that we can schedule the coalition formation process synchronously.

B. Throughput Characteristic Function

We firstly give the definition of the throughput characteristic function and then explain it detailedly in the rest of this section.

Definition 1 (Throughput Characteristic Function): The throughput characteristic value for any coalition S, $S \subseteq N$, where $|S| = 1$ and $|S| = 0$, is 0. For other coalition S, where $|S| \geq 2$, the throughput characteristic function $v(S)$ is defined as:

$$v(S) = \frac{1}{\triangle t} \sum_{(a,b)\in SD, a,b\in S} Q_{ab} \cdot \max_{k\in P_{ab}(S)} \left\{ t(k) = \prod_{(i,j)\in k} \frac{p_{ij}}{D_{ij}^2} \right\} \tag{1}$$

where

1) $\triangle t$ is a certain time interval
2) $SD = \{(a,b)|\ (a,b)$ is a source-destination pair$\}$
3) Q_{ab} is the required number of data packets transmitting between pair (a,b)
4) $P_{ab}(S)$ is the set of routing paths inside coalition S which connect pair (a,b)
5) $k \in P_{ab}(S)$ is one of the path in $P_{ab}(S)$ and $k = \{(i,j)|\ i,\ j$ are the adjacent nodes on the same routing path$\}$
6) $t(k)$ stands for the reliability of routing path k
7) p_{ij} is the trustworthiness of path (i,j)
8) D_{ij} is the distance between node i and j □

Figure 1 shows an example coalition labelled with parameters in the throughput characteristic function. In the following paragraphs, we will explain each parameter one by one.

When a coalition is formed, it can generate a weighted directed graph $G(S)$, where vertexes are nodes inside the coalition, edges represent routing direction between nodes, and weights are the probabilities that one node wants to communicate with another. From this graph, we perform a routing discovery procedure to discover the first several possible routing paths $P(S)$ for each source-destination pair inside the coalition. The number of routing paths is related to the size of the coalition. When the coalition size increases, more possible paths can be found and more reliable routing and forwarding transmission can be obtained.

For every possible routing path k between the source-destination pair, we get a reliability evaluation $t(k)$. From the coalition point of view, the maximal value of $t(k)$ over all k means the best service that the coalition can provide to this source-destination pair. In other words, it indicates the maximal payoff that the pair can benefit from the coalition. We also use $t(i,j)$ to denote $t(k)$, where i, j are two end nodes of path k.

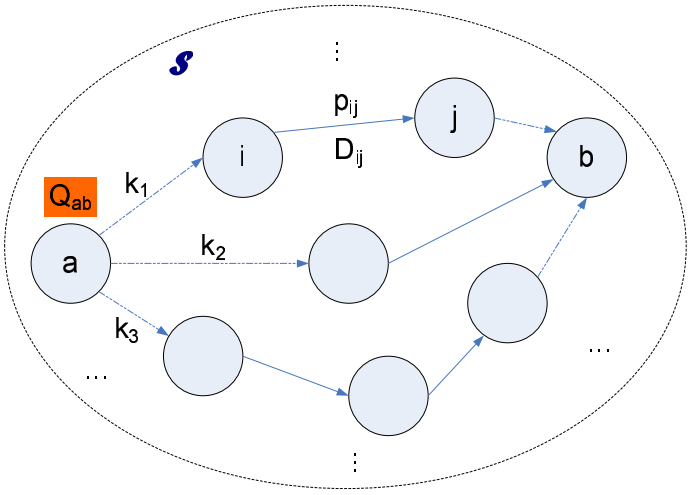

Fig. 1. Coalition S labelled with parameters in throughput characteristic function

The probability that node i wants to communicate with node j implies the trustworthiness of the routing path from i to j. It is obtained from two ways: direct experience and indirect recommendation. The direct experience p is the fraction of number of observed successful transmission times by all the transmission times between i and j, shown in (2).

$$p = \frac{u_{succ}}{u_{all}} \tag{2}$$

The indirect recommendation comes from node i's neighbors. Each neighbor of i returns probability opinions about both i and j, then i combines those probabilities of all neighbors together. Please note that we consider not only neighbors' recommendations towards j but also towards i, which represents the opinions towards the routing path from i to j. Multiplying by node i's own evaluation to its neighbors, we then get the more believable indirect probability p' of communication from i to j. The form is given in (3).

$$p' = \frac{\sum_{l\in NB_i} p_{il} p_{li} p_{lj}}{|NB_i|} \tag{3}$$

where $|NB_i|$ is the number of neighbors of node i.

Since direct experience and indirect recommendation have different weights, which can be adjusted to fit into different applications, we then combine the probability p_{ij} in (4).

$$\begin{aligned} p_{ij} &= \alpha p + (1-\alpha) p' \\ &= \alpha \frac{u_{succ}}{u_{all}} + (1-\alpha) \frac{\sum_{l\in NB_i} p_{il} p_{li} p_{lj}}{|NB_i|} \end{aligned} \tag{4}$$

Finally, the reliability of a routing path is determined by not only the communication probability but also the physical connection between the two nodes. Even though both nodes have good reputation, the path is still lack of reliability if they are too far away from each other. So we take another metric, distance D_{ij}, into consideration. And because the signal fading of the link is in inverse proportion to the square of distance, so we use D_{ij}^2 to represent the connectivity of the link.

C. Payoff Allocation Inside Coalition

The throughput characteristic function describes the total expected gain of a coalition from the cooperation. Since some nodes may contribute more to the coalition than others, now we consider the problem of how to fairly distribute the gains among all the nodes. In other words, what payoff can nodes reasonably expect from cooperation. Shapley value [14] is one way to distribute the total gains to players, which is applicable when the payoff function satisfies the following two conditions:

$$\begin{array}{ll} 1. & v(\phi) = 0 \\ 2. & v(S \cup T) \geq v(S) + v(T) \end{array} \tag{5}$$

where S and T are disjoint subsets of N. Then the amount that player i gets is as follows:

$$x_i(v) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n-|S|-1)!}{n!}(v(S \cup \{i\}) - v(S)) \tag{6}$$

To employ this equation, we now justify that the proposed throughput characteristic function satisfies the two conditions in (5).

Theorem 1: Shapley Value method is applicable to the payoff allocation inside coalitions given our proposed throughput characteristic function $v(S)$.

Proof: Firstly, from the definition of throughput characteristic function $v(S)$ in 1, we easily know that $v(\phi) = 0$, which satisfy the first condition of (5).

Secondly, on the basis of $v(S)$, we have the following equations:

$$v(S) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S} Q_{ab} \cdot \max_{k \in P_{ab}(S)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

$$v(T) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in T} Q_{ab} \cdot \max_{k \in P_{ab}(T)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

$$\Longrightarrow \quad v(S \cup T) =$$

$$\frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S \cup T} Q_{ab} \cdot \max_{k \in P_{ab}(S \cup T)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

The larger the coalition becomes, the more number of possible routing paths can be discovered. Accordingly, the maximal reliability increases when obtained from a larger set. On the premise of certain amount of required transmission data packets and certain time interval, the expected throughput of the larger coalition will be increased. That is, $v(S \cup T) \geq v(S) + v(T)$ is satisfied.□

In summery, we can distribute the total payoff of the coalition to each players according to Shapley Value Equation.

D. Game Rules and Threatening Mechanism

There might be some misbehaving nodes in the network but they will perform bad behaviors on the premise of not compromising their own behalf. On the basis of the predefined throughput characteristic function, we can design a set of game rules so as to implementing a threatening mechanism.

The strategy space of each node is $\{join, notjoin\}$. That is, the node either joins into a coalition or doesn't join into the coalition. The game rules are:

1) A node will join into a coalition only if it can get more payoff share than it stands individually.
2) A node will deviate from the current coalition and join into another coalition only if it can get more payoff share there than that of here.
3) A coalition will refuse to admit a node if the node cannot increase the total payoff of the coalition.
4) A coalition will exclude a node if the node cannot benefit the coalition or even damage the total payoff of the coalition.
5) Nodes who are finally failed to join into any coalition will be denied from the network.

These rules form a threatening mechanism in the network. Take the selfish nodes for example, they do not forward others' routing or data packets in order to save their own communication and computation resource. But under the condition of the above game rules, they will hardly be admitted into coalitions such that their own traffic cannot be delivered to the destination because of poor reputation. This is a potential threat for them.

Before joining into or deviating from a coalition, every node will compare the possible payoff share it will obtain with the current payoff share it has obtained. Then following the above game rules, a new coalition topology will be formed.

IV. Coalition Formation Procedure

A. Coalition Formation Algorithm

As a further refinement, we are going to design a coalition formation algorithm that satisfy the definition of $v(S)$. We introduce Gale-Shapley Deferred Acceptance Algorithm (DAA) [15] to help nodes forming coalitions. This algorithm was proposed to solve the stable marriage problem and was proven that at the end of the algorithm, no one wants to switch partners to increase his/her happiness. In this paper we firstly apply this algorithm to the coalition formation of wireless networks.

The coalition formation procedure is conducted iteratively by all the nodes in the network. It is described in Algorithm 1 and 2.

Algorithm 1 Coalition Formation Algorithm

```
while timeleft≠ 0 do
  for 0 to Δt do
    normal routing and forwarding process, gain experience
  end for
  update direct probability p_ij, distance D_ij
  compute t(i, j) for every neighbor of i, and sort them
  for all coalition S containing any src a or any dst b do
    findmatch(S)
  end for
  for all node i not in any coalition S do
    degrade i
  end for
  timeleft ← timeleft - Δt
end while
```

Algorithm 2 Find Matching Partner Algorithm

```
findmatch(S):
for all a ∈ S do
  chose first several preferences with highest t(a, .)
  conduct DAA algorithm to find partner a' of a
  add new match {a, a'} to coalition S
  update all members' routing table and corresponding state of S
end for
```

B. Integration with Wireless Routing Protocols

The proposed coalitional game model can be integrated with all kinds of routing protocols, such as AODV [16], DSR [17], DSDV [18] and so on, of many types of wireless network, e.g. mobile ad hoc networks and wireless sensor networks. We take AODV routing protocol for example to illustrate how to integrate the game model with routing behaviors.

Firstly, we extend the original routing table of AODV protocol by adding four fields:

1) Number of members in the coalition that the concerned entry has joined into;
2) Direct communication probability from the current node to the concerned entry;
3) Indirect communication probability from the current node to the concerned entry;
4) Distance between the current node with the concerned entry.

Secondly, besides original routing request and reply (RREQ, RREP) packet types, several new control packet types are defined, such as Matching REQuest/REPly (MREQ, MREP) and Probability REQuest/REPly (PREQ, PREP) and so on. MREQ/MREP are matching request and reply packets to exchange the matching preference list and notify the matching result. PREQ/PREP packets are used to collect neighbors' recommendation of communication probability.

Thirdly, a new dedicated timer must be set up to control the iteration of coalition formation procedure.

V. Theoretical Analysis

We now theoretically analyze our model from two aspects: 1) Speed of convergence and size of coalition and 2) Non-emptiness of core [19]. We will show that the coalition formation speed is fast and the size of the coalition keeps growing and even a grand coalition can be reached. We will also show that cooperation is made attractive from the individual point of view because the cost of participating in the network operation is compensated with a higher reputation value. On the other hand, when the number of cooperating nodes increases, the cost for participation is compensated by a more reliable network that in turn increases the benefit of cooperation.

A. Speed of Convergence and Size of Coalition

From the coalition formation algorithm we can see that at each round of formation, every coalition member tries to find a partner. So the coalition size is increased almost at a rate of two times. Therefore, the speed of coalition formation is fast, which means the convergence time of formation is short. And the size will keep growing until a grand coalition is reached or all misbehaving nodes are identified.

B. Non-emptiness of Core

The stable status of coalitional game is that no coalition can obtain a payoff that exceeds the sum of its members' current payoffs, which means no deviation is profitable for all of its members. The core is the set of imputation vectors which satisfies the following two conditions:

$$\begin{array}{ll} 1. & \sum_{i=1}^{n} x_i = v(N) \\ 2. & \sum_{i \in S} x_i \geq v(S), \forall S \in 2^N \end{array} \tag{7}$$

The first condition is to guarantee the efficiency of payoff allocation. N is called the grand coalition. The second condition ensures that no coalition is unhappy, and it is a very strong constraint. We can see that whether the core is nonempty or not is determined by the definition of characteristic function $v(S)$ and the payoff distribution method among the coalition members.

We have defined the throughput characteristic function and the payoff allocation method among coalition in previous sessions. Based on the definition, we now discuss the several situations of the core.

We denote the allocation profile $x(S) = \sum_{i \in S} x_i(S), \forall S \in 2^N$. The relation between $x(S)$ and $v(S)$ has two situations.

$x(S) < v(S)$
: In this situation, the core is empty. But when $|S| = 1$, which means the node do not belong to any coalition, this node cannot form a source-destination pair and consequently no throughput can be obtained. While considering the Shapley value in (6), the payoff share is always larger than 0, which implies that rational nodes always have incentive to cooperate with each other.

$x(S) \geq v(S)$

If this situation can be reached, the core is nonempty. The stable outcome will last for a certain time under certain conditions. However, in the mobile ad hoc network, there are some factors that will destroy the current equilibrium and enforce the network to re-organize again. The first factor is that not all the nodes are reasonable, and the second one is the incompleteness of information due to the nodes mobility, underlying detection mechanism and so on. If that is the case, we can still observe $x(S) - v(S)$. The difference between them means how hard the core status will be destroyed. The larger the difference, the lower the probability that coalition S will deviate. Then we can get the probability that the core would remain as follows:

$$p_{keep} = 1 - \prod_{S} [\ 1 - p_{deviate}(x(S) - v(S))\ ] \quad (8)$$

where $p_{deviate}(x(S) - v(S))$ can be approximated as an exponential distribution for further investigation.

VI. Conclusions

The work we present has such contributions as following. Firstly, we novelly bring the idea of applying coalitional game model to the security issues of wireless networks. Secondly, we well define the throughput characteristic function which not only describes the network performance metric but also expresses the quantification of security metric. And we also give the payoff distribution method for coalition members to share the utility value fairly. Thirdly, a coalition formation algorithm is designed and can be integrated with any routing protocol of wireless networks. Fourthly, from the theoretical analysis, we conclude that the convergence of coalition formation is quite fast and the coalition size can be very large, which means nodes are ready to form into coalitions and perform good behaviors, so that we can prevent bad behaviors and identify misbehaving nodes effectively. We also discuss the nonempty of stable status of coalition formation and conclude that the core in wireless networks is difficult to achieve and easy to be destroyed. But we can then still investigate the node deviation probability and get certain network properties for future applications.

Acknowledgment

The work described in this paper was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CUHK4150/07E). We also thank Dr. Haixuan Yang and Prof. Jianwei Huang for their constructive suggestions, and thank the anonymous reviewers for their insightful comments.

References

[1] L. Anderegg and S. Eidenbenz, "Ad hoc-vcg: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *MobiCom 2003: Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*. New York, NY, USA: ACM Press, 2003, pp. 245–259.

[2] L. Buttyan and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Department of Communication Systems, Swiss Federal Institute of Technology - Lausanne, Tech. Rep. DSC/2001/001, 2001.

[3] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *INFOCOM 2003: Proceedings of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2003, pp. 1987–1997.

[4] S. Zhong, L. E. Li, Y. G. Liu, and Y. R. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks - an integrated approach using game theoretical and cryptographic techniques," in *MobiCom 2005: Proceedings of the 11th Annual International Conference on Mobile Computing and Networking*. New York, NY, USA: ACM Press, 2005, pp. 117–131.

[5] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *CMS 2002: Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[6] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks." in *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*. Lausanne, CH: IEEE, June 2002.

[7] A. Patcha and J.-M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, vol. 2, no. 2, pp. 146–152, March 2006.

[8] A. Agah, S. K. Das, and K. Basu, "A game theory based approach for security in wireless sensor networks," in *Proceedings of IEEE International Conference on Performance, Computing, and Communications (IPCCC)*, 2004, pp. 259–263.

[9] J. Liu and V. Issarny, "An incentive compatible reputation mechanism for ubiquitous computing environments," *International Journal of Information Security*, vol. 6, no. 5, pp. 297–311, September 2007.

[10] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," in *Proceedings of IEEE Aerospace Conference*, vol. 2, March 2004, pp. 1286–1295.

[11] K. Kane and J. C. Browne, "Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*. New York, NY, USA: ACM, 2006, pp. 105–113.

[12] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, February 2006.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of Mobile Computing and Networking (MobiCom '00))*, 2000, pp. 255–265, http://citeseer.nj.nec.com/marti00mitigating.html.

[14] L. S. Shapley, *A Value for n-person Games*, ser. Annals of Mathematical Studies. Princeton University Press, 1953, vol. 28, ch. Contributions to the Theory of Games, pp. 307–317.

[15] D. Gale and L. Shapley, "College admissions and the stability of marriage," *American Mathematical Monthly*, vol. 69, pp. 9–14, 1962.

[16] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector (aodv) routing," Internet Draft, Feb 2003, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt.

[17] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (dsr)," Internet Draft, Apr 2003, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt.

[18] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in *Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*. London, UK: ACM Press, 1994, pp. 234–244, http://doi.acm.org/10.1145/190314.190336.

[19] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. The MIT Press, 1994.