Constrained Coalitional Games and Networks of Autonomous Agents

John S. Baras, Tao Jiang and Punyaslok Purkayastha
Institute for Systems Research,
Department of Electrical and Computer Engineering,
Department of Computer Science and,
Fischell Department of Bioengineering
University of Maryland, College Park, MD 20742, USA
Email: {baras, tjiang, punya}@umd.edu

***Abstract*— We develop a unifying analytical and optimization-based framework for the design, operation and performance evaluation of networks of dynamic autonomous agents. The fundamental view is that agents in such a network are dynamic entities that collaborate because via collaboration they can accomplish objectives and goals much better than working alone, or even accomplish objectives that they cannot achieve alone at all. Yet the benefits derived from such collaboration require some costs (e.g. communications), or equivalently, the collaboration is subject to constraints. Understanding and quantifying this tradeoff between the benefits *vs* the costs of collaboration, leads to new methods that can be used to analyze, design and control/operate networks of agents. Although the inspiration for the framework comes from social and economic networks, the fundamental ideas and in particular the methodology of dynamic constrained coalitional games (DCCG) can unify many concepts and algorithms for networks in various areas: social networks, communication networks, sensor networks, economic networks, biological networks, physics networks. We then analyze a specific instance of such tradeoffs arising in the design of security aware network protocols. We extend network utility maximization (NUM) so as to encompass security metrics such as "trust". The trust values assigned to nodes are based on interaction history and community-based monitoring. The effect of these trust values on the resulting protocols is that in routing and media access scheduling node trustworthiness is automatically considered and used. We develop a distributed algorithm for the joint physical-MAC-routing protocol design. Our extension to NUM with security concerns leads to resilient networks.**

Keywords: coalitions; games; collaboration; security; network utility; cross-layer.

I. INTRODUCTION

Dynamic networked systems are used as models for many phenomena and situations in science and engineering: communication networks, collaborating robots, organizations, societal systems and communities, commercial groups like merchant associations and virtual corporations, social systems based on the Internet (web-based social systems, economic systems like linked markets, biological systems like groups of dolphins or insects or cells, networks of biological reactions as in systems biology, wireless sensor networks, particle and other physics networks. Discovering fundamental principles governing the design-synthesis, control-operation, and performance evaluation of dynamic networked systems represents a major research challenge currently in science and engineering at large. The recent emphasis on and significance of this challenge is well described in the reports on *Network Science* [1], [2].

Autonomic networks rely on the collaboration of participating nodes for almost all their functionalities, for instance, to route data between source and destination pairs that are outside each other's communication range. In the case of packet forwarding, the fundamental user decision is between forwarding or not forwarding data packets sent by other users. Given the constraints (mostly related to energy) that the user faces, there is a very real cost incurred when choosing to forward.

In this paper we develop the fundamental view that agents in such a network are dynamic entities that collaborate because via collaboration they can accomplish objectives and goals much better than working alone, or even accomplish objectives that they cannot achieve alone at all. Yet the benefits derived from such collaboration require some costs (or expenditures), for example due to communications, or due to energy expenditure. Or in equivalent terms, the collaboration is subject to constraints (static or dynamic). Understanding and quantifying this tradeoff between the benefits *vs* the costs of collaboration, lead to new methods that can be used to analyze, design and control/operate networks of agents. Multiple metrics for benefits and costs can be considered within this framework; that is we can consider vector valued benefits and costs of collaboration. Although the inspiration for the framework comes from social and economic networks, it is our thesis that the fundamental ideas and in particular the methodology of dynamic constrained coalitional games can unify many concepts and algorithms for networks in various areas.

We assume that users want to be connected to many other users, directly (one-hop) or indirectly (multi-hop, through other users). Connections (or links) can be physical (like

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. Research also supported by the U.S. Army Research Office under grant No DAAD19-01-1-0494.

978-1-4244-1688-2/08/$25.00 ©2008 IEEE

a direct communication medium), or logical (or relational or functional) (like members of a subunit in an organization). Thus, the associated graphs (as well as neighborhoods) representing these connections can be physical or logical. By activating a communication link towards one of their neighbors, they gain by having access to the users with which that neighbor has activated *her* links, and so on, recursively. In the meanwhile, activation of links introduces cost.

Different with previous work in the literature, we study collaboration based on the notion of *coalitions*. The concept of users being connected to each other, and acquiring access to all the other users that each of them had so far access to, can be well captured by *coalitional game theory* (also known as cooperative game theory) [3], [4]). The key characteristic that distinguishes cooperative game theory from non-cooperative game theory is that players can negotiate collectively [5].

A question that has only relatively recently began to attract attention ([6] is the first work in this area) is the actual way in which the coalition is formed. The coalitional game is usually modelled as a *two-phase process*. Players must first decide whether or not to join a coalition. This is done by pairwise games, in which *both* players have to agree to activate a link between them and thus join the same coalition. In our work, this pairwise game involves, for each node, a comparison between the cost for activating the link towards the other node, and the benefit from joining the coalition that the other player is a member of. In the second step, players in one coalition negotiate the payoff allocation based on the total payoff of the coalition. The central problem is to study the convergence of the iterated pairwise game and whether the dynamics result in a stable coalition.

Optimization-based approaches have been extensively used over the years to study resource allocation problems in communication networks; examples are Kelly [7], and more recently network utility maximization (NUM) [8]. Recent advances in NUM driven cross-layer design [8] have led to top-down development of next generation wireless network architectures. By linking decomposition of the NUM problem to different layers of the network stack, we are able to design protocols, based on NUM algorithms, with much better performance over current network protocols. Cross-layer design [9], [10] achieves high performance by joint design of various layer protocols. Cross-layer design is more beneficial in wireless networks because the wireless channel is a shared medium where transmissions of users interfere with each other. A scheduling policy has to resolve the contention between various users attempting transmissions, which require global information.

In recent years, network security has become extremely important. Security in wireless networks is even more critical. Nodes in a network are assigned "trust" values that indicate their security status. These trust weights are developed by observing directly the actions of nodes (i.e. reputations) and by community-based monitoring [11], [12], [13], [14]. They are disseminated via efficient methods so that they are timely available to all nodes [15].

We investigate in this paper the critical tradeoff between protocol performance and network security, by developing an extension of NUM that incorporates security concerns. We consider network flows that share the resources of a wireless network. Each flow is described by its source-destination node pair. The effect of these trust weights on the resulting protocols is that in the scheduling problems involved (whether they are at the MAC or the routing protocol) 'node trustworthiness' is automatically considered and used. For example packets will not be routed through suspicious nodes. Or suspicious nodes will not be scheduled by the MAC protocol. The resulting protocols render the network resilient.

The rest of the paper is organized as follows: Section II describes the mathematical framework within which we deal with the concepts just discussed. The two-phase coalitional game is defined in Sec. III. Section IV investigates the dynamics of the iterated pairwise game including its convergence and the network topology at the equilibrium. We discuss the stability of the network at the equilibrium in constrained coalitional games in Sect. V. Section VI introduces the system model for secure protocols we consider in this paper, including the trust values, utility function, interference model and the statement of the optimization problem. Based on the dual function derived from Sec. VI, the decomposition of the dual function is studied in Sec. VII. Section VIII discusses the distributed scheduling algorithm. Section IX summarizes our conclusions.

II. Problem Formulation: Wireless Communications

The set of nodes in the network is $\mathcal{N} = \{1, 2, \ldots, n\}$. The communication structure of the network is represented by an *undirected* graph G, where a link between two nodes implies that they are able to directly communicate; these undirected links are also called *pairwise links*. For instance, in wireless networks, reliable transmissions require that two nodes cooperate in order to avoid collisions and interference.

Let $G^{\mathcal{N}}$ represent the complete graph, where every node is directly connected to every other node, and let the set $\mathcal{G} = \{G | G \subseteq G^{\mathcal{N}}\}$ be the set of all possible graphs with nodes $\mathcal{N}$. If i and j are *directly* linked in G, we write $ij \in G$. Let $G + ij$ denote the graph obtained by adding link ij to the existing graph G where $ij \notin G$ and $G - ij$ denote the graph obtained by severing link ij from the existing graph G where $ij \in G$ (i.e., $G + ij = G \cup \{ij\}$ and $G - ij = G \setminus \{ij\}$). The set of nodes in graph G is $\mathcal{N}(G) = \{i | i \in G\}$ and $n(G)$ is the number of nodes in G.

Once a link is added, two end nodes join the coalition and agree to forward all the traffic from each other. Note that *indirect communication* between two players requires that there is a path connecting them. A path in G connecting i_1 and i_m is a set of distinct nodes $\{i_1, i_2, \ldots, i_m\} \subset \mathcal{N}(G)$, such that $\{i_1 i_2, i_2 i_3, \ldots, i_{m-1} i_m\} \subset G$.

The communication structure G gives rise to a partition of the node set into groups of nodes who can communicate with each other. A *coalition* of G is a subgraph $G' \subset G$, where

$\forall i \in \mathcal{N}(G')$ and $j \in \mathcal{N}(G')$, $i \neq j$, there is a path in G' connecting i and j, and $ij \in G$ implies $ij \in G'$.

A. Collaboration gain

Users obtain benefits by joining a coalition. We use a simple model here, whereby we assume that each node potentially offers to other nodes benefits V per time unit; e.g. number of bits per time unit each node could provide – a function of the link capacity. The potential benefit V is an expected value, which may be reduced during transmissions in the network. Following the Jackson-Wolinsky *connections model* [16], the gain of node i is defined as

$$w_i(g) = \sum_{j \in G} V \delta^{r_{ij}-1}, \qquad (1)$$

where r_{ij} is the number of hops in the shortest path between i and j (also known as the *geodesic distance* in graph theory), and $0 \leq \delta \leq 1$ is the communication depreciation rate. If there is no path between i and j, $r_{ij} = \infty$. Paths with smaller number of hops induce higher gain. The depreciation can be explained by communication reliability and efficiency due to transmission failures or delay.

B. Collaboration cost

On the other hand, activating links is costly. For instance, the cost for user i to activate her communication link to user j can be equal to the transmission energy (or power) necessary for i to send data to j. Following common wireless propagation and transmission power consumption models, we define the cost c_{ij} as

$$c_{ij} = P d_{ij}^{\alpha}, \qquad (2)$$

where P is a parameter depending on the transmitter/receiver antenna gain and the system loss not related to propagation, d_{ij} is the *geometric distance* (different from the geodesic distance r_{ij}), and α is the path loss exponent depending on the specific propagation environment.

III. Coalition formation game

The coalition formation is modelled as a two-phase process, which is called *coalition formation game* in the literature [4].

A. Phase I: pairwise game

The pairwise game is modelled as an iterated process in which individual nodes activate and delete links based on the improvement that the resulting networks offers them relative to the current network. Each user receives a payoff based on the network configuration that is in place.

Initially the n nodes are disconnected. The nodes meet over time and have the opportunity to form links with each other. Time, T, is divided into periods and is modelled as a countable, infinite set, $T = \{1, 2, \ldots, t, \ldots\}$. Let $G^{(t)}$ represent the network that exists at the end of period t. A *strategy* of node i is a vector, defined as $\boldsymbol{\gamma_i} = (\gamma_{i,1}, \ldots, \gamma_{i,i-1}, \gamma_{i,i+1}, \ldots, \gamma_{i,n})$, where $\gamma_{i,j} \in \{0, 1\}$ for each $j \neq i$. $\gamma_{i,j} = 1$ states that node i wants to form a link with node j, while $\gamma_{i,j} = 0$ states that i does not. The set of all strategies of node i is denoted by Γ_i. The set $\Gamma = \Gamma_1 \times \cdots \times \Gamma_n$ is the strategy space of all the nodes. A link ij is formed in network G only if $\gamma_{i,j} = 1$ and $\gamma_{j,i} = 1$. A strategy profile $\boldsymbol{\gamma}^{(t)} = (\boldsymbol{\gamma_1}^{(t)}, \ldots, \boldsymbol{\gamma_n}^{(t)})$ at time period t corresponds to the network $G^{(t)}$ at time t.

Define $\mathcal{N}_i(G) = \{j \in \mathcal{N} | ij \in G\}$ as the neighbor set of node i. Furthermore, a pair of nodes are *connected* in network G if there is a path between i and j, denoted as $i \overset{G}{\longleftrightarrow} j$. We define $\mathcal{C}_i(G) = \{j \in \mathcal{N} | i \overset{G}{\longleftrightarrow} j\}$ as the set of all nodes with whom i communicates, either directly or through other nodes. The payoff of node i from the network G is defined as

$$v_i(G) = w_i(G) - c_i(G) = \sum_{j \in \mathcal{C}_i(G)} V \delta^{r_{ij}-1} - \sum_{j \in \mathcal{N}_i(G)} P d_{ij}^{\alpha}. \qquad (3)$$

The iterated pairwise game is repeated in each time period $t = 1, 2, \ldots$. Let p_{ij} be the probability that the node pair ij is selected, in each time period, to play the pairwise game. If both ij and ik are selected, i cannot play two games simultaneously. This dynamic process requires no communication or synchronization for selecting node pairs and playing games. Each pair of nodes tosses a coin to decide whether they need play the game. If a node is selected to play the game, he first checks if he plays two or more games simultaneously. If yes, it stops all of the games and informs its neighbors. Therefore, the dynamic pairwise game is purely distributed. The nodes act myopically, activating a link if it makes each at least as well off and one strictly better off, and deleting the link if its deletion makes either player better off. Mathematically speaking, if only node pair ij is selected in time period t, then the network $G^{(t+1)}$ has either

- $G^{(t+1)} = G^{(t)} - ij$ if $v_i(G^{(t)} - ij) > v_i(G^{(t)})$ or $v_j(G^{(t)} - ij) > v_j(G^{(t)})$, or
- $G^{(t+1)} = G^{(t)} + ij$ if $v_i(G^{(t)} + ij) > v_i(G^{(t)})$ and $v_j(G^{(t)} + ij) \geq v_j(G^{(t)})$, or $v_i(G^{(t)} + ij) \geq v_i(G^{(t)})$ and $v_j(G^{(t)} + ij) > v_j(G^{(t)})$, or
- $G^{(t+1)} = G^{(t)}$ if none of the above is satisfied.

If after some time period t, no additional links are formed or severed, then network formation has reached a *stable state*. Thus a coalition or coalitions are formed at the stable state. Then the coalition formation game moves to the second phase, in which users act together to achieve maximum payoffs.

B. Phase II: coalitional game

A coalition is a subset of nodes that is connected in the subgraph induced by the active links. If two nodes of separate coalitions join, then the two coalitions *merge* into one. In this paper, we are interested in the total productivity of the coalition formed, how it is allocated among the individual nodes and the stability of the coalition.

Coalition formation has been widely studied in economics and sociology in the context of coalitional games [4], [17]. In our game, some nodes are not directly connected with each other; therefore the game we consider has to take the communication constraints into consideration. Myerson [18] was the first to introduce a new game associated with communication constraints, the *constrained coalitional game*, which incorporates both the possible gains from cooperation as modelled by the coalitional game and the restrictions on communication reflected by the communication network.

An important concept in coalitional games is the characteristic function v [19]. Since the game we study has communication constraints, the characteristic function v is defined on a particular network rather than on a set of nodes in general coalition games, i.e., $v : G^N \to \mathbb{R}$ defined on all subsets of G with the convention: $v(\emptyset) = 0$. Notice that in our work the empty set $\emptyset$ represents a graph where there is no link between any two nodes in the graph. Given $G \subset G^{\mathcal{N}}$, $v(G)$ is interpreted as the maximum payoff the network G can get given the network structure.

In our case, the value of v is the maximum aggregate of the payoffs from all nodes in the graph

$$v(G) = \sum_{i \in G} v_i(G) \tag{4}$$

A payoff allocation rule $x : G \to \mathbb{R}^n$ describes how the value $v(G)$, associated with each network, is distributed to the individual nodes. $x_i(G)$ is the payoff of node i from network G and under the characteristic function v. For a graph G', which is a subgraph of G, define

$$x(G') = \sum_{i \in G'} x_i(G).$$

The payoff allocation is *feasible* if $x(G) \leq v(G)$ and *efficient* if $x(G) = v(G)$. In our case, the payoff may not be transferable, so the payoff allocation rule represents the payoff that each node receives from the network, i.e., $x_i(G) = v_i(G)$. It is easy to show that such a payoff allocation rule is feasible and efficient. We will discuss the stability of the constrained coalitional game in detail in Sect. V.

IV. Dynamics of the Iterated Pairwise Game

A. Convergence

We are interested in the conditions under which all nodes in the network are connected, i.e., $\mathcal{C}_i = \mathcal{N}, \forall i \in \mathcal{N}$. The coalition that contains all the nodes is called the "grand coalition". To study convergence, we define *pairwise stability*.

Definition 1 A network G is *pairwise stable* if

- For all $ij \in G$, $v_i(G) \geq v_i(G - ij)$ and $v_j(G) \geq v_j(G - ij)$,
- For all $ij \notin G$, if $v_i(G) < v_i(G + ij)$ then $v_j(G) > v_j(G + ij)$ or if $v_j(G) < v_j(G + ij)$ then $v_i(G) > v_i(G + ij)$.

Then we have the following result (see [20] for the proof):

Lemma 1: The iterated pairwise game converges to a pairwise stable network or a cycle of networks.

Since it is possible to converge to an inefficient, pairwise stable network, some random perturbations are needed to help the network jump out of the inefficient stable network. In evolutionary games, mutations are introduced such that the evolution of the game is modelled as a Markov chain, where the states of the Markov chain are the strategy profiles γ. The work of Harsanyi and Selten [21] and Kardori, et al, [22] show that by letting the mutation probability go to 0 in a certain way, the game converges to a unique Pareto equilibrium. The mutations for network formation mean that when two nodes agree to form a link, with a probability ϵ, the link is not formed, or when a link is to be deleted (one node chooses to sever it), it is not deleted with probability ϵ.

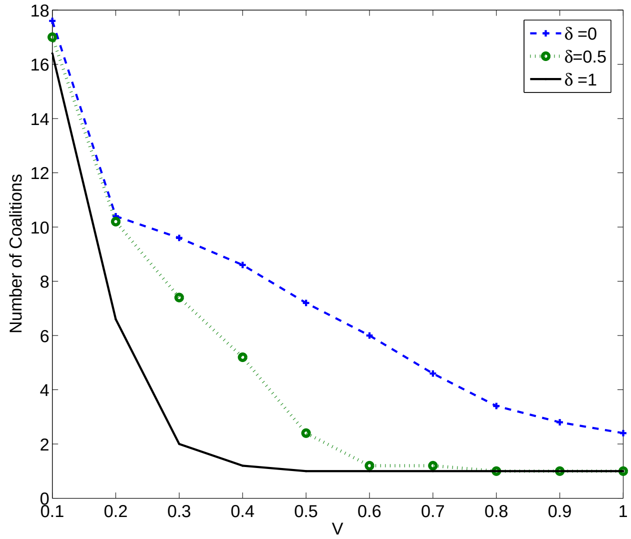


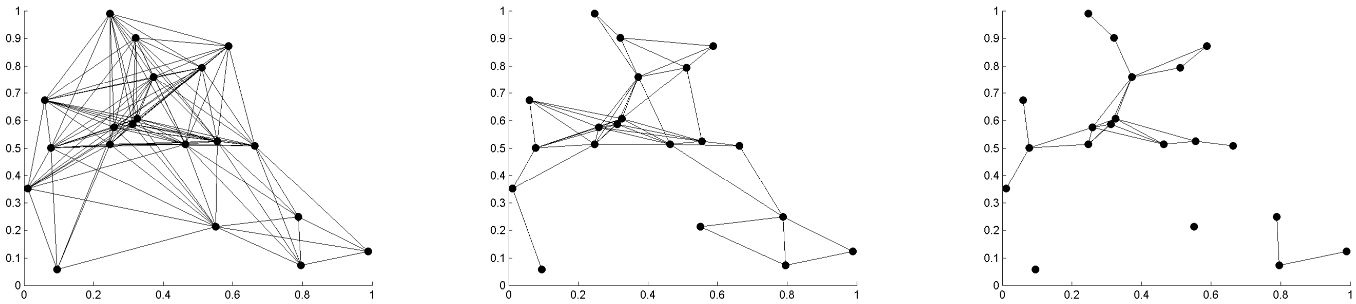
Fig. 1. Number of coalitions *vs* payoff V. $P = 10, \alpha = 2$.

One of the main differences our model has compared to other game models [23] is that the cost is not a constant, but a function of the distance between two nodes. Therefore, the physical locations of nodes in the network are important for the coalition formation. We consider the network as a random network where nodes are placed according to a uniform Poisson point process on the $[0, 1] \times [0, 1]$ square with the periodic boundary. We are mainly concerned with results that occur with high probability as $n \to \infty$. Based on the connectivity analysis of the continuous percolation model in [24] and [25], we have (see [20] for the proof):

Theorem 2: The coalition formation at the stable state depends on the parameters δ for gain and α for cost.

1) Given $\delta = 0$, $V = P \left(\frac{\log n}{n}\right)^{\frac{\alpha}{2}}$ is a *sharp* threshold for establishing the grand coalition.
   - If V is greater than the threshold, w.h.p., all nodes collaborate with at least one of their neighbors.
   - If V is less than the threshold, w.h.p., the network is partitioned into small coalitions.
2) For $0 < \delta \leq 1$, the threshold is less than $P \left(\frac{\log n}{n}\right)^{\frac{\alpha}{2}}$.

In simulation experiments, 20 nodes are randomly placed on a $[0, 1] \times [0, 1]$ square. Two nodes are selected to play the pairwise game according to a fixed probability $1/n(n-1)$, where $n = 20$. Figure 1 shows the number of coalitions when the network reaches the pairwise stable state. The threshold



(a) P = 0.5 (low cost); complete graph (b) P = 2 (middle cost); small world topology (c) P = 4 (high cost); partitioned network

Fig. 2. Topology of the network with various cost parameters. $V = 1, \delta = 0.2, \alpha = 2$ for all three figures.

predicted by our analytic results does exist for different δ's. When $\delta = 1$, the phase transition happens very sharply; a grand coalition is formed. On the other hand, for $\delta = 0$, only nodes closer to each other may form a link.

B. Topology

Three figures in Fig. 2 give the topology of a network formed with different cost parameters. As we can observe, when cost is low, the network forms as a complete graph. The other extreme end is when the cost is high, which results in a partitioned network. The most valuable topology is shown in Fig. 2(b). This figure represents the most common scenario in real life. Interestingly, the topology shows the *small-world* property: most links are connected between neighbors with few long-range shortcuts. Recently, there has been substantial research on the small-world model in various complex networks, such as the Internet and biological systems. Our formation game converges to a small world topology as well. This further proves that the small world model is an efficient communication structure.

V. Stability of Coalitions

We have also investigated a stronger stability concept : a *core stable* network [26].

Definition 2 A network $G \subset G^{\mathcal{N}}$ is *core stable*, if there does not exist any set of nodes $\mathcal{S} \subset \mathcal{N}$ and $\hat{G} \subset G^{\mathcal{N}}$ such that:

- $x_i(\hat{G}) \geq x_i(G)$ for all $i \in \mathcal{S}$ and there is at least one node with strict inequality,
- if $ij \in \hat{G}$ but $ij \notin G$, then $i, j \in \mathcal{S}$,
- if $ij \notin \hat{G}$ but $ij \in G$, then either $i \in \mathcal{S}$ and/or $j \in \mathcal{S}$.

Core stability allows that a node is able to interact and coordinate with any other node in the same coalition. This stronger stability is very useful in real networks, where users in the network can act together to achieve better payoffs.

VI. System Model for Secure Protocols

In this section, we introduce an extension of Network Utility Maximization (NUM) [8], [7], [27], as a method to design network protocols, from a cross-layer perspective, that take into account security or information assurance considerations. All previous work on NUM assumes that nodes function correctly. For instance, intermediate nodes always successfully forward all packets, and they follow the routing and scheduling protocols. However, nodes do not always function correctly in reality. They may be compromised by attackers, their communications may be blocked or interfered by attackers, or they may just simply malfunction. Wireless networks are especially vulnerable to attacks because of the inherent properties of the shared wireless media.

We consider a multihop wireless network with node set $\mathcal{N}$. Let $\mathcal{L}$ denote the set of links ij such that the transmission from node i to node j is possible. The interference constraints among transmission links will be described later. The wireless network can be described as a graph $(\mathcal{N}, \mathcal{L})$.

A. Trust

The particular concept of security we are using is "trust". Trust is a very critical concept not only in computer networks, but also in various other networks that involve intelligent decisions, such as social, economic and biological networks. All the connections and communications in these networks imply the existence of trust. Trust management is to collect, analyze and present trust related evidence and to make assessments and decisions regarding trust relationships between entities in a network [28]. The collection of trust evidence and assessments and decisions of trust are beyond the scope of this paper; see [11], [12], [13], [14]. We assume that there are mechanisms to efficiently evaluate the 'trustworthiness' of nodes in the network. For instance, in wireless environments, monitoring mechanisms can help detect the behaviors of neighboring nodes and thus infer their trust values [29]. In this paper, we assume the trust value of node i is fixed and denoted as v_i. The methods and algorithms extend easily to time varying values of trust.

B. Data flows and utility functions

There are F flows that share the network resources and each flow f is associated with a source node s_f and a destination node d_f. The set of all F flows is denoted as $\mathcal{F}$. Let x_f be the rate with which data is sent from s_f to d_f over possibly multiple paths and multiple hops.

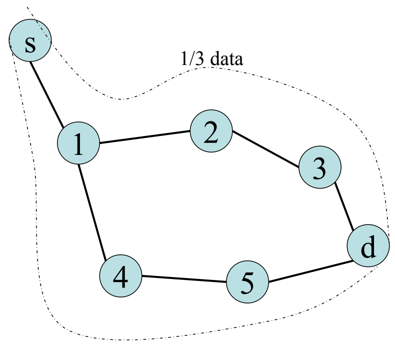


Fig. 3. An example network with 2 routes for flow from s to d.

In our model, the flow can use different routes in the network. Suppose the set of routes for flow f is R_f. A route $r \in R_f$ is a set of nodes on the route, i.e., $i \in r$ means that node i is on route r. We define the *trust value* (or trustworthiness) of route r as the product of the trust values of nodes on the route, that is

$$v_r = \prod_{i \in r} v_i.$$

Clearly, there are several different ways to assign a trust value to a route given the trust values of the nodes on it; see [12], [14], [13]. We have selected this particular way here to simplify the exposition. Let p_r be the portion of data of flow f transmitted on route r. The *aggregate trust value* of flow f is

$$g_f = \sum_{r \in R_f} p_r v_r. \tag{5}$$

For instance, Fig. 3 shows the flow f from node s to d. The flow uses two routes. One third passes through nodes 1, 2 and 3, while the rest passes through nodes 1, 4 and 5. The aggregate trust value of flow f is

$$g_f = v_1(\frac{1}{3}v_2v_3 + \frac{2}{3}v_4v_5). \tag{6}$$

g_f represents a measure of the trust (or security quality) of all routes that serve flow f traffic. It is an average. There are several ways to assign a trust value to the set of routes serving a flow; see [12], [13]. We have used this particular one for simplicity.

Naturally users prefer data to be transmitted on paths with high trust values. To represent this user preference we associate a utility function with each flow f, which is a function of the data rate x_f and of the trust values of the paths that serve the traffic of flow f. There are several ways to define such utility functions, and their dependence on rates and trust. Here we use utility functions of the form $U_f(x_f g_f)$, which reflect the "utility" of flow f when it can successfully transmit at data rate x_f. We assume, as is usual in NUM [8], [27], that $U_f(\cdot)$ is strictly concave, nondecreasing and continuously differentiable. For two flows with the same data rate, the one using paths with higher aggregate trust value has higher utility. We let $\hat{x}_f = x_f g_f$ denote the 'effective data rate' for flow f, from the perspective of security (or trust).

C. Interference model and stability

The data rate of each link depends on the transmission power and interference from other transmissions. We let $u(H, P, BW, N_0)$ denote the rate a particular link transmits, as a function of the power assigned $P = [P_{ij}, ij \in \mathcal{L}]$, the gain matrix H, the noise power N_0, and the link bandwidth BW. We assume H, BW and N_0 are constants (i.e. not design variables) so the rate function depends only on P.

We let $\boldsymbol{\mu} = \{\mu_{ij}\}_{ij \in \mathcal{L}}$ denote the rate vector over all links in $\mathcal{L}$. Then $\boldsymbol{\mu} = u(P)$. We let Ω denote a bounded region of $|\mathcal{L}|$ dimensions, representing the set of $\boldsymbol{\mu}$ that can be achieved in a given time slot due to the interference constraints [30]. Notice that Ω may not be convex. We let $\hat{\Omega} := Co\{\Omega\}$ denote the convex hull of Ω. $\hat{\Omega}$ can be achieved by timesharing between different rate vectors in Ω. $\hat{\Omega}$ is convex, closed and bounded.

The *capacity region* Λ of the network [30] is the largest set of rate vectors $\boldsymbol{x}$ such that $\boldsymbol{x} \in \Lambda$ is a necessary condition for network stability under *any* scheduling policy. We assume that nodes keep a queue for each flow. Let μ_{ij}^f denote the amount of capacity on link ij that is allocated for flow f. We have the following definition of the capacity region [30], [8].

Definition 3 The *capacity region*, Λ, of the network contains the set of flow rates $\boldsymbol{x}$ for which there exists $\boldsymbol{\mu}$ that satisfies the following [30].

1) $\mu_{ij}^f \geq 0$ for all $ij \in \mathcal{L}$ and for all $f \in \mathcal{F}$.
2) for all $f \in \mathcal{F}$ and for all $i \in \mathcal{N}$, we have

$$\sum_{j:(i,j) \in \mathcal{L}} \mu_{ij}^f - \sum_{j:(j,i) \in \mathcal{L}} \mu_{ji}^f - x_f \mathbf{1}(i = s_f) \geq 0. \tag{7}$$

3) $\{\sum_f \mu_{ij}^f\} \in \hat{\Omega}$.

$\mathbf{1}(i = s_f)$ is an indicator function. $\mathbf{1}(i = s_f) = 1$ if i is the source of flow f, and $\mathbf{1}(i = s_f) = 0$ otherwise. The condition 2) is the flow constraint that must hold at each node, and the condition 3) captures the interference constraints.

VII. Utility Optimization and Dual Decomposition

Our goal is to design a scheduling mechanism such that the flow rate x_f solves the following optimization problem:

$$\begin{aligned} \text{maximize}_{\hat{\boldsymbol{x}}} \quad & \sum_f U_f(\hat{x}_f) && (8) \\ \text{subject to} \quad & \boldsymbol{x} \in \Lambda && (9) \\ & \hat{x}_f = g_f \cdot x_f \text{ for all } f \in \mathcal{F} && (10) \end{aligned}$$

We refer to the above as the *primal problem.* Due to the strict concavity assumption of $U_f(\cdot)$ and the convexity of the capacity region, there exists a unique optimizer of the primal problem, which we refer as $\hat{\boldsymbol{x}}^*$.

In order for us to provide a distributed solution to the problem we use the technique of dual decomposition [31], [27]. By decomposing the optimization problem, we develop decentralized algorithms. Some of the optimal algorithms require centralized information and thus are not feasible for distributed implementation.

Notice that the variables g_f and $\hat{x}_f$ are coupled by the second constraint Eqn. (10). In this work, we take the log of variables to decouple g_f and $\hat{x}_f$ and log change of variables and constants: $\hat{x}'_f = \log \hat{x}_f$, $g'_f = \log g_f$, $x'_f = \log x_f$, and $U'_f(\hat{x}'_f) = U_f(e^{\hat{x}'_f})$. Now the primal problem is separable.

After the log change, we decompose the primal problem by defining Langrange multipliers λ_i^f and ν_f that are associated with the stability constraints stated in Eqn. (9) and (10). We get the following dual function:

$$\begin{aligned} L(\boldsymbol{\lambda}, \boldsymbol{\nu}, \hat{\boldsymbol{x}}, \boldsymbol{x}, \boldsymbol{\mu}, \boldsymbol{g}) &= \sum_f \max_{x'_f} \left\{ \nu_f x'_f - \lambda_{s_f}^f e^{x'_f} \right\} && (11) \\ &+ \sum_f \max_{\hat{x}'_f} \left\{ U'_f(\hat{x}'_f) - \nu_f \hat{x}'_f \right\} && (12) \\ &+ \max_{\boldsymbol{g}'} \sum_f \nu_f g'_f && (13) \\ &+ \max_{\mu \in \hat{\Omega}} \sum_{ij \in \mathcal{L}} \sum_{f \in \mathcal{F}} \mu_{ij}^f (\lambda_i^f - \lambda_j^f) && (14) \end{aligned}$$

The dual objective function is

$$h(\boldsymbol{\lambda}, \boldsymbol{\nu}) = \sup_{\substack{\boldsymbol{x} \in \Lambda \\ \hat{x_f} = g_f \cdot x_f}} L(\boldsymbol{\lambda}, \boldsymbol{\nu}, \hat{\boldsymbol{x}}, \boldsymbol{x}, \boldsymbol{\mu}, \boldsymbol{g}) \qquad (15)$$

For a given $\boldsymbol{\lambda}$ and $\boldsymbol{\nu}$, there are now three, decoupled, maximization problems we can solve separately, i.e., source rate control, routing and scheduling. By solving for these independently, we can produce $\hat{\boldsymbol{x}}'^*(\boldsymbol{\lambda}, \boldsymbol{\nu})$, $\boldsymbol{x}'^*(\boldsymbol{\lambda}, \boldsymbol{\nu})$, $\boldsymbol{\mu}^*(\boldsymbol{\lambda}, \boldsymbol{\nu})$ and $\boldsymbol{g}^*(\boldsymbol{\lambda}, \boldsymbol{\nu})$. Given these values, we can then solve the dual problem by minimizing $h(\boldsymbol{\lambda}, \boldsymbol{\nu})$ over $\boldsymbol{\lambda}, \boldsymbol{\nu}$. Because the capacity region Λ is a convex set, there is no duality gap between the primal and the dual. In the rest of this section, we discuss the dual decomposition techniques in details.

The data rate of flow f is determined by the maximization over x' in the problem represented by Eqn. (11) and Eqn. (12) taken together. Note that each source node adjusts its rate using only local information $\lambda_{s_f}^f$ and ν_f, thus the source rate control can be distributed across source nodes.

Eqn. (13) determines the route.

$$\boldsymbol{g}' = \text{argmax}_{\boldsymbol{g}'} \sum_f \nu_f g'_f. \qquad (16)$$

We have that the optimal routing for flow f is to always choose the route with the highest trust value. Since the trust values are fixed, routing can be decided off-line.

Eqn. (14) determines the schedule.

$$\boldsymbol{\mu} = \text{argmax}_{\mu \in \hat{\Omega}} \sum_{ij \in \mathcal{L}} \sum_{f \in \mathcal{F}} \mu_{ij}^f (\lambda_i^f - \lambda_j^f) \qquad (17)$$

To maximize Eqn. (17), the term inside the second summation should take one single flow f such that $(\lambda_i^f - \lambda_j^f)$ is maximized. Therefore we have that

$$\mu_{ij}^f = \mu_{ij} \text{ if } f = \text{argmax}_f (\lambda_i^f - \lambda_j^f), \qquad (18)$$

and $\mu_{ij}^f = 0$ otherwise. The schedule of link rates in Eqn. (18) is the same as the *back-pressure scheduler* introduced by Tassiulas [32]. Notice that the maximization in Eqn. (18) is performed over $\hat{\Omega}$, which requires centralized knowledge. In the next section, we propose a distributed algorithm which optimizes the network utility.

VIII. Distributed Algorithm

The scheduling sub-problem discussed in the last section requires global knowledge on the rate vector, which becomes the bottleneck for solutions in wireless networks. In this section, we develop a distributed implementation of the maximization problem. We assume that time is divided into slots. At each time slot, source nodes choose the flow data rate and the scheduling policy selects data to be forwarded on each link.

The source node of each flow uses its local multiplier and the utility function associated with that flow to update the flow rate in an iterative manner. One example of the rate controller is directly derived from Eqn. (11) and Eqn. (12):

$$\begin{aligned} x'_f[t+1] &= \text{argmax}_{x'_f} \left\{ \nu_f[t] x'_f - \lambda_{s_f}^f[t] e^{x'_f} \right\}, && (19) \\ \hat{x}'_f[t+1] &= \text{argmax}_{\hat{x}'_f} \left\{ U'_f(\hat{x}'_f) - \nu_f[t] \hat{x}'_f \right\}. && (20) \end{aligned}$$

The subgradient of $h(\boldsymbol{\lambda}, \boldsymbol{\nu})$ is given by

$$\begin{aligned} \frac{\partial h}{\partial \lambda_i^f} &= \sum_{j:ij \in \mathcal{L}} \mu_{ij}^f - \sum_{j:ij \in \mathcal{L}} \mu_{ji}^f - e^{x'_f} \mathbf{1}(i = s_f), && (21) \\ \frac{\partial h}{\partial \nu_f} &= g'_f + x'_f - \hat{x}'_f. && (22) \end{aligned}$$

We can then use the following subgradient method to solve the dual problem.

$$\begin{aligned} \lambda_i^f[t+1] &= \left\{ \lambda_i^f[t] - \beta[t] \left(\sum_{j:ij \in \mathcal{L}} \mu_{ij}^f[t] - \right. \right. \\ &\qquad \left. \left. \sum_{j:ij \in \mathcal{L}} \mu_{ji}^f[t] - e^{x'_f[t]} \mathbf{1}(i = s_f) \right) \right\}^+, && (23) \\ \nu_f[t+1] &= \left\{ \nu_f[t] - \beta[t] (g'_f[t] + x'_f[t] - \hat{x}'_f[t]) \right\}^+ && (24) \end{aligned}$$

where $\beta[t], t = 1, 2, \ldots$ is a sequence of positive step sizes. $\mu_{ij}^d[t]$, $g'_f[t]$, $\hat{x}'_f[t]$ and $x'_f[t]$ are defined as earlier with time slot t. According to Theorem 2.3 in [33], we know that there is no duality gap, the iterations converge to an $\boldsymbol{x}'$, which solves the maximization problem, and such a $\boldsymbol{x}'$ is the unique optimal solution.

Notice that the scheduling problem of Eqn. (17) requires global information. In this work, we consider the solution to the scheduling problem that is coupled to the power control problem, as in Lin and Shroff [34]. The link transmission powers determine an explicit form for the allowable rate region $\hat{\Omega}$. The scheduling problem is posed as an optimization problem, whose solution gives us the transmission powers. At optimality, each node should transmit at full power or shut off, and also should transmit to at most one neighbor - the solution is thus distributed.

IX. Conclusions

In this paper, we studied autonomic networks, which rely on the collaboration of participating nodes. There are fundamental tradeoffs between the benefit from collaboration and the required cost for collaboration. This conflict naturally led us to game-theoretic methods.

We developed constrained coalitional games as a promising methodology to analyze such fundamental tradeoffs. These are two-phase coalition formation games. In the first phase, users play pairwise games to decide whether to form or sever a link between them based on their payoffs. This phase leads to coalition formation. In the second phase, users in the same coalition interact to maximize the total payoff. We investigated the convergence of the iterated pairwise games and derived conditions for forming a grand coalition. The network topology of the resulting coalition was also investigated. We also studied the stability of the formed coalition in the sense of core stability.

We next investigated an important application of such tradeoffs by introducing security considerations in the cross layer design of network protocols via network utility maximization. The specific concept of security we used is "trust". Users get higher utility by transmitting data through nodes of higher trust values. Thus, trust weights are used as parameters in the optimization problem. Through decomposition of the dual, we showed that the trustworthiness of nodes is automatically considered in the routing and scheduling problems. We also developed a decentralized algorithms that achieves utility maximization. The resulting trust aware protocols are resilient to network errors and attacks.

References

[1] National Research Council of the National Academies, *Network Science*. The National Academies Press, 2005.

[2] ——, *Strategy for an Army Center for Network Science, Technology, and Experimentation*. The National Academies Press, 2007.

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

[4] M. Slikker and A. Van den Nouweland, *Social and Economic Networks in Cooperative Game Theory*. Kluwer Academic Publishers, 2001.

[5] R. B. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1991.

[6] R. J. Aumann and R. B. Myerson, "Endogenous formation of links between players and of coalitions: An application of the shapley value," in *The Shapley Value: Essays in Honor of Lloyd Shapley*, A. Roth, Ed. Cambridge University Press, Cambridge, UK, 1988, pp. 175–191.

[7] F. Kelly, M. A.K., and D. Tan, "Rate control in communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research Society*, vol. 49, pp. 237–252, 1998.

[8] M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, "Layering as optimization decomposition: A mathematical theory of network architectures," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 255–312, January 2007.

[9] X. Lin, N. B. Shroff, and R. Srikant, "A tutorial on cross layer optimization in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1452–1463, August 2006.

[10] R. Jurdak, *Wireless Ad Hoc and Sensor Networks : A Cross-Layer Design Perspective*. Springer, 2007.

[11] J. S. Baras and T. Jiang, "Cooperation, trust and games in wireless networks," in *Proceedings of Symposium on Systems, Control and Networks , in honor of P. Varaiya*, 2005, pp. 183–202.

[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] J. S. Baras, "Security and trust for wireless autonomic networks : System and Control methods," *European Journal of Control*, vol. 13, no. 2, pp. 105–133, 2007.

[14] T. Jiang and J. S. Baras, "Trust evaluation in anarchy: A case study on automomous networks," in *Proceedings of 25th IEEE Conference on Computer Communications (Infocom06)*, Barcelona, Spain, 2006.

[15] ——, "Trust document distribution in MANETs," Proceedings of 2007 Milcom, 2007.

[16] M. O. Jackson and A. Wolinsky, "A strategic model of social and economic networks," *Journal of Economic Theory*, vol. 71, no. 1, pp. 44–74, October 1996.

[17] B. Dutta and M. O. Jackson, Eds., *Networks and Groups: Models of Strategic Formation*. Springer-Verlag Berlin Heidelberg, 2003.

[18] R. B. Myerson, "Graphs and cooperation in games," *Mathematics of Operations Research*, vol. 2, pp. 225–229, 1977.

[19] F. Forgo, J. Szep, and F. Szidarovszky, *Introduction to the Theory of Games: Concepts, Methods, Applications*. Kluwer Academic Publishers, 1999.

[20] T. Jiang and J. S. Baras, "Fundamental tradeoffs and constrained coalitional games in autonomic wireless networks," in *Proceedings of 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt07)*, Limassol, Cyprus, 2007.

[21] J. C. Harsanyi and R. Selten, *A General Theory of Equilibrium in Games*. Cambridge MIT Press, 1988.

[22] M. Kandori, G. J. Mailath, and R. Rob, "Learning, mutation, and long run equilibria in games," *Econometrica*, vol. 61, no. 1, pp. 29–56, 1993.

[23] V. Bala and S. Goyal, "A noncoperative model of network formation," *Econometrica*, vol. 68, no. 5, pp. 1181–1129, September 2000.

[24] R. Meester and R. Roy, *Continuum Percolation*. Cambridge University Press, 1996.

[25] M. Penrose, *Random Geometric Graphs*. Oxford University Press, 2003.

[26] M. O. Jackson and A. Watts, "The evolution of social and economic networks," *Journal of Economic Theory*, vol. 106, pp. 265–295, 2002.

[27] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1439–1451, August 2006.

[28] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The role of trust management in distributed systems security," *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, pp. 185–210, 1999.

[29] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, Boston, Massachusetts, United States, 2000, pp. 255–265.

[30] M. J. Neely, E. Modiano, and C. E. Rohrs, "Dynamic power allocation and routing for time varying wireless networks," in *Proceedings of IEEE INFOCOM*, vol. 1, April 2003, pp. 745–755.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. Cambridge, MA: Cambridge, 2004.

[32] L. Tassiulas, "Scheduling and performance limits of networks with constantly varying topology," *IEEE Transaction on Information Theory*, vol. 43, no. 3, pp. 1067–1073, May 1997.

[33] N. Z. Shor, *Minimization Methods for Non-Differentiable Functions*. Berlin: Springer-Verlag, 1985.

[34] X. Lin and N. B. Shroff, "Joint rate control and scheduling in multihop wireless networks," in *Proceedings of 48th IEEE COnference on Decision and Control*, vol. 2, Paradise Island, Bahamas, December 2004, pp. 1484–1489.