Distributed Aggregative Games on Graphs in Adversarial Environments

Bahare Kiumarsi(✉) and Tamer Başar

Coordinated Science Laboratory, University of Illinois at Urbana-Champaign,
1308 West Main Street, Urbana, IL 61801, USA
{kiumarsi,basar1}@illinois.edu

Abstract. Existing solutions to aggregative games assume that all players are fully trustworthy for cooperative tasks or, in a worst-case scenario, are selfish players with no intent to intentionally harm the network. Nevertheless, the need to believe that players will behave consistently exposes the network to vulnerabilities associated with cyber-physical attacks. This paper investigates the effects of cyber-physical attacks on the outcome of distributed aggregative games (DAGs). More specifically, we are seeking to answer two main questions: (1) how a stealthy attack can deviate the game outcome from a cooperative Nash equilibrium, and by doing so, (2) by how much efficiency of a DAG degrades. To this end, we first show that adversaries can stealthily manipulate the outcome of a DAG by compromising the Nash equilibrium solution and consequently lead to an emergent misbehavior or no emergent behavior. This study will intensify the urgency of designing novel resilient solutions to DAGs so that the overall network sustains some notion of acceptable global behavior in the presence of malicious agents. Finally, we corroborate and illustrate our results by providing simulation examples. Simulations reveal that the adverse effect of a compromised agent is considerably worse than that of a selfish agent.

Keywords: Distributed aggregative games · Adversarial environment

1 Introduction

Game theory has been widely and successfully employed in many applications to model both selfish objectives of participants, as well as their global and common objectives. Aggregative game is a special type of a game in which the objective function for each agent depends on the local state of the agent (to fulfill an individual selfish objective) as well as on an aggregate quantity of the network,

Research reported in this paper was sponsored in part by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-17-2-0196. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

L. Bushnell et al. (Eds.): GameSec 2018, LNCS 11199, pp. 296–313, 2018.
https://doi.org/10.1007/978-3-030-01554-1_17

such as the average or sum of the states (actions) of all agents (to fulfill a common group objective) [1–7]. Applications span from demand-side management in smart grids [8–10] to charging coordination of plug-in electric vehicles [11,12], power and rate control in communication networks [13–15], and economic markets [16].

Most of the existing solutions to aggregative games employ a central coordinator that receives the decision variable of all the agents, calculates the aggregate decision, and broadcasts it to all agents. The agents then use this aggregate estimate to minimize their objective functions and consequently find a Nash equilibrium solution of the game. However, to avoid massive communication requirement and provide scalability, decision algorithms need to be distributed in the sense that each agent should take its decision using local information of its own state and its neighbors' states. In [17,18], a distributed method is presented to estimate the aggregate decision and consequently find the Nash equilibrium. Agents exchange their information with their neighbors to reach consensus on the aggregate value. The information flow of agents is captured by a graph structure. Such a game will be referred to as distributed aggregate game (DAG) on graphs, or simply, DAG, throughout the paper.

Existing Nash equilibrium solutions to DAGs, however, assume that all agents are fully trustworthy for cooperative tasks or, in the worst-case scenario, are selfish agents with no intent to intentionally harm the network. Nevertheless, information exchange on a communication graph in DAGs makes it vulnerable to malicious cyber-physical attacks and the need to believe that agents will behave consistently exposes the network to threats associated with cyber-physical attacks. In the case of a malicious attack, in contrast to selfish agents with no intent to intentionally harm the system, compromised agents (i.e., agents that are directly attacked) seek to intentionally maximize the damage inflicted on the network at all cost. Therefore, a thorough analysis of the outcome of a DAG in the presence of malicious agents is needed and this paper aims to take the first step toward that objective. In the paper, we focus on the role of the attacker and show that it can (1) compromise the Nash equilibrium solution through a malicious attack on only one agent and significantly degrade the overall performance of the network, and (2) make the network never reach a Nash equilibrium solution and thus lead to a non-emergent behavior significantly affecting the agents' interactions.

The rest of the paper is organized as follows. Section 2 introduces the basics of graph theory and DAG on graphs. Vulnerability of Nash equilibrium to the malicious behavior is discussed in Sect. 3. Simulation results and conclusions are provided in Sects. 4 and 5, respectively.

2 Preliminaries

This section introduces some basic concepts of graph theory and formulates the distributed aggregative games (DAGs) problem.

2.1 Graph Theory

A directed graph (digraph) is a pair $\mathcal{G} = (\mathcal{V}_{\mathcal{G}}, \mathcal{E}_{\mathcal{G}})$ where $\mathcal{V}_{\mathcal{G}} = \{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ is a set of N nodes and $\mathcal{E}_{\mathcal{G}}$ is a set of edges. A typical element of $\mathcal{E}_{\mathcal{G}}$ is denoted (α_i, α_j), which is viewed as an edge connecting α_i to α_j. The corresponding adjacency matrix is denoted by $E = [a_{ij}]$ with weights $a_{ij} > 0$ if $(\alpha_j, \alpha_i) \in \mathcal{E}_{\mathcal{G}}$, and $a_{ij} = 0$ if $(\alpha_j, \alpha_i) \notin \mathcal{E}_{\mathcal{G}}$ and $a_{ii} = 0$ for all $i = 1, 2, \ldots, N$. The in-degree of node α_i is $d_i(\alpha_i) = \sum_{j=1}^{N} a_{ij}$. The diagonal in-degree matrix D is defined as $D = \text{diag}\{d_i(\alpha_i)\}$. The graph Laplacian matrix is defined as $L = D - E$. Graph $\mathcal{G}$ is strongly connected if α_i and α_j are connected for all distinct nodes $\alpha_i, \alpha_j \in \mathcal{V}_{\mathcal{G}}$. A graph is undirected if there is a directed path from α_i to α_j, then there is a directed path from α_j to α_i.

2.2 Aggregative Games

An aggregative game is modeled as a non-cooperative game being played among a set of agents $\mathcal{N} = \{1, \ldots, N\}$. Agent i takes action u_i to minimize its own objective function, which is dependent on the aggregate value (e.g., summation or average) of all agents.

The aggregate value (sum) of all agents is

$$\bar{u} = \sum_{j=1}^{N} u_j \tag{1}$$

Defining

$$\bar{u}_{-i} = \sum_{j=1, j \neq i}^{N} u_j \tag{2}$$

gives

$$\bar{u} = u_i + \bar{u}_{-i} \tag{3}$$

Then, the objective of agent i is given by [19]

$$\begin{aligned} &\text{minimize} \;\; J_i(u_i, \bar{u}) \\ &\text{subject to } u_{l_i} \leq u_i \leq u_{u_i} \end{aligned} \tag{4}$$

where J_i is the cost function of agent i and u_{l_i}, u_{u_i} are allowable decision bounds for agent i. One example that fits in this framework is demand side management in the level of consumers for which the cost function of agent i is given as [20]

$$J_i(u_i, \bar{u}) = d_i(u_i - u_{d_i})^2 + l(\bar{u})\, u_i \tag{5}$$

where the aggregate value $\bar{u}$ is the sum of the power consumption of all agents, and u_{d_i} is the nominal energy schedule required to provide the desired level of comfort for the consumer. Moreover, $l(\bar{u})$ is an increasing price function as a function of the aggregate value of power consumption. The first term in this cost function models the curtailment cost that each agent encounters for deviating from its state of comfort (the selfish objective) and the second term models the cost encounters for deviating from the optimal group behavior (the aggregate group objective).

The most common solution concept for an aggregative game is the Nash equilibrium solution. Letting the aggregate decision to be the sum value, the goal of the dynamic aggregative game is to assure that the result of minimization is Nash equilibrium, defined as follows [21].

Definition 1. *(Nash equilibrium:) An N-tuple of policies* $\{u_1^*, \ldots, u_N^*\}$ *is said to form a Nash equilibrium for an N-agent games if*

$$J_i(u_i^*, \frac{1}{N}u_i^* + \frac{1}{N}\bar{u}_{-i}^*) \leq J_i(u_i, \frac{1}{N}u_i + \frac{1}{N}\bar{u}_{-i}^*), \qquad \forall u_i, \;\; i = 1, \ldots, N \tag{6}$$

and the N-tuple $\{J_1^*, \ldots, J_N^*\}$ *denotes the Nash equilibrium outcome of the N-agent games.*

In most of the existing solutions to aggregative games, a central coordinator receives the decision variable of all the agents, calculates the aggregative decision $\bar{u}$, and broadcasts it to all agents. However, to avoid massive communication requirement and provide scalability, decision algorithms need to be distributed in the sense that each agent should take its decision using local information of its own state and its neighbors' states. In [17,18], a distributed method is presented to estimate the aggregate decision and consequently find the Nash equilibrium. Agents communicate over a communication network specified by an undirected graph to estimate the aggregate decision. The aggregate decision can be found in a distributed fashion so that each agent exchanges its aggregate estimate with its own neighbors on the graph to achieve consensus on the aggregate decision.

Let U_i be the estimation of the aggregate decision for agent i. For the cost function (5), a distributed protocol can be designed as follows for agent i based on its own decision variable u_i and its estimate of the aggregate value [22]

$$\dot{U}_i = -U_i - \sum_{j=1}^{N} a_{ij}\left(U_i - U_j\right) - \sum_{j=1}^{N} a_{ij}\left(w_i - w_j\right) + N u_i \tag{7a}$$

$$\dot{w}_i = \sum_{j=1}^{N} a_{ij}\left(U_i - U_j\right) \tag{7b}$$

$$\dot{u}_i = -\alpha_i(2d_i(u_i - u_{d_i}) + l_i(U_i) + u_i\frac{\partial l_i(U_i)}{\partial U_i}) \tag{7c}$$

where α_i is a fixed positive parameter and w_i is an intermediate variable.

Remark 1. Note that the cost function (5) only shows up in (7c) and our following analysis is not limited to this type of cost function. In fact, as shown later, (7a), which is used to estimate the aggregate value, is independent of the cost function and can be adversely affected by the attacks, and consequently affect the decision making done in (7b). Moreover, under some conditions on the cost function, the existence of the Nash equilibrium of the aggregative game is guaranteed (See Assumption 1 in [19]).

Theorem 1. *Consider N agents with cost function defined in (5). Let their actions be updated based on (7a), (7b), (7c). Then, $U_i \rightarrow \sum_{i=1}^{N} u_i$ and the agents reach a Nash equilibrium.*

Proof. See [22].

Remark 2. Distributed consensus algorithms over graphs, however, are vulnerable to cyber-physical attacks [23–32]. If agents are not empowered with built-in resilient functionalities, sophisticated attacks can be intentionally designed by an intruder to maximize the damage to the network and prevent the multi-agent system from accomplishing a desired emergent behavior. The attacker can leverage a single compromise into becoming a network-wide compromise; intact agents are not immune from disruption by attacks on compromised agents.

3 Vulnerability of Nash Equilibrium of DAG to Malicious Behavior

In this section, we analyze the effects of malicious behavior on the outcome of the aggregative games.

Before proceeding, we need the following definitions.

Definition 2. *Agent i is called intact agent if it is not directly under attack.*

Definition 3. *Agent i is called compromised agent if it is directly under attack and broadcasts disrupted information about its estimation of the aggregate value, i.e. U_i, to its neighbors.*

Definition 4. *Agent i is called selfish agent if it broadcasts the correct information about the estimation of the aggregate value, U_i, to its neighbors, but does not update its action u_i and choose it guided by its own selfish objective.*

Definition 5. *The matrices $\bar{L} \in \mathcal{R}^{N-1 \times N-1}$ and $\underline{L} \in \mathcal{R}^{N-M \times N-M}$ are subgraphs of Laplacian matrix $L \in \mathcal{R}^{N \times N}$ obtained by removing one node and M nodes, respectively.*

Definition 6. *The diagonal matrix $G = diag[g_1, \ldots, g_{N-1}]$ is called pinning matrix and $g_i \neq 0$ if there is a edge between node i (intact node) and node N (compromised node), otherwise $g_i = 0$.*

Remark 3. Note that a selfish agent only cares about its own selfish objective and does not care about the global group objective. However, in contrast to a compromised agent, it has no intention to harm the network.

Theorem 2. *Let*

$$Z_i = \sum_{j=1}^{N} a_{ij} \left(w_i - w_j\right) \tag{8}$$

with w_i defined in (7a), (7b), (7c). Then $\sum\limits_{i=1}^{N} Z_i = 0$, and consequently, one has $\sum\limits_{i=1}^{N} U_i \rightarrow N \sum\limits_{i=1}^{N} u_i$ for (7a), (7b), (7c).

Proof. Since the graph is undirected, if agent i communicates w_i to agent j (and consequently Z_i has $w_i - w_j$ component,) agent j communicates w_j to agent i (and consequently Z_j has $w_j - w_i$ component). Therefore, for every $w_i - w_j$, there is a corresponding $w_j - w_i$ that cancels it out in $\sum\limits_{i=1}^{N} Z_i$ and consequently $\sum\limits_{i=1}^{N} Z_i = 0$. Now, in the steady state $\dot{U}_i \rightarrow 0$ and $U_i = U_j$ $\forall j$. Thus, for (7a), one has

$$U_i \rightarrow -\sum_{j=1}^{N} a_{ij} \left(w_i - w_j\right) + N u_i \tag{9}$$

Using the fact that $\sum\limits_{i=1}^{N} Z_i = 0$, this results in

$$\sum_{i=1}^{N} U_i \rightarrow N \sum_{i=1}^{N} u_i \tag{10}$$

This completes the proof.

Condition (10) is a necessary condition under which the agents reach consensus on summation, i.e. $U_i \rightarrow \sum\limits_{i=1}^{N} u_i$. In the following, it is shown that the attacker can cause violation of this condition and consequently results in a wrong consensus or no consensus at all, and thus adversely affects the effectiveness of the games solution. It is also shown that if one agent in the graph is a compromised agent and does not update its estimation about the aggregate value, the compromised agent acts as a leader and the aggregate value of all other agents reach consensus on its corrupted and wrong value, regardless of agents' actions. If more than one agent are compromised, then it is shown that agents do not reach consensus on a single value, but different values within the convex hull of compromised agents. Finally, it is also shown that this single compromised agent compromises the Nash solution and can either harm the agents' comfort level by consuming less than they are allowed to or significantly increase the price by consuming more than they have to for the case of demand response management.

Lemma 1. *Suppose $A \in \mathcal{R}^{n\times n}$ satisfies $A + A^T < 0$ and $B \in \mathcal{R}^{n\times n}$ is invertible. Then, the matrix*

$$H = \begin{bmatrix} A & B^T \\ -B & \mathbf{0} \end{bmatrix} \tag{11}$$

is Hurwitz.

Proof. See [33].

Theorem 3. *Suppose that agent N is a compromised agent and does not update its estimation about the aggregate value, i.e. $U_N(t) = \mathrm{U}$. Then, the aggregate values in (7a), (7b), (7c) converge to* U*, regardless of the actions of all the agents, i.e, $u_i \;\; \forall i = 1, \ldots, N$.*

Proof. The distributed protocol (7a), (7b), (7c) in the presence of one compromised agent can be rewritten as

$$\begin{aligned}\dot{U}_i =& -U_i - (\sum_{j=1}^{N-1} a_{ij}\,(U_i - U_j) + g_i\,(U_i - \mathrm{U})) - \\ & (\sum_{j=1}^{N-1} a_{ij}\,(w_i - w_j) + g_i\,(w_i - \mathrm{w})) + N u_i \end{aligned} \tag{12a}$$

$$\dot{w}_i = \sum_{j=1}^{N-1} a_{ij}\,(U_i - U_j) + g_i\,(U_i - \mathrm{U}) \tag{12b}$$

$$\dot{u}_i = -\alpha_i(2d_i(u_i - u_{d_i}) + l_i(U_i) + u_i \frac{\partial l_i(U_i)}{\partial U_i}) \tag{12c}$$

where g_i is defined in Definition 6, and U and w are the constant values broadcasted by the compromised agent.

Define error quantities as $\bar{U}_i(t) := U_i(t) - \mathrm{U}$ and $\bar{W}_i(t) := w_i(t) - \mathrm{w}$. The error dynamics in compact form are given as

$$\begin{bmatrix} \dot{\bar{U}}(t) \\ \dot{\bar{W}}(t) \end{bmatrix} = \begin{bmatrix} -\mathrm{I} - (\bar{L} + G) & -(\bar{L} + G) \\ \bar{L} + G & \mathbf{0} \end{bmatrix} \begin{bmatrix} \bar{U}(t) \\ \bar{W}(t) \end{bmatrix} + \begin{bmatrix} -\mathbf{1}\mathrm{U} + Nu(t) \\ \mathbf{0} \end{bmatrix} \tag{13}$$

where $\bar{U} = [\bar{U}_1, \ldots, \bar{U}_{N-1}]^T$, $\bar{W} = [\bar{W}_1, \ldots, \bar{W}_{N-1}]^T$, and $u = [u_1, \ldots, u_{N-1}]^T$.

Define

$$K(t) = -\mathbf{1}\mathrm{U} + Nu(t) \tag{14}$$

The transfer function from $\bar{U}(t)$ to $K(t)$ is given as

$$T(s) = \frac{\bar{U}(s)}{K(s)} = s[s^2\mathrm{I} + (\mathrm{I} + (\bar{L} + G))s + (\bar{L} + G)^2]^{-1} \tag{15}$$

Note that $\bar{L} + G$ is positive definite and thus can be written as $\bar{L} + G = Q\mathit{\Lambda} Q^T$ with eigenbasis $Q = [q_1, \ldots, q_{N-1}]$ corresponding to real eigenvalues $\mathit{\Lambda} = diag[\lambda_1, \ldots, \lambda_{N-1}]$ with $\lambda_j > 0 \; \forall j = 1, \ldots, N-1$. Using this fact, the transfer function (15) can be rewritten as

$$\begin{aligned} T(s) = \frac{\bar{U}(s)}{K(s)} =& s[Q^T(s^2\mathrm{I} + (\mathrm{I} + \Lambda)\mathrm{s} + \Lambda^2)\mathrm{Q}]^{-1} \\ =& \sum_{j=1}^{N-1} \frac{s}{s^2\mathrm{I} + (\mathrm{I} + \mathrm{\lambda_j})\mathrm{s} + \mathrm{\lambda_j}^2} {q_j}^T q_j \end{aligned} \tag{16}$$

Using (16), $\bar{U}(s)$ becomes

$$\bar{U}(s) = T(s)K(s) = (\sum_{j=1}^{N-1} \frac{s}{s^2\mathrm{I} + (\mathrm{I} + \mathrm{\lambda_j})\mathrm{s} + \mathrm{\lambda_j}^2} {q_j}^T q_j) \frac{-\mathbf{1}\mathrm{U} + Nu}{s} \tag{17}$$

Using Lemma 1 for (13), which shows that $T(s)$ is stable, and the Final Value Theorem, one has

$$\lim_{t \to \infty} \bar{U}(t) = \lim_{s \to 0} s\bar{U}(s) = \lim_{s \to 0} sT(s)K(s) = 0, \tag{18}$$

which results in

$$U_i(t) \to \mathrm{U} \tag{19}$$

This completes the proof.

Remark 4. One might argue that if a compromised agent does not update its estimate of the aggregate value, it can be identified as a frozen agent and ignored by its neighbors. However, a compromised agent can for example change its update law to $\dot{x}_N = b\,exp(-a\,t)$, $x_N(0) = \mathrm{U}$. It can be shown that, in this case, agents' estimates of the aggregate value will eventually converge to $\mathrm{U} + b$, while the compromised agent is not frozen.

Theorem 4. *Let node N be a compromised agent. Then, on convergence, one has $\sum_{i=1}^{N} U_i \not\to N \sum_{i=1}^{N} u_i$. Therefore, $U_i \to \mathrm{U} \neq \sum_{i=1}^{N} u_i$.*

Proof. The equivalence of Z_i that shows up in (7a) and defined in Theorem 1 in the presence of one compromised node is

$$\sum_{j=1}^{N-1} a_{ij}\,(w_i - w_j) + g_i(w_i - \mathrm{w}) \tag{20}$$

where w is the value of the internal estimation variable of the compromised node. It was shown in Theorem 2 that $\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}\,(w_i - w_j) = 0$. Letting agent N to be the compromised agent and broadcasting w, and ignoring the information it receives from its neighbors, one has

$$\sum_{i=1}^{N-1}(\sum_{j=1}^{N-1} a_{ij}\,(w_i - w_j) + g_i(w_i - \mathrm{w})) = \sum_{i=1}^{N-1} g_i(w_i - \mathrm{w}) \neq 0 \tag{21}$$

On the right-hand side of (21), the information flowed from neighbors of the compromised agent is ignored since it does not listen to its neighbors.

At the steady state, (12a), (12b), (12c) satisfies

$$\sum_{i=1}^{N-1} U_i = -\sum_{i=1}^{N-1}(\sum_{j=1}^{N-1} a_{ij}(w_i - w_j) + g_i(w_i - \mathrm{w})) + N\sum_{i=1}^{N-1} u_i \tag{22}$$

Considering (21) in (22) and adding $U_N = \mathrm{U}$ to both sides of (22) result in

$$\sum_{i=1}^{N} U_i = -\sum_{i=1}^{N-1} g_i(w_i - \mathrm{w}) + N\sum_{i=1}^{N-1} u_i + \mathrm{U} \tag{23}$$

Since in the steady state, $u_N \neq \frac{1}{N}(-\sum_{i=1}^{N-1} g_i(w_i - \mathrm{w}) + \mathrm{U})$, then (23) results in $\sum_{i=1}^{N} U_i \nrightarrow N\sum_{i=1}^{N} u_i$. On the other hand, $\sum_{i=1}^{N} U_i = N\sum_{i=1}^{N} u_i$ is a necessary condition for $U_i = \sum_{i=1}^{N} u_i$. Therefore, $U_i \nrightarrow \sum_{i=1}^{N} u_i$ and this completes the proof.

Theorem 5. *Suppose that more than one agent in the network are compromised and do not update their estimation about the aggregate value. Then, the aggregate values in (7a) converge to a convex hull spanned by the value of the compromised agents regardless of the actions of other agents.*

Proof. The distributed protocol (7a), (7b), (7c) in the presence of multiple compromised agents can be rewritten as

$$\dot{U}_i = -U_i - (\sum_{j=1}^{N-M} a_{ij}\,(U_i - U_j) + \sum_{k=1}^{M} g_i^k\,(U_i - \mathrm{U}_0^k)) -$$

$$(\sum_{j=1}^{N-M} a_{ij}\,(w_i - w_j) + \sum_{k=1}^{M} g_i^k\,(w_i - \mathrm{w}_0^k)) + N u_i \tag{24a}$$

$$\dot{w}_i = \sum_{j=1}^{N-M} a_{ij}\,(U_i - U_j) + \sum_{k=1}^{M} g_i^k\,(U_i - \mathrm{U}_0^k) \tag{24b}$$

$$\dot{u}_i = -\alpha_i(2d_i(u_i - u_{d_i}) + l_i(U_i) + u_i\frac{\partial l_i(U_i)}{\partial U_i}) \tag{24c}$$

where M is the number of compromised agents, U_0^k, $k = 1, \ldots, M$ is the constant values broadcasted by the compromised agents, and $g_i^k \neq 0$ if there is a direct edge between node i and compromised node k, and $g_i^k = 0$ otherwise.

The distributed protocol (24a) and (24b) in compact form are written as

$$\dot{U} = -U - \sum_{k=1}^{M} H_k\,(U - \mathbf{1}_{N-M} \otimes \mathrm{U}_0^k) -$$

$$\sum_{k=1}^{M} H_k\,(w - \mathbf{1}_{N-M} \otimes \mathrm{w}_0^k) + N u \tag{25a}$$

$$\dot{w} = \sum_{k=1}^{M} H_k\,(U - \mathbf{1}_{N-M} \otimes \mathrm{U}_0^k) \tag{25b}$$

where

$$H_k = \frac{\underline{\mathrm{L}}}{M} + G_k$$

and

$$G_k = \begin{bmatrix} g_1^k & 0 & 0 & 0 \\ 0 & g_2^k & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & g_{N-M}^k \end{bmatrix}$$

It is shown in [34] that the convex hull spanned by leaders is given as

$$\mathrm{C} = \sum_{k=1}^{M} \left[\left[\left(\sum_{r=1}^{M} H_r \right)^{-1} H_k \, \mathbf{1}_{N-M} \right] \otimes \mathrm{U}_0^k \right] \tag{26}$$

Define error quantities as $\underline{\mathrm{U}}_i := U_i - \mathrm{C}$ and $\underline{\mathrm{W}}_i := w_i - \bar{\mathrm{w}}$. The error dynamics in compact form are given as

$$\begin{bmatrix} \dot{\underline{\mathrm{U}}}(t) \\ \dot{\underline{\mathrm{W}}}(t) \end{bmatrix} = \begin{bmatrix} -\mathrm{I} - H & -H \\ H & \mathbf{0} \end{bmatrix} \begin{bmatrix} \underline{\mathrm{U}}(t) \\ \underline{\mathrm{W}}(t) \end{bmatrix} + \begin{bmatrix} -\mathbf{1}\mathrm{C} + Nu(t) \\ \mathbf{0} \end{bmatrix} \tag{27}$$

where $\underline{\mathrm{U}}(t) = [\underline{\mathrm{U}}_1(t), \ldots, \underline{\mathrm{U}}_{N-M}(t)]^T$, $\underline{\mathrm{W}}(t) = [\underline{\mathrm{W}}_1(t), \ldots, \underline{\mathrm{W}}_{N-M}(t)]^T$, and $H = \sum\limits_{k=1}^{M} H_k$.

Introduce

$$\underline{\mathrm{K}}(t) := -\mathbf{1}\mathrm{C} + Nu \tag{28}$$

The transfer function from $\underline{\mathrm{U}}(t)$ to $\underline{\mathrm{K}}(t)$ is given by

$$\underline{\mathrm{T}}(s) = \frac{\underline{\mathrm{U}}(s)}{\underline{\mathrm{K}}(s)} = s[s^2\mathrm{I} + (\mathrm{I} + H)s + H^2]^{-1} \tag{29}$$

Similar to Theorem 3, the transfer function (29) can be rewritten as

$$\underline{\mathrm{T}}(s) = \sum_{j=1}^{N-M} \frac{s}{s^2\mathrm{I} + (\mathrm{I} + \eta_\mathrm{j})\mathrm{s} + {\eta_\mathrm{j}}^2} {p_j}^T p_j \tag{30}$$

where η_j, $j = 1, \ldots, N-M$ are the eigenvalues of matrix H, and p_j are the corresponding eigenvectors.

Using (15), $\underline{\mathrm{U}}(s)$ is defined as

$$\underline{\mathrm{U}}(s) = \underline{\mathrm{T}}(s)\underline{\mathrm{K}}(s) = (\sum_{j=1}^{N-M} \frac{s}{s^2\mathrm{I} + (\mathrm{I} + \eta_\mathrm{j})\mathrm{s} + {\eta_\mathrm{j}}^2} {p_j}^T p_j) \frac{-\mathbf{1}\mathrm{C} + Nu}{s} \tag{31}$$

Using Lemma 1 and the Final Value Theorem, one has

$$\lim_{t\to\infty} \underline{\mathrm{U}}(t) = \lim_{s\to 0} s\underline{\mathrm{U}}(s) = \lim_{s\to 0} s\underline{\mathrm{T}}(s)\underline{\mathrm{K}}(s) = 0, \tag{32}$$

which results in

$$U_i \rightarrow \mathrm{C} \tag{33}$$

This completes the proof.

Remark 5. The compromised agents might be able to collude and communicate only with each other to reach consensus on a compromised value. This way, compromised agents will update their values to avoid being identified as frozen agents and the estimation of all agents will reach consensus on the consensus value of compromised agents.

Theorem 6. *Consider the aggregative game with cost function (5) and update law (7a), (7b), (7c), with the setting of demand side management. Let $u^* = (u_1^*, u_2^*, \ldots, u_N^*)$ be the Nash equilibrium solution to the game, when there is no compromised agent. Assume now that agent N does not update its value and broadcast $\mathrm{U} \neq U^* = \sum_{i=1}^{N} u_i^*$. Then, the agents reach a compromised Nash solution, and*

(1) if $\mathrm{U} >> U^*$, the level of comfort of the agents will be adversely and significantly harmed.
(2) if $\mathrm{U} << U^*$, the agents will be misled to increase their consumption and the price will adversely be increased.

Proof

(1) It was shown in Theorem 4 that U_i $\forall i = 1, \ldots, N-1$ converge to U, regardless of agents' actions. Therefore, in convergence, (7a)–(7c) actually minimize

$$J_i = d_i(u_i - u_{d_i})^2 + l(\mathrm{U})\, \mathrm{u_i} \tag{34}$$

Since $l(\mathrm{U})$ is now independent of actions of other agents, they reach eventually their best response, which is decoupled from actions of other agents and is affected only by the action of the compromised agent. In the most extreme case, if $\mathrm{U} >> U^*$, $l(\mathrm{U}) = \mathrm{l_{max}}$ for all agents and then, (34) becomes

$$J_i = d_i(u_i - u_{d_i})^2 + l_{max}\, u_i \tag{35}$$

Therefore, agents will misleadingly think that the overall consumption and thus the price are high and take actions to minimize it by minimizing their comfort level.

(2) The same as (1), $l(\mathrm{U})$ is independent of actions of agents and is only controlled by the compromised agent. Agents will misleadingly think that the overall consumption and consequently the price are low and thus move toward maximizing their comfort levels. In the most extreme case,

$$J_i = d_i(u_i - u_{d_i})^2 + l_{min}\, u_i \tag{36}$$

This will significantly increase their price.

Remark 6. If there is more than one compromised agent, as shown in Theorem 5, agents do not reach consensus on the aggregate value and their estimations on the aggregate value converge to different values within the convex hull of compromised agents' values. In this case, the same as Theorem 5, one can show that the actions of agents are decoupled and $l(\bar{u})$ is only affected by compromised agents. In fact, agent i on convergence minimizes

$$J_i = d_i(u_i - u_{d_i})^2 + l(C_i)\, u_i \tag{37}$$

where $C_i \in \mathrm{C}$ and $l(C_i)$ only depends on the compromised agents, but it is different for all agents. Therefore, the attackers can adversely affect comfort level of some of the agents and the price of some other agents at the same time.

Remark 7. Note that in the presence of an attack, if agent i cares mostly about the price, i.e. $d_i << 1$ in (5), then if U $>> U^*$, it will choose its minimum allowed action, which minimizes its comfort level. On the other hand, if agent i is selfish, i.e. $d_i >> 1$, it will not be affected by the attack. Moreover, if the compromised agent broadcasts a time varying signal such as a sinusoidal, agents will never reach an emergent behavior and their actions will fluctuate and not reach a steady state.

4 Simulation Results

In this section, we consider 5 agents that are communicating with each other through an undirected graph shown in Fig. 1. Each agent optimizes the cost function (5). Figure 2 shows the estimation of the aggregate value for all agents in the absence of compromised agents in the network. Figure 3 shows the actions of all agents in the absence of an adversary. It can be seen that from these results that all agents estimate the same aggregate value, and this aggregate value in Fig. 2 is the actual summation of the actions of agents in Fig. 3.

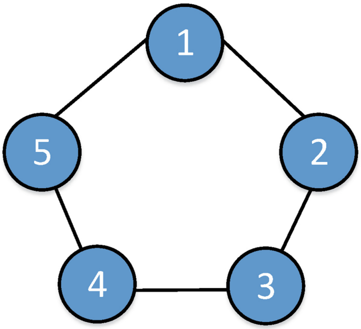

Fig. 1. Communication network between agents

Now, we consider the cases with compromised or selfish agents.

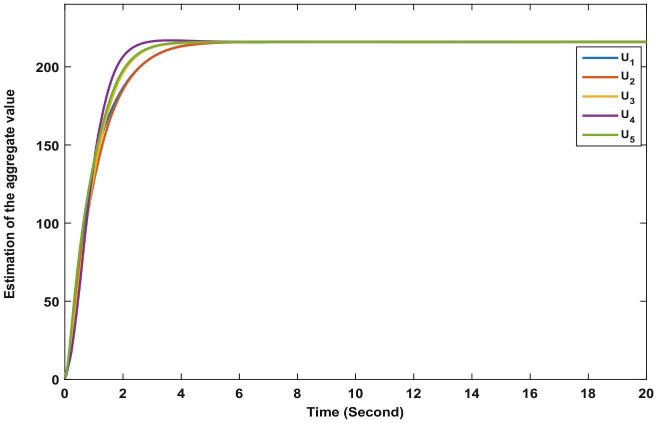

Fig. 2. Estimation of the aggregate value by all agents in the absence of an adversary in the environment

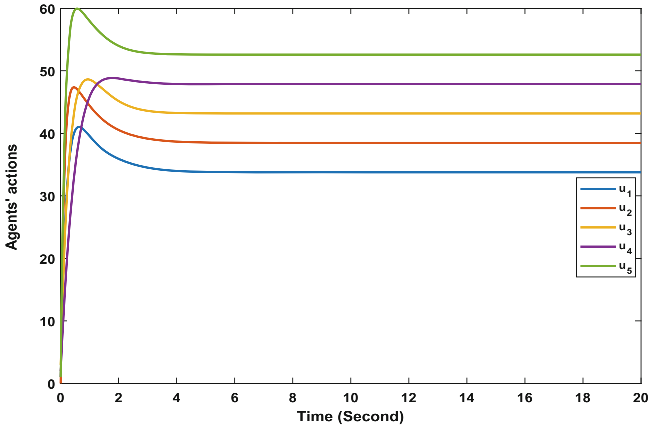

Fig. 3. The actions of all agents in the absence of an adversary

4.1 Presence of One Compromised Agent in the Network

In the scenario considered here, we assume that Agent 4 is a compromised agent and does not listen to its neighbors about the aggregate value. This agent always sends a fixed value 500 to its neighbors. Figure 4 shows that the estimates of all agents of the aggregate value converge to the value of the compromised agent, regardless of their actions. The actions of all agents in the presence of the compromised agent are shown in Fig. 5. These figures corroborate the results of Theorems 3 and 4. It is obvious that, compared to Figs. 2 and 3, the actions of agents are significantly affected by the compromised agent and their summation is not equal to the estimated aggregate value.

4.2 Presence of Multiple Compromised Agents in the Network

Here we assume that Agents 3 and 4 are compromised agents. Figures 6 and 7 show that the estimate of the aggregate value for all agents converge to different values within the convex hull spanned by the compromised agents. It can be seen that, compared to Fig. 3, the actions of agents are affected by the compromised agents.

4.3 Presence of a Selfish Agent in the Network

In this scenario, we assume that Agent 3 just cares about its selfish comfort objective and keeps its power consumption at 30 for all the time. Figures 8 and

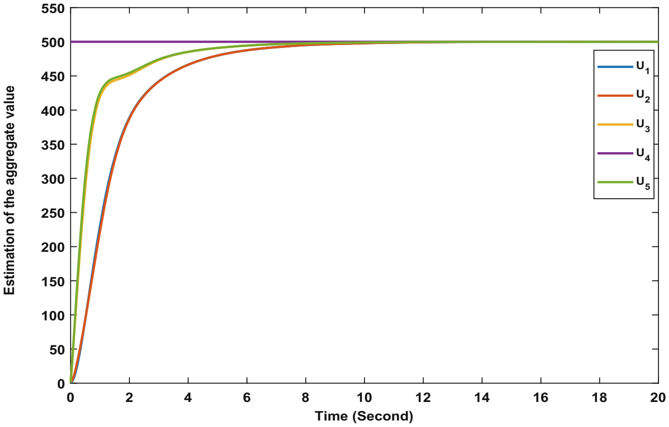

Fig. 4. Estimation of aggregate value by all agents in the presence of one compromised agent

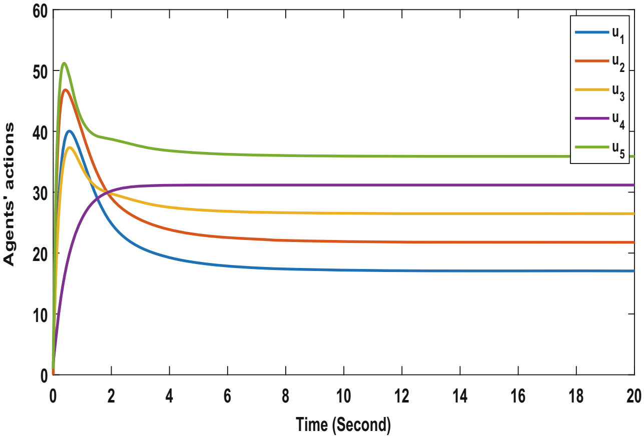

Fig. 5. The actions of all agents in the presence of one compromised agent

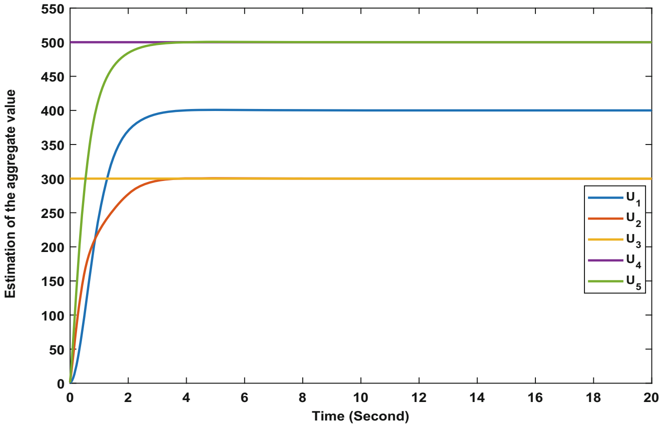

Fig. 6. Estimation of the aggregate value by all agents in the presence of multiple compromised agents

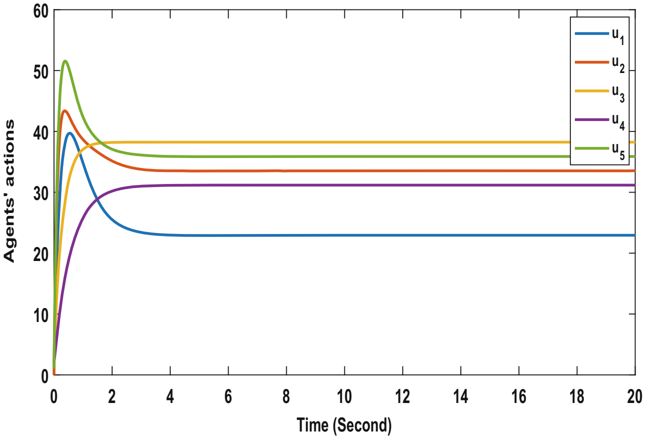

Fig. 7. The actions of all agents in the presence of multiple compromised agents

9 show the estimates of the aggregate value and all agents' actions, respectively. One can see that the estimates of the aggregate values converge to summation of the actions of all agents and, compared to Fig. 3, the actions of the agents except the selfish one do not change.

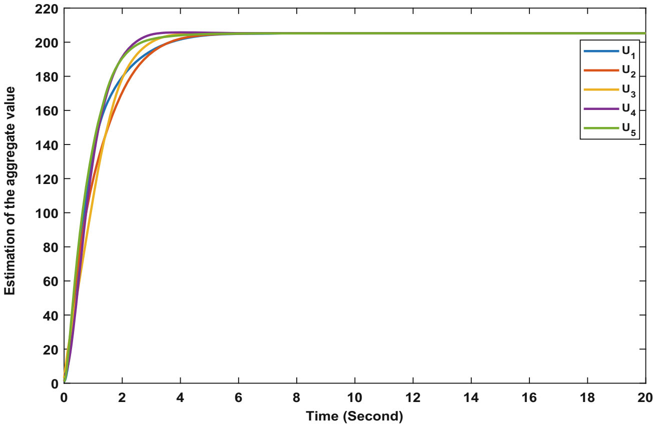

Fig. 8. Estimation of the aggregate value by all agents in the presence of a selfish agent

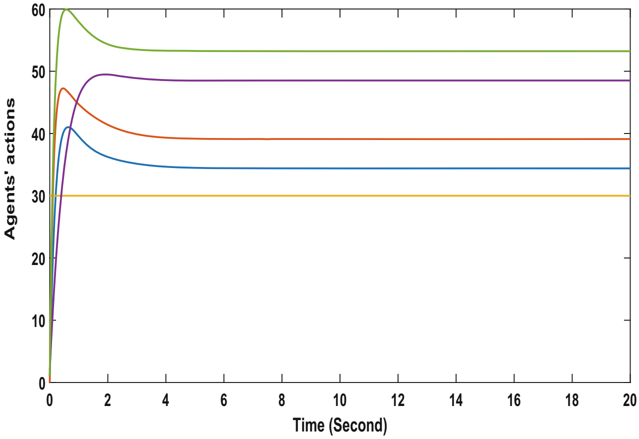

Fig. 9. The actions of all agents in the presence of a selfish agent

5 Conclusion

We have analyzed, in this paper, the adverse effects of malicious behavior on the Nash solution of distributed aggregative games (DAGs) on graphs. We have shown that the game solution can reach a consensus value that does not depend on agents' actions, and actually depends only on the broadcast value of the compromised agent. This study intensifies the urgency of empowering the agents with built-in resilient functionalities to decrease the damage to the network in the presence of unexpected behaviour. The next step would be to design resilient protocols to assure that all agents in the network operate in an acceptable level of functionality in the presence of cyber attacks.

References

1. Cornes, R., Hartley, R.: Fully aggregative games. Econ. Lett. **116**(3), 631–633 (2012)
2. Huang, M., Caines, P.E., Malhame, R.P.: Large-population cost-coupled LQG problems with nonuniform agents: Individual-mass behavior and decentralized Nash equilibria. IEEE Trans. Autom. Control **52**, 1560–1571 (2007)
3. Lasry, J.-M., Lions, P.-L.: Mean field games. Jpn. J. Math. **2**, 229–260 (2007)
4. Bauso, D., Pesenti, R.: Mean field linear quadratic games with set up costs. Dyn. Games Appl. **3**, 89–104 (2013)
5. Grammatico, S., Parise, F., Colombino, M., Lygeros, J.: Decentralized convergence to Nash equilibria in constrained deterministic mean field control. IEEE Trans. Autom. Control **61**, 3315–3329 (2016)
6. Bauso, D., Tembine, H., Başar, T.: Robust mean field games. Dyn. Games Appl. **6**, 277–303 (2016)
7. Moon, J., Başar, T.: Linear quadratic risk-sensitive and robust mean field games. IEEE Trans. Autom. Control **62**, 1062–1077 (2017)
8. Mohsenian-Rad, A.H., Wong, V.W.S., Jatskevich, J., Schober, R., Leon-Garcia, A.: Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. IEEE Trans. Smart Grid **1**, 320–331 (2010)
9. Bagagiolo, F., Bauso, D.: Mean-field games and dynamic demand management in power grids. Dyn. Games Appl. **4**, 155–176 (2014)
10. Chen, H., Li, Y., Louie, R.H.Y., Vucetic, B.: Autonomous demand side management based on energy consumption scheduling and instantaneous load billing: an aggregative game approach. IEEE Trans. Smart Grid **5**, 1744–1754 (2014)
11. Ma, Z., Callaway, D.S., Hiskens, I.A.: Decentralized charging control of large populations of plug-in electric vehicles. IEEE Trans. Control Syst. Technol. **21**, 67–78 (2013)
12. Parise, F., Colombino, M., Grammatico, S., Lygeros, J.: Mean field constrained charging policy for large populations of plug-in electric vehicles. In: 53rd IEEE Conference on Decision and Control, pp. 5101–5106, December 2014
13. Alpcan, T., Başar, T.: Distributed algorithms for Nash equilibria of flow control games, pp. 473–498. Birkhäuser, Boston (2005)
14. Başar, T.: Control and game-theoretic tools for communication networks. Appl. Comput. Math. **6**(2), 104–125 (2007)
15. Barrera, J., Garcia, A.: Dynamic incentives for congestion control. IEEE Trans. Autom. Control **60**, 299–310 (2015)
16. Kizilkale, A.C., Mannor, S., Caines, P.E.: Large scale real-time bidding in the smart grid: a mean field framework. In: 2012 IEEE 51st IEEE Conference on Decision and Control, CDC, pp. 3680–3687, December 2012
17. Koshal, J., Nedi, A., Shanbhag, U.V.: A gossip algorithm for aggregative games on graphs. In: 2012 IEEE 51st IEEE Conference on Decision and Control, CDC, pp. 4840–4845, December 2012
18. Swenson, B., Kar, S., Xavier, J.: Distributed learning in large-scale multi-agent games: a modified fictitious play approach. In: 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers, ASILOMAR, pp. 1490–1495, November 2012
19. Koshal, J., Nedić, A., Shanbhag, U.V.: Distributed algorithms for aggregative games on graphs. Oper. Res. **64**(3), 680–704 (2016)

20. Parise, F., Gentile, B., Grammatico, S., Lygeros, J.: Network aggregative games: distributed convergence to Nash equilibria. In: 2015 54th IEEE Conference on Decision and Control, CDC, pp. 2295–2300, December 2015
21. Başar, T., Olsder, G.J.: Dynamic Noncooperative Game Theory. SIAM, Philadelphia (1999)
22. Ye, M., Hu, G.: Game design and analysis for price-based demand response: an aggregate game approach. IEEE Trans. Cybern. **47**, 720–730 (2017)
23. Teixeira, A., Sandberg, H., Johansson, K.H.: Networked control systems under cyber attacks with applications to power networks. In: Proceedings of the 2010 American Control Conference, pp. 3690–3696, June 2010
24. Sundaram, S., Hadjicostis, C.N.: Distributed function calculation via linear iterative strategies in the presence of malicious agents. IEEE Trans. Autom. Control **56**, 1495–1508 (2011)
25. Pasqualetti, F., Bicchi, A., Bullo, F.: Consensus computation in unreliable networks: a system theoretic approach. IEEE Trans. Autom. Control **57**, 90–104 (2012)
26. Pasqualetti, F., Drfler, F., Bullo, F.: Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control **58**, 2715–2729 (2013)
27. Zhu, M., Martnez, S.: On the performance analysis of resilient networked control systems under replay attacks. IEEE Trans. Autom. Control **59**, 804–808 (2014)
28. Zhu, Q., Başar, T.: Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Syst. **35**, 46–65 (2015)
29. Mo, Y., Sinopoli, B.: Secure estimation in the presence of integrity attacks. IEEE Trans. Autom. Control **60**, 1145–1151 (2015)
30. Khanafer, A., Baar, T.: Robust distributed averaging: when are potential-theoretic strategies optimal? IEEE Trans. Autom. Control **61**, 1767–1779 (2016)
31. Moghadam, R., Modares, H.: An internal model principle for the attacker in distributed control systems. In: 2017 IEEE 56th Annual Conference on Decision and Control, CDC, pp. 6604–6609, December 2017
32. Kamdem, G., Kamhoua, C., Lu, Y., Shetty, S., Njilla, L.: A Markov game theoritic approach for power grid security. In: 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops, ICDCSW, pp. 139–144, June 2017
33. Freeman, R.A., Yang, P., Lynch, K.M.: Stability and convergence properties of dynamic average consensus estimators. In: Proceedings of the 45th IEEE Conference on Decision and Control, pp. 338–343, December 2006
34. Haghshenas, H., Badamchizadeh, M.A., Baradarannia, M.: Containment control of heterogeneous linear multi-agent systems. Automatica **54**, 210–216 (2015)