2016 American Control Conference (ACC)
Boston Marriott Copley Place
July 6-8, 2016. Boston, MA, USA

Resilient Consensus for Multi-Agent Systems with Quantized Communication

Yiming Wu[1], Xiongxiong He[†,1] and Shuai Liu[2,3]

***Abstract*— In this paper, we investigate the resilient consensus problem for multi-agent systems with quantized communication. We assume that each agent in the network can only exchange quantized information with its neighbors. A novel quantized-data based secure control law with built-in security mechanism is proposed to achieve consensus in the presence of attack agents. It is shown that for a directed network, as long as the number of attack nodes is bounded in each node' neighborhood, the consensus can be achieved with a given sufficient network connectivity. Finally, we offer a numerical example to demonstrate the validity of the derived results.**

I. INTRODUCTION

Distributed consensus over multi-agent networks has become a hot research topic in the systems and control community during the last few years (see [1], [2], [3], [4], [5], [6], [7] and the references therein). The problem is widely encountered in the engineered applications such as robots, traffic congestion control, unmanned air vehicles, formation flight, and microgrids.

As a special case of distributed consensus, resilient consensus algorithms have been studied extensively over the years [8], [9], [10]. A pioneering work on the resilience of consensus networks to misbehaving nodes appears in [11], where the authors consider the case that all the well-behaving nodes in the network reach a common state required by a special leader node, when the communication topology is non-complete. The authors of [12] address the resilience of consensus problem for linear multi-agent networks, and propose three effective algorithms to detect and identify misbehaving nodes. To achieve accurate consensus state, [13] proposes a novel reputation-based secure controller with distributed security mechanisms. In [14] and [15], the authors introduce a novel graph-theoretic property known as r*-robustness*, based on which a consensus control strategy that is resistant to malicious nodes is provided. Later, the authors of [16] extend the above results to the case of second-order systems. Moreover, some other strategies for resilience of consensus algorithms are considered in [17], [18], [19]. The comprehensive survey for recent works on secure consensus can be found in [20] and [21].

This work is supported by National Natural Science Foundation (NNSF) of China under Grants 61473262, 61304045 and 61573220.

[†]Corresponding author.

[1]Yiming Wu and Xiongxiong He are with the College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, P.R. China yimgwu@hotmail.com, hxx@zjut.edu.cn

[2]Shuai Liu is with School of Control Science and Engineering, Shandong University, Jinan 250061, China lius0025@ntu.edu.sg

[3]Shuai Liu is also with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore

In resilient consensus literature, we observe that much work are developed under the assumption that all agents in the network can get exact information from their neighbors. However, for practical distributed multi-agent systems, each agent's computational load and energy storage are limited, and the links between two nodes can be subjected to communication bandwidth constraints. Therefore, consensus problems based on quantized communication become interesting and more meaningful.

In this paper, we would like to develop a resilient consensus algorithm for multi-agent networks with quantized communication. In particular, the system considered in this paper contains two types of agents: loyal agents and attack agents. Each loyal agent will update its value under a given distributed control law. While, the attack agent will not obey the law and purposely affect the loyal agents' updates by transmitting false information to its neighbors. The algorithm is designed based on the local quantized information provided to each agent by its neighbours. It will be proved that when the information-exchange network is satisfied with the given sufficient conditions, a consensus for all the loyal agents can be achieved. A numerical simulation is given to demonstrate the effectiveness of the algorithm.

This paper is organized as follows: Some useful preliminaries in graph theory, logarithmic quantization and Dini derivatives are reviewed in Section II. In Section III, the resilient consensus problem with quantized communication data is formulated and main results are established in Section IV. Then in section V, we illustrate the results via a numerical simulation. Finally, some concluding remarks are made in Section VI.

II. PRELIMINARIES

In this section, some basic notations on algebraic graph theory and features of Dini derivatives and logarithmic quantization are reviewed.

A. Graph theory

A weighted directed graph (or digraph) of order n is defined as $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}, A_\mathcal{G}\}$, where $\mathcal{V}$ is a non-empty set of vertices (or nodes), $\mathcal{E}_\mathcal{G} \subset \mathcal{V} \times \mathcal{V}$ is a set of edges, and $A_\mathcal{G} = [a_{i,j}] \in \mathbb{R}^{n\times n}$ is called the weighted adjacency matrix associated with $\mathcal{G}$. For an edge $(i,j) \in \mathcal{E}_\mathcal{G}$, i is called the parent node whose messages can flow to node j. It is defined by $a_{i,i} = 0, a_{i,j} > 0$ if $(j,i) \in \mathcal{E}_\mathcal{G}$ and $a_{i,j} = 0$ otherwise. Denote $\mathcal{N}_i = \{j \,|j \in \mathcal{V}, (j,i) \in \mathcal{E}_\mathcal{G}\}$ the set of neighbors of i and d_i the number of neighbors of i. A directed path from node i_1 to node i_p is given by a sequence of ordered edges of

the form $(i_1, i_2), (i_2, i_3), ..., (i_{p-1}, i_p)$ with $(i_{j-1}, i_j) \in \mathcal{E}_\mathcal{G}$, $\forall j \in \{2, 3, ..., p\}$. The graph $\mathcal{G}$ is said to have a spanning tree if there is a root node without any parent such that there exists a direct path from this node to the rest of nodes. Given a piecewise constant function $\sigma(t)$, $\mathcal{G}^{\sigma(t)} = \{\mathcal{V}, \mathcal{E}^{\sigma(t)}\}$ denotes a time-varying graph.

Then, we introduce some notions of robustness for a directed graph. The following definition is adopted, with minor changes, from [14].

Definition 2.1: (r-robust graph) Consider a directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$, we say $\mathcal{G}$ is an r-robust graph, where $r \in \mathbb{Z}^+$, if for all possible pairs of nonempty subsets, $\mathcal{V}_1$, $\mathcal{V}_1 \subset \mathcal{V}$, there is at least one node $i \in \mathcal{V}_\kappa$, $\kappa = 1, 2$ such that $|\mathcal{N}_i \backslash \mathcal{V}_\kappa| \geq r$.

By employing the concept of robust graph, the next lemmas show some properties of such graphs [14], [22].

Lemma 2.1: [14] Let directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$ be an r-robust graph. Then $\mathcal{G}' = \{\mathcal{V}, \mathcal{E}'_\mathcal{G}\}$, where $\mathcal{E}'_\mathcal{G}$ is a new set of edges removed at most s incoming edges for each node, is $(r - s)$-robust.

Lemma 2.2: [22] Consider directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$. If $\mathcal{G}$ is a 1-robust graph, then $\mathcal{G}$ contains a spanning tree.

B. Dini derivatives

Given a continuous function $f : (t_0, t_1) \to \mathbb{R}$ $(t_0 < t_1)$, the upper right-hand Dini derivative $D^+ f(\cdot)$ at t is defined as

$$D^+ f(t) = \limsup_{s \to 0^+} \frac{f(t+s) - f(t)}{s}.$$

It is well known that $f(t)$ is non-increasing over (t_0, t_1) if and only if $D^+ f(t) \leq 0$, $t \in (t_0, t_1)$ (refer to [23] for a more detailed derivation). The following lemma shows a basic property of Dini derivative.

Lemma 2.3: [24] Let $V_i(t, x) : \mathbb{R} \times \mathbb{R}^m \to \mathbb{R}$ be of class C^1, where $i \in \mathcal{I}_0 = \{1, 2, ..., n\}$. Let $V(t, x) = \max_{i \in \mathcal{I}_0} V_i(t, x)$. Then $D^+ V(t, x(t)) = \max_{i \in \mathcal{I}(t)} \dot{V}_i(t, x(t))$, where $\mathcal{I}(t) = \{i \in \mathcal{I}_0 : V_i(t, x(t)) = V(t, x(t))\}$.

C. Concepts in logarithmic quantization

In the following, we provide a brief review of the logarithmic quantization. For more details, see [25]. A quantizer $q(\cdot) : \mathbb{R} \to \Gamma$ is a mapping from $\mathbb{R}$ to the set Γ of quantized levels, where Γ is finite or denumerable. The quantizer $q(\cdot)$ is called logarithmic if it has the form $\Gamma = \{\pm w_{(i)} : w_{(i)} = \rho^i w_{(0)}, i = 0, \pm 1, \pm 2, ...\} \cup \{0\}$, $0 < \rho < 1$, $w_{(0)} > 0$. The associated quantizer $q(\cdot)$ is defined as follows:

$$q(x) = \begin{cases} w_{(i)}, & \text{if } \frac{1}{1+\beta} w_{(i)} < x < \frac{1}{1-\beta} w_{(i)} \\ 0, & \text{if } x = 0 \\ -q(-x), & \text{if } x < 0 \end{cases} \quad (1)$$

where $\beta = \frac{1-\rho}{1+\rho} \in (0, 1)$ is called sector bound. The quantization density for quantizer (1) is defined as $\frac{-2}{\ln \rho}$. It is noted that the smaller the β, the more the number of quantization levels in any given subset of $\mathbb{R}$. In this paper, we assume $q(\cdot)$ is enough to use levels to represent all the signals.

III. PROBLEM STATEMENT

Consider a continuous time multi-agent system with n agents, the network model of the system can be described with a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}_\mathcal{G}\}$. Each node in $\mathcal{V}$ represents an autonomous agent. Without loss of generality, we assume that there are two types of agents in our network: loyal agents and attack agents. We denote $\mathcal{V}_l$ and $\mathcal{V}_a$ the set of loyal nodes and the set of attack nodes, respectively. Clearly, we have $\mathcal{V} = \mathcal{V}_l \bigcup \mathcal{V}_a$, $\emptyset = \mathcal{V}_l \bigcap \mathcal{V}_a$.

Consider each loyal node with the following dynamics:

$$\dot{x}_i(t) = u_i(t), \quad i \in \mathcal{V}_l \quad (2)$$

where $x_i \in \mathbb{R}$ is the state value of i, and $u_i \in \mathbb{R}$ is the control protocol to be designed. Assume that node i can receive its neighbors' quantized state information

$$y_{i,j}(t) = q(x_j(t)), \ j \in \mathcal{N}_i, \ i \in \mathcal{V}_l \quad (3)$$

where $q(\cdot)$ is defined as in (1).

Since the state update depends on neighboring nodes' information, a set of attack nodes can affect the state updates of their neighbors by transmitting false states. In this paper, the goal of the attack agent is to prevent the system from reaching consensus or mislead system state into an invalid value (unsafe region). Assume that each attack node knows the encoding and decoding schemes of the entire network, and does not follow the protocol (2) to update its state. Instead, it is assumed to have the capability to update its state arbitrarily and convey false information to its neighbors.

To make the discussion simple, we assume that there are up to k such attack nodes in each node's neighborhood. We will refer to this model as "f-locally attack model".

Let us define $M(t)$ and $m(t)$ as the maximum and minimum current state values of all the loyal nodes, respectively, i.e., for $t \geq 0$,

$$M(t) = \max_{i \in \mathcal{V}_l} x_i(t), \quad m(t) = \min_{i \in \mathcal{V}_l} x_i(t). \quad (4)$$

Then, we introduce the following definition.

Definition 3.1: Under the f-locally attack model, the system (2) with quantized communication is said to achieve resilient consensus if it satisfies the following conditions:

$$m(0) \leq \inf_{t \geq 0} \min_{i \in \mathcal{V}_l} x_i(t) \leq \sup_{t \geq 0} \max_{i \in \mathcal{V}_l} x_i(t) \leq M(0), \quad (5)$$

$$\lim_{t \to \infty} (q(x_i(t)) - q(x_j(t))) = 0, \ \forall i, j \in \mathcal{V}_l. \quad (6)$$

In Definition 3.1, condition (5) guarantees that each loyal node's state remains in the safety interval ϱ determined by the maximum and minimum initial values of the loyal nodes all the time. This condition is equivalent to that for any $t \geq 0$ and $i \in \mathcal{V}_l$, $x_i(t) \in \varrho = [m(0), M(0)]$. On the other hand, condition (6) guarantees all loyal nodes eventually converge to a common quantized state.

Remark 3.1: It is worth mentioning that here we just consider the quantized state $q(x)$ as the final consensus state. There may exist consensus error between the real state and quantized state, while investigating the influence of such as quantization density, initial states and the parameters of the network graph on the consensus error will be our next work.

IV. ALGORITHM FOR RESILIENT CONSENSUS

Now we present the detailed description of the proposed algorithm: To update its state at time t, each loyal node $i \in \mathcal{V}_l$, firstly extracts the current received states (quantized data) of neighbors into a set, denoted as $\Theta_i(t) = \{q(x_j(t)) \,|j \in \mathcal{N}_i\}$, then sorts the elements in $\Theta_i(t)$ from the largest to the smallest. If there exist no less than f data strictly larger than $q(x_i(t))$, then i discards precisely the largest f data in the sorted set $\Theta_i(t)$ by temporarily cutting off corresponding incoming communication links. Otherwise, i discards all of these data in $\Theta_i(t)$; Meanwhile, node i applies the similar manipulation to the smallest data in set $\Theta_i(t)$.

Let $\mathcal{F}_i(t)$ be the set of elements which discarded by node i at time t. Then we design the following control $u_i(t)$ for node i:

$$u_i(t) = \sum_{j \in \mathcal{N}_i / \mathcal{F}_i(t)} [y_{i,j}(t) - y_{i,i}(t)], i \in \mathcal{V}_l. \tag{7}$$

Substituting the protocol (7) into the system (2) - (3) leads to

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i / \mathcal{F}_i(t)} [q(x_j(t)) - q(x_i(t))], i \in \mathcal{V}_l. \tag{8}$$

It is worthwhile to mention that although the initial network considered there is fixed, the protocol (7) involving manipulations of communication edges can lead the network to a stochastically time-varying graph $\mathcal{G}_{\sigma(t)} = (\mathcal{V}, \mathcal{E}_{\sigma(t)})$.

Assumption 4.1: There exists a scalar $\tau_D > 0$ as a lower bound between any two switching time instants t_k, $t_{k+1} \in \sigma(t)$, i.e., $t_{k+1} - t_k \geq \tau_D$.

From protocol (7) above, we know that each loyal node may remove up to $2f$ data from the set $\Theta_i(t)$. However, when the attack nodes' state information is not inside the range of the top and bottom f data of the sorted list, the above algorithm cannot remove this data effectively. Under this case, the loyal nodes may possibly adopt these attack nodes' values for updating their own states. This special attack node is summarized in the following definition.

Definition 4.1: A mild attack node is a node q, $q \in \mathcal{V}_a$ whose state information is received and kept by its loyal neighbor p, $p \in \mathcal{V}_l$ under the protocol (7) at time t. Then, the state $x_q(t)$ can be expressed as a convex combination of all the quantized state information of loyal nodes. i.e.,

$$x_q(t) = \sum_{j \in \mathcal{V}_l} \varphi_{p,j}(t) q(x_j(t)), \quad q \in \mathcal{V}_a \cap \mathcal{N}_i, \tag{9}$$

where $0 \leq \varphi_{p,j}(t) \leq 1$ and $\sum_{j \in \mathcal{V}_l} \varphi_{p,j}(t) = 1$.

From the above definition, we can observe that each mild attacker' value is a convex combination of values of all loyal agents. It is thus clear that $x_q(t) \in \varrho$, $\forall q \in \mathcal{N}_i / \mathcal{F}_i(t)$. For each loyal node p which does not adopt attackers' state values in the protocol (7) at time t, we just set $\varphi_{p,j}(t) = 0, j \in \mathcal{V}_l$.

Now, let us state the main result of this paper.

Theorem 4.1: Consider the multi-agent system (2) with interaction protocol (7). The communication topologies among the nodes satisfy a $(2f+1)$-robust graph. Then, the resilient consensus can be achieved under the f-locally attack model.

Proof: We firstly prove that the safety condition (5) holds with ϱ, i.e., $x_i(t) \in \varrho$ for any t and $i \in \mathcal{V}_l$. From the definition (4), we have $x_i(0) \leq M(0)$. Assume this case is violated at time t^*. When this happens, it holds that: $x_i(t) \leq M(0)$ for $t \in [0, t^*]$ for all $i \in \mathcal{V}_l$; At time t^* there exists a node $i \in \mathcal{V}_l$ such that we have $x_i(t^*) = M(0)$ and $\dot{x}_i(t^*) > 0$. Suppose this case holds. Then recall the structure of (8), we have

$$\dot{x}_i(t^*) = \sum_{j \in \mathcal{N}_i / \mathcal{F}_i(t)} [q(x_j(t^*)) - q(x_i(t^*))], \; i \in \mathcal{V}_l. \tag{10}$$

We can find that each term on the right hand side is non-positive as $q(x_i(t^*)) = q(M(0)) \geq q(x_j(t^*))$; and therefore $\dot{x}_i(t^*) \leq 0$, which results a contradiction. The other direction $x_i(t) \geq m(0)$ can be proved using similar arguments. Then the safety condition (5) is satisfied.

It remains to prove the consensus condition (6). We define $W = \max_{i \in \mathcal{V}_l}\{x_i\} - \min_{j \in \mathcal{V}_l}\{x_j\}$ as a candidate Lyapunov function. Due to the dynamic topologies, W may not be continuously differentiable, but W is still continuous. Hence, it is possible to analyze the Dini derivative of W to obtain its convergence property. We define $x_{\max} = x_I$, $x_{\min} = x_J$ where $I \triangleq \max_i\{i : x_i = \max_{k \in \mathcal{V}_l}\{x_k\}\}$, and $J \triangleq \min_i\{i : x_i = \min_{k \in \mathcal{V}_l}\{x_k\}\}$. For the quantizer (1), we have $\text{sign}(q(x)) = \text{sign}(x)$, $\max_{i \in \mathcal{V}_l} q(x_i(t)) = q(x_{\max}(t))$, and $\min_{i \in \mathcal{V}_l} q(x_i(t)) = q(x_{\min}(t))$. Since $q(x_{\max}) \geq q(x_i(t)) \geq q(x_{\min})$ for all $i \in \mathcal{V}_l$, the following equations hold by Lemma 2.3: $\dot{x}_{\max} = \sum_{j \in \mathcal{N}_{\max}} [q(x_j) - q(x_{\max})] \leq 0$, and $\dot{x}_{\min} = \sum_{j \in \mathcal{N}_{\min}} [q(x_j) - q(x_{\min})] \geq 0$. Thus, W is non-increasing throughout the closed loop system evolution.

Now we prove $D^+W(t) \to 0$ as $t \to \infty$. Suppose that $D^+W(t)$ does not converge to zero as $t \to \infty$. Under this case, there must exist a constant $\varepsilon_0 > 0$ so that for $\bar{T} > 0$, there is a positive $t > \bar{T}$ such that $D^+W(t) \leq -\varepsilon_0$ (note that $D^+W \leq 0$).

Then we know that there must exist a constant $\delta_0 > 0$ and a time sequence $\{t_i\}_{i \in \mathbb{N}}$, with $t_i \to \infty$ as $i \to \infty$, so that $D^+W(t) \leq -\varepsilon_0$ and $|t_{i+1} - t_i| > \delta_0$ for any i. For Δt where $D^+W(t)$ is continuous, i.e. $t_k \notin \Delta t$ for all i, since the safety condition (5) guarantees that $x_i(t)$ and $\dot{x}_i(t)$ bounded, we have that $D^+W(t)$ is uniformly continuous. Therefore, there is a $\delta_1 > 0$ such that for any time t' and t'' satisfying $|t' - t''| < \delta_1$, it holds that:

$$\left|D^+W(t') - D^+W(t'')\right| < \frac{\varepsilon_0}{2}. \tag{11}$$

This implies that

$$\begin{aligned} D^+W(t) &= -\left|D^+W(t_i) - (D^+W(t_i) - D^+\bar{V}(t))\right| \\ &\leq -(|D^+W(t_i)| - |D^+W(t_i) - D^+W(t)|) \\ &\leq -\varepsilon_0 + \tfrac{\varepsilon_0}{2} \\ &= -\tfrac{\varepsilon_0}{2}. \end{aligned} \tag{12}$$

for $\forall t \in [t_i - \delta_1, t_i + \delta_1]$.

Now consider the other situation when t_i is right after a discontinuity t_k. Under this situation, $D^+W(t) \leq -\varepsilon_0/2$ might not be satisfied if $t_k \in [t_i - \delta_1, t_i + \delta_1]$ as $D^+W(t)$ may increase at t_k. However, by assumption 4.1, there exists a dwell time τ_D before the next discontinuity time instant. This ensures that there is a constant $\delta_2 \in (0, \tau_D)$ such that $D^+W(t) \leq -\varepsilon_0/2$ for all $t \in [t_k, t_k + \delta_2]$. Then, integrate $D^+W(t)$ over $(0, \infty)$, we have

$$\begin{aligned} \int_0^\infty D^+W(t)\mathrm{d}t &\leq \lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} D^+W(t)\mathrm{d}t \\ &\leq -\lim_{N\to\infty} \sum_{i=1}^{N} \int_{t_i-\delta}^{t_i+\delta} \tfrac{\varepsilon_0}{2}\mathrm{d}t \qquad (13) \\ &= -\lim_{N\to\infty} N\varepsilon_0\delta \\ &= -\infty, \quad \delta \in \min\{\delta_1, \delta_2\}. \end{aligned}$$

This is obviously a contradiction to objective condition $W(t) \geq 0$, for all $t > 0$. We have thus shown, by this contradiction, that $D^+W(t) \to 0$ as time to infinity, which implies $\lim_{t\to\infty} W(t) = constant$, i.e., the agents with maximal and minimal state eventually keep fixed state. For agent I, this is equivalent to $\sum_{j\in\mathcal{N}_I}[q(x_j) - q(x_{\max})] = 0$, and since $q(x_{\max}) \geq q(x_j)$ for all $j \in \mathcal{N}_I$, the latter implies that $q(x_j) = q(x_{\max})$ for all $j \in \mathcal{N}_I$. Pick any $k \in \mathcal{N}_I$, where k does not coincide with the maximum node. Then $q(x_k) \geq q(x_j)$, for all $j \in \mathcal{N}_k$ and hence $\dot{x}_k = \sum_{j\in\mathcal{N}_k}[q(x_j) - q(x_k)] \leq 0$. If $\dot{x}_k < 0$, then necessarily $\dot{x}_I < 0$ since $q(x_k) = q(x_{\max})$. Hence we also have $\dot{x}_k = 0$ and hence $q(x_j) = q(x_k) = q(x_{\max})$ for all $j \in \mathcal{N}_k$. We just repeat the same operation for a random $l \in \mathcal{N}_k$. Since the initial network is a $(2f+1)$-robust graph, after removing up to $2f$ incoming links for each loyal node, the network is still 1-robust from Lemma 2.1. Then by Lemma 2.2, it is easy to know that the graph must contain a spanning tree, and consequently, there exist a limited iterations of the above process that diffuses to all node in the topology. Thus, all nodes in the path to agent I from the root node possess the same state of $q(x_{\max})$. Similarly, we can show that all nodes in the path to agent J from the root node possess the same state of $q(x_{\min})$. We can obtain that all agents in spanning tree hold the states of the maximum and the minimum, i.e., $q(x_{\max}) = q(x_{\min})$. Therefore, the consensus property (6) is satisfied. ■

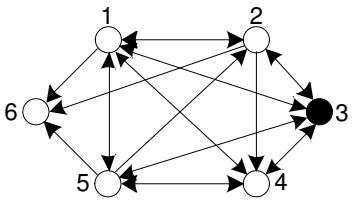

Fig. 1. Communication graph $\mathcal{G}$.

V. EXAMPLE AND SIMULATIONS

Let us consider a system consisting of 5 loyal nodes and 1 attack node. The communication links are connected as Fig. 1. The initial values of the agents are given by $x_1(0) = 17.2$, $x_2(0) = 20.5$, $x_3(0) = 5.9$, $x_4(0) = 8.7$, $x_5(0) = 0.8$, and $x_6(0) = 10.3$. The logarithmic quantizer (1) with $w_{(0)} = 30$, $\beta = 0.1$ is applied. Suppose that node 3 is an attack agent whose dynamic is designed as

$$\dot{x}_3(t) = -0.8x_3(t) + 0.8u_3.$$

For the simulations, let the reference input $u_3 = 28$. Obviously, the goal of node 3 is to mislead the loyal nodes' states to the extremely value 28 which is outside of the range of interval $\varrho = [0.8, 20.5]$.

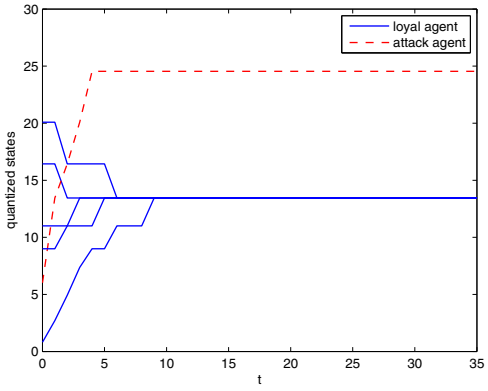

Fig. 2. State trajectories of the system with logarithmic quantizer (1).

Based on Lemma 2.1, one can verify that the system topology in Fig. 1 satisfies a 3-robust graph. Also we can find that there is at most one attack neighbor ($f = 1$) for each node in the graph. Then, the robustness condition of the network topology in Theorem 4.1 is satisfied. The state trajectory of the system under the protocol (7) is shown in Fig. 2. We can see that all loyal nodes' ultimate states converge to 13.4, which is within the safety interval set $\varrho = [0.8, 20.5]$.

VI. CONCLUSIONS

The secure consensus control problem for multi-agent systems in the face of malicious attacks has been studied in this paper. Based on a local security mechanism, a novel quantization-based resilient consensus protocol has been designed to achieve agreement under a f-locally bounded attack model. Theoretical analysis proved that, if the network connectivity satisfies $(2f + 1)$-robust, then the information consensus value of all the loyal nodes can be achieved. Finally, the numerical example showed the effectiveness of the algorithm.

REFERENCES

[1] A. Jadbabaie, J. Lin *et al.*, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on Automatic Control*, vol. 48, no. 6, pp. 988–1001, 2003.

[2] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, 2004.

[3] L. Moreau, "Stability of multiagent systems with time-dependent communication links," *IEEE Transactions on Automatic Control*, vol. 50, no. 2, pp. 169–182, 2005.

[4] S. Liu, L. Xie, and H. Zhang, "Distributed consensus for multi-agent systems with delays and noises in transmission channels," *Automatica*, vol. 47, no. 5, pp. 920–934, 2011.

[5] Y. G. Sun and L. Wang, "Consensus of multi-agent systems in directed networks with nonuniform time-varying delays," *IEEE Transactions on Automatic Control*, vol. 54, no. 7, pp. 1607–1613, 2009.

[6] W. Ren, R. W. Beard *et al.*, "Consensus seeking in multiagent systems under dynamically changing interaction topologies," *IEEE Transactions on Automatic Control*, vol. 50, no. 5, pp. 655–661, 2005.

[7] S. Liu, L. Xie, and F. L. Lewis, "Synchronization of multi-agent systems with delayed control input information from neighbors," *Automatica*, vol. 47, no. 10, pp. 2152–2164, 2011.

[8] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Resilient continuous-time consensus in fractional robust networks," in *Proceedings of the 2013 American Control Conference (ACC)*. IEEE, 2013, pp. 1237–1242.

[9] W. Zeng and M.-Y. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE Transactions on Cybernetics*, vol. 44, no. 11, pp. 2038–2049, 2014.

[10] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Transactions on Cybernetics*, vol. 44, no. 11, pp. 2024–2037, 2014.

[11] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[12] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[13] W. Zeng and M.-Y. Chow, "A reputation-based secure distributed control methodology in d-ncs," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 11, pp. 6294–6303, 2014.

[14] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[15] H. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *American Control Conference (ACC), 2012*. IEEE, 2012, pp. 5855–5861.

[16] S. M. Dibaji and H. Ishii, "Consensus of second-order multi-agent systems in the presence of locally bounded faults," *Systems & Control Letters*, vol. 79, pp. 23–29, 2015.

[17] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1495–1508, 2011.

[18] N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *Proceedings of the 2012 ACM symposium on Principles of distributed computing*. ACM, 2012, pp. 365–374.

[19] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[20] R. C. Cavalcante, I. I. Bittencourt, A. P. da Silva, M. Silva, E. Costa, and R. Santos, "A survey of security in multi-agent systems," *Expert Systems with Applications*, vol. 39, no. 5, pp. 4835–4846, 2012.

[21] Y. Jung, M. Kim, A. Masoumzadeh, and J. B. Joshi, "A survey of security issue in multi-agent systems," *Artificial Intelligence Review*, vol. 37, no. 3, pp. 239–260, 2012.

[22] Y. Wu, X. He, S. Liu, and L. Xie, "Consensus of discrete-time multi-agent systems with adversaries and time delays," *International Journal of General Systems*, vol. 43, no. 3-4, pp. 402–411, 2014.

[23] F. H. Clarke, Y. S. Ledyaev, R. J. Stern, and P. R. Wolenski, *Nonsmooth analysis and control theory*. Springer Science & Business Media, 2008, vol. 178.

[24] G. Shi, K. H. Johansson, and Y. Hong, "Reaching an optimal consensus: dynamical systems that compute intersections of convex sets," *IEEE Transactions on Automatic Control*, vol. 58, no. 3, pp. 610–622, 2013.

[25] S. Liu, T. Li, L. Xie, M. Fu, and J.-F. Zhang, "Continuous-time and sampled-data-based average consensus with logarithmic quantizers," *Automatica*, vol. 49, no. 11, pp. 3329–3336, 2013.