2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Consensus Resiliency of Stochastic Observation via Ring Lattices of Sensors Facing Byzantine Attacks

Haotian Peng, Yuke Li and Li Jin

Abstract— **We consider the observation of a random, binary environment state via a set of sensing nodes connected through a ring lattice. Each node obtains a correct observation with a positive probability and broadcasts its observation to its neighbors. A system operator selects a consensus threshold for the number of consistent observations, and a consensus is reached when any node has accumulated sufficient consistent observations. A Byzantine attacker can manipulate a certain number of nodes to broadcast misleading information, and thus prohibit a correct consensus. We formulate this problem as a zero-sum game and analyze the equilibria. We show that the attacker has a dominant strategy for selecting the nodes to manipulate and the information to broadcast/block. We show that, unless the attacker's budget is abundant, the system operator can select an optimal consensus threshold to balance between the chance of a correct consensus and the risk of a wrong consensus. We also use the equilibrium structure to characterize the network resiliency, i.e., the minimal number of Byzantine nodes that would eliminate the chance of a correct consensus, given the size and connectivity of the ring lattice. The results are relevant for hardware surveillance, infrastructure inspection, disaster response, etc.**

Index terms: Byzantine faults, security games, Nash equilibrium, network resiliency.

I. Introduction

Networked sensors are commonly used for observation, with consensus generated by a centralized infrastructure based on distributed information exchanges among neighboring sensors. This partially decentralized observation strategy is more efficient, scalable, and resilient than fully centralized strategies [1], [2], making it suitable for various tasks including hardware surveillance [3], [4], infrastructure inspection [5], [6], [7], disaster response [8], [9], and public security [10]. However, the decentralized nature of networked sensors may lead to vulnerability to malicious attacks [11], [12]. In particular, Byzantine attacks are a class of worst-case adversarial behaviors that compromise the integrity of the network by manipulating certain nodes to spread misleading information in the network, thus leading to confusion or wrong consensus [12].

Motivated by this challenge, we consider the resiliency of consensus-based observation of a common state in the face of Byzantine attacks. In this paper, we focus on ring lattice networks as shown in Fig. 1. The ring lattice topology employed in this paper is relevant in many scenarios, such as multiple unmanned aerial vehicles (UAVs) surrounding a stronghold during drone warfare and determining whether to attack, and multiple UAVs monitoring a radiation center after a nuclear contamination incident to assess the radiation situation. We formulate the interaction between a centralized system operator and a Byzantine attacker as a zero-sum game, where the utility of the system operator is the probability of attaining a correct consensus. By characterizing the equilibrium structure of the game, we study the behaviors of the attacker and possible responses of the operator. The results provide insights for analyzing system resiliency and the improvement of networked sensors.

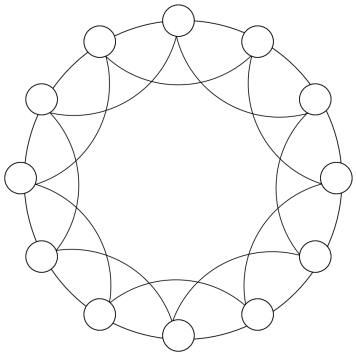


Fig. 1: A ring lattice $R_{12,2}$.

The resiliency of networked sensors in the face of Byzantine attacks has received increasing attention over the past two decades. Lamport et al. [13] first introduced the so-called *Byzantine generals problem*, which considers the consensus on a mixing set of loyal and traitorous generals (nodes). There exists a line of work on sensing networks with Byzantine nodes, the majority of which has been focused on complete graphs; only a limited amount of literature discussed incomplete graphs and/or more general network structures. Previous work on complete graphs has concentrated on enhancing Byzantine fault tolerance [14], [15] and decreasing computation complexity [16]. Various models for imperfect loyal nodes have also been studied [17], [18], [19]. In terms of resiliency analysis, Kingston et al. [20] suggest a saturated innovation update algorithm to increase the network's resiliency. Castro et al. [21] proposed an algorithm based on noisy local measurements and a gradient descent update to address Byzantine faults. However, it is still unclear to what extent these results can be generalized to incomplete graphs. Some results for incomplete graphs

This work was in part supported by the National Natural Science Foundation of China, SJTU UM Joint Institute, J. Wu & J. Sun Foundation.

H. Peng and L. Jin are with the UM Joint Institute, Shanghai Jiao Tong University, China. Y. Li is with the Yale University, USA. (Emails: htpeng@sjtu.edu.cn, li.jin@sjtu.edu.cn, yukeli33@gmail.com)

have been developed [22], [23]. In particular, Kaikhura et al. [24] proposed a robust distributed weighted average consensus algorithm in the context of data falsification attacks. Sundaram[25] raised a robustness standard in distributed state estimation for LTI systems under Byzantine attacks by a local-filtering algorithm. However, there is very limited research on the Byzantine attacks in incomplete networks using game-theoretic models.

In this paper, we investigate the problem of estimating a static binary random variable based on observations by a ring lattice of sensors (nodes). In our previous work [26], we reformulated the estimating problem into a game-theoretic problem where agents strategically transmit messages and coordinate actions on a hierarchical graph. Our work in this paper provides an game-theoretical approach to the classical Byzantine generals problem on another practical graph. The random variable represents the state of the environment, and the observations are subject to a positive probability of error. Achieving consensus among the nodes will result in a decision, and a decision that aligns with the actual environment state is preferred. We consider a zero-sum game between a system operator and a malicious Byzantine attacker. The operator selects a threshold for consensus, i.e., the minimum number of consistent observations required for a consensus. The attacker selects the nodes to manipulate and determines the information to broadcast from the manipulated nodes. The operator (resp. attacker) aims to maximize (resp. minimize) the probability of attaining a correct consensus.

We characterize the equilibrium structure of the zero-sum game. Our analysis reveals that the attacker's dominant strategy is to partition the network into as many approximately equal parts as possible by manipulating a certain number of Byzantine nodes (Theorem 1). We observe that the game has two regimes of qualitatively different equilibria, which depend on the number of Byzantine nodes relative to the network size and connectivity. Specifically, when there are too many Byzantine nodes, the system operator cannot receive correct estimation. Otherwise, the operator can play strategically to ensure a strictly positive probability of correct estimation (Theorem 2).

We also use the properties of the equilibria to gain valuable insights into the resilience of the sensor network. We derive a closed-form quantification of the network's resilience (Proposition 1). Specifically, the resilience score is defined as the minimum number of Byzantine nodes that can eliminate the chance of achieving a correct consensus. We find that this resilience score increases approximately with the square root of both the degree and the size of the ring lattice.

The paper is organized as follows: In Section II, we formulate the zero-sum game with Byzantine attacks. Section III analyzes the Nash equilibrium of the game and demonstrates the model's resiliency under various numbers of Byzantine nodes. We conclude the paper in Section IV and discuss future directions for research.

II. Problem formulation

In this section, we formulate the zero-sum game between the operator and the attacker. We first develop the model for networked sensors without Byzantine nodes (Section II-A). Then, we specify the model for the Byzantine attacker and formulate the security game (Section II-B).

A. Network model without Byzantine nodes

Consider a regular ring lattice $R_{n,a}$ with nodes $V = \{1, 2, \ldots, n\}$ and degree a (Fig. 1). We define N_i as the neighbor set of node $i \in V$; note that $|N_i| = 2a$ for all $i \in V$. A node can only send messages to or receive messages from its neighboring nodes. A path s is a sequence of immediately connected, non-repeating nodes. We write $i \in s$ if node i is on path s. We denote the set of paths from i to j as S_i^j and define $S_i = \cup_j S_i^j$. The set of all paths is S. We use $|s|$ to denote the length, i.e. the number of *links*, on path s.

A system operator aims to estimate the value of a binary random variable X with Bernoulli distribution

$$\Pr\{X = 1\} = 1 - \Pr\{X = 0\} = \pi \in (0, 1).$$

The estimation is based on the consensus among the observations from each node, which follows a typical three-stage procedure, viz. sensing, information fusion, and decision making [24] as follows.

Sensing: At discrete time $t = 0$, each node i makes an observation and obtains Y_i, which we denote as $Y = [Y_1, Y_2, \ldots, Y_n]^T$, where Y_i is the observation of node i. We assume that Y_i's are independent of each other and depend on X as follows:

$$\Pr\{Y_i = X\} = p_i,$$
$$\Pr\{Y_i = 1 - X\} = 1 - p_i.$$

where p_i is the observation accuracy of node i. For the sake of simplification, it is assumed that each node has the same observation accuracy, i.e. $p_i = p$.

An observation Y_i is said to be *correct* if $Y_i = X$ and said to be *class-y* if $Y_i = y \in \{0, 1\}$.

Information fusion: Every node i will broadcast its observation Y_i to its neighbors as a message. When a node receives a message, it will relay to all its neighbors. If a message is sent to a node that the message has visited, the node will disregard this message. After sufficiently long time, each node i will receive the observations from all nodes j that communicate with i. Let V_i be the set of nodes that communicate with i. At the end of information fusion, every node reports the numbers of class-0 and class-1 messages that it has received, which are given by

$$K_i^y := \sum_{j \in V_i} \mathbb{I}\{Y_j = y\}, \quad y \in \{0, 1\}. \tag{1}$$

where $\mathbb{I}$ is the indicator function. In the absence of Byzantine nodes, all nodes communicate, so K_i^y is independent of i.

Decision making: The operator specifies a threshold $1 \leq K \leq n$ that determines the consensus of the observations of

X as follows. Let

$$Z^y := \sum_{i \in V} \mathbb{I}\{|K_i^y| \geq K\}, \quad y \in \{0,1\}.$$

Then, the operator's estimation is determined by

$$\hat{X} = \begin{cases} 1 & \text{if } Z^1 > Z^0, \\ 0 & \text{if } Z^0 > Z^1, \\ -1 & \text{otherwise.} \end{cases}$$

The operator aims to maximize the probability that the estimation agrees with the state, i.e.,

$$\Pr\{\hat{X} = X\}.$$

Note that the above probability depends on the consensus threshold K, which we consider to be the decision for the operator:

$$\sigma_o = K.$$

We will derive the formula for $\Pr\{\hat{X} = X\}$ in the next section, after the attacker model is defined.

B. Model for Byzantine attacker

We consider a Byzantine attacker that is capable of manipulating some nodes in the network. We assume that the attacker knows the true value of X. The attacker aims to minimize the probability of a correct consensus; Hence, the attacker plays a zero-sum game against the operator.

The decision for the attacker includes the following.

1) Selecting the set of nodes to hack. The set of hacked nodes is denoted by $M \subset V$. Following the convention of the Byzantine general problem, we call M the set of *traitorous* (or *Byzantine*) nodes and $V \backslash M$ the set of *loyal* nodes. Let m be the cardinality of M:

$$m := |M|.$$

   where $|\cdot|$ is the cardinality of a set.
2) Manipulating the observation by a hacked node. That is, $\{Y_i; i \in M\}$ can be arbitrarily falsified by the attacker.
3) Blocking the messages received by a hacked node. That is, the attacker can block any path in

$$\mathcal{Q}(M) := \{s \in S : j \in s, j \in M\}$$

   We denote the set of blocked paths by Q, which is a subset of Q(M).

Hence, the decision for the attacker is

$$\sigma_a := \Big(M, \{Y_i, i \in M\}, Q\Big).$$

Note that in the face of Byzantine attacks, the behavior of K_i^y as defined in (1) is no longer trivial. In this zero-sum game, the system operator and the attacker choose their strategy simultaneously without information of their competitor. Then, we can write the utilities for both players as

$$u_o(\sigma_o, \sigma_a) := \Pr\{\hat{X} = X\},$$
$$u_a(\sigma_a, \sigma_o) := -\Pr\{\hat{X} = X\}.$$

Before proceeding, we note that if $m \geq n/2$, the game is trivial in the sense that the attacker can manipulate the estimation result regardless of the operator's strategy. Hence, we make the following assumption for the subsequent analysis:

Assumption 1: $m < n/2$.

Let K_1 (resp. K_2) be the maximum number of correct (resp. incorrect) observations that any loyal node receives; i.e.,

$$K_1 := \max_{i \in V} K_i^X,$$
$$K_2 := \max_{i \in V} K_i^{1-X}.$$

Given $\sigma_o = K$, for any strategy σ_a for the attacker, the probability of a correct estimation is given by

$$\begin{aligned} &\Pr\{\hat{X} = X\} = 1 - \Pr\{\hat{X} \neq X\} \\ &= 1 - \Pr\{K_2 \geq K\} \\ &\quad - \sum_{i=m}^{K-1} \Pr\{K_2 = i\} \Pr\{K_1 < K | K_2 = i\}. \end{aligned} \tag{2}$$

In the above equation, $\Pr\{K_2 \geq K\}$ is the probability of reaching an incorrect consensus and $\sum_{i=m}^{K-1} \Pr\{K_2 = i\} \Pr\{K_1 < K | K_2 = i\}$ is the probability of being unable to reach both correct and incorrect consensus. As long as $K_2 \geq K$, Z^{1-X} will be n, which leads to an incorrect consensus. With sufficiently long time, we immediately have

$$\Pr\{K_2 \geq K\} = \sum_{i=K-m}^{n-m} \binom{n-m}{i} (1-p)^i p^{n-m-i},$$
$$\Pr\{K_2 = i\} = \binom{n-m}{i-m} (1-p)^i p^{n-m-i}.$$

The calculation of $\Pr\{K_1 < K | K_2 = i\}$ will be discussed in the next section, when we characterize the properties of the game. A *Nash equilibrium* (NE) of the above zero-sum game is a combination of strategies for both players (σ_o^*, σ_a^*) such that neither player can improve its utility by unilaterally playing an alternative strategy. The *best response* for a player is a strategy that maximizes its utility with the other player's strategy fixed. A strategy is *dominant* if it is the best response for all strategies for the other player.

III. Analysis of Equilibrium

In this section, we analyze the NE of the zero-sum game. Under sufficiently long time, the pure strategy NE is guaranteed. We first discuss the best response for the attacker σ_a^*, which turns out to be a dominant strategy (Section III-A). Then, we calculate the utility for both players and develop the equilibrium strategy σ_o^* for the system operator (Section III-B).

A. Attacker's Dominant Strategy

Since the attacker can block messages on certain paths, it can actually partition the network into disconnected parts. We define a *partition group* as a set of Byzantine nodes containing at least a consecutive nodes in the ring; see Fig. 2.

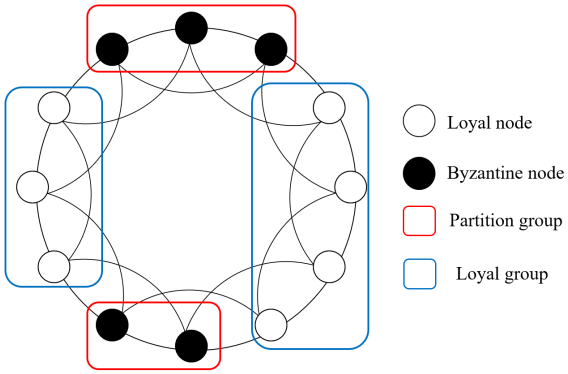


Fig. 2: A ring lattice $R_{12,2}$ with $r = 2$

Define the number of partition groups as r. If all nodes in a partition group G block every path $s \in \mathcal{Q}(G)$, then no messages can transmit through $G \subset M$.

We also define a *loyal group* as a group of loyal nodes, in which any two nodes have at least one path $s \notin \mathcal{Q}(M)$ between them. When $r \leq 1$, all loyal nodes will constitute one loyal group with $n - m$ nodes, because the Byzantine nodes cannot block all paths between any two loyal nodes in such cases. When $r > 1$, there will be r loyal groups divided by r partition groups. We call the biggest loyal group as the *optimal loyal group*. The number of loyal nodes in the optimal loyal group is l^*. When there is only one loyal group, we always have $l^* = n - m$. An example of loyal groups and partition groups is shown in Fig. 2.

Let $l^*_{\min}$ represents the minimum value of l^*. Based on the value of m, $l^*_{\min}$ can be expressed as

$$l^*_{\min} = \begin{cases} n - m, & m < 2a \\ \lceil (n-m)/r \rceil, & m \geq 2a \end{cases}$$

Then, we can characterize the attacker's best response as follows:

Theorem 1: (Dominant Strategy for the Attacker). The attacker's best response under any strategy for the operator is as follows. To determine M:

1) Select $r = \lfloor m/a \rfloor$ partition groups.
2) If $r > 1$, loyal nodes should be divided into r loyal groups with either $l^*_{\min}$ or $l^*_{\min} - 1$ loyal nodes.

At each Byzantine node $j \in M$,

1) If $Y_i = X$, then block all paths $s \in S_i$ such that $j \in s$;
2) If $Y_i = 1 - X$, then do not block any path $s \in S_i$ such that $j \in s$;
3) $Y_j = 1 - X$;

Proof.

Selection of M:

Then, consider the optimal rules for the attacker. Based on the information fusion of loyal nodes and the dominant strategy of Byzantine nodes, an incorrect message can be transmitted freely in the network, while a correct message will be blocked by partition groups. Based on (2), we know that the attacker can only affect $\Pr\{K_1 < K | K_2 = i\}$. We prove the rules for the attacker by considering two cases:

When $m < 2a$, we have $r \leq 1$ where we only need to consider rule 1. Since the loyal nodes will always constitute a loyal group with $n - m$ nodes, rule 1 is met because the attacker cannot get a better payoff by unilaterally changing the number of partition groups.

When $m \geq 2a$, we state the probability $\Pr\{K_1 < K | K_2 = i\}$ by

$$\begin{aligned} \Pr\{K_1 < K | K_2 = i\} &= \Big| \bigcap_{j=1}^{r} L_j^c \Big| \binom{n-m}{n-m-i}^{-1} \\ &= \sum_{I \subseteq [r]} (-1)^{|I|} \Big| \bigcap_{j \in I} L_j \Big| \binom{n-m}{n-m-i}^{-1}. \end{aligned} \tag{3}$$

In (3), $\Big| \bigcap_{j=1}^{r} L_j^c \Big|$ is a inclusion-exclusion formula representing the number of cases that $K_1 < K$. Let the number of loyal nodes in the j-th group, $j \in \{1, 2, \ldots, r\}$ is l_j. L_j represents all cases that there are no less than K nodes in l_j receive correct observation as

$$L_j = \begin{cases} 0, & l_j < K, \\ \sum_{u=K}^{l_j} \binom{l_j}{u} \binom{n-m-l_j}{n-m-i-u}, & l_j \geq K. \end{cases}$$

Note that $\Big| \bigcap_{j \in \emptyset} L_j \Big| = \binom{n-m}{n-m-i}$ represents the total number of conditions.

The attacker aims to maximize $\Pr\{K_1 < K | K_2 = i\}$ for $i \in [m, K-1]$, if not an empty set, i.e. maximize the numerator.

Rule 1 is proved by contradiction. Suppose the attacker choose to control $r < \lfloor m/a \rfloor$ partition groups, we prove that controlling $r + 1$ partition groups is a better strategy.

We assume that $l^* \geq K$ when the attacker controls r partition groups, or $Z^X = 0$ if all Byzantine nodes choose to block every correct message. In such case, the attacker's payoffs are the same for controlling r and $r + 1$ partition groups.

Then we add an additional partition group to cut the optimal loyal group into two groups with $K-1$ and l^*-K+1 nodes, respectively. Consider the case where K correct observations are obtained in the group. Each node j inside can obtain $K_j^X = K$ through information fusion without the additional partition group. However, $K_j^X \leq K - 1$ for nodes in the group with $K - 1$ nodes after cutting, which leads to a smaller Z^X. In this case, $\Pr\{K_1 < K | K_2 = i\}$ decreases, which leads to decrease of $\Pr\{\hat{X} = X\}$. Therefore, controlling $r + 1$ partition group is a better strategy. The attacker should control the maximum number of partition groups, i.e. $r = \lfloor m/a \rfloor$.

Rule 2 is also proved by contradiction. If each loyal group does not have exactly $l^*_{\min}$ or $l^*_{\min} - 1$ loyal nodes, there exist two loyal groups A and B with l_A and l_B loyal nodes, respectively, where $l_A - l_B \geq 2$. We prove that partitioning these two groups into two groups with $l_A - 1$ and $l_B + 1$ loyal nodes is a better strategy.

1) When $r(K-1) < n-m-i$, there must be at least one group that contains at least K correct observations according to the pigeonhole principle. Therefore, $\Pr\{K_1 < K | K_2 = i\} = 0$ as $K_1 \geq K$, the attacker receives the same payoff regardless of how it divides the loyal nodes.
2) When $r(K-1) \geq n-m-i$, without loss of generality, consider a node o in group A, we show that putting node o into group B is a better strategy.
Consider the numerator in the case of $Y_o = 1$ (In other cases, placing node o in group or A or B makes no difference to the decision making). If the grouping remains unchanged, the numerator contains the cases where the other $l_A - 1$ nodes in group A can accommodate at most $K-2$ correct observations while group B can accommodate at most $K-1$. If node o is moved to group B, the numerator contains the cases where the other $l_A - 1$ nodes in group A will have the capacity for at most $K-1$ correct observations while group B can accommodate at most $K-2$ correct observations. By subtracting w_2 and w_1, we obtain:

$$\begin{aligned}\Delta &= \tbinom{l_A-1}{K-1} \sum_{j=0}^{K-2} \tbinom{l_B}{j} C_j - \tbinom{l_B}{K-1} \sum_{j=0}^{K-2} \tbinom{l_A-1}{j} C_j \\ &= \sum_{j=0}^{K-2} \left(\tbinom{l_A-1}{K-1}\tbinom{l_B}{j} - \tbinom{l_A-1}{j}\tbinom{l_B}{K-1} \right) C_j\end{aligned}$$

where $C_j \geq 0$ is a constant refering to the number of cases that $K_1 < K$ by putting $n-m-i-j$ correct observations in the rest of loyal groups. Since

$$\begin{aligned}\frac{\binom{l_A-1}{K-1}\binom{l_B}{j}}{\binom{l_A-1}{j}\binom{l_B}{K-1}} &= \frac{(l_A-1-j)!\,(l_B-K+1)!}{(l_A-K)!\,(l_B-j)!} \\ &= \frac{(l_A-1-j)\dots(l_A-K+1)}{(l_B-j)\dots(l_B-K+2)} > 1,\end{aligned}$$

as $l_A - 1 > l_B$ and $j < K-1$. Therefore, we can obtain that $\Delta > 0$, which indicates that it is better to put node o into the smaller group B rather than group A.
Based on the aforementioned reasoning, it can be proved that in the end, each loyal group contains $l^*_{\min}$ or $l^*_{\min} - 1$ loyal nodes. At this point, the attacker cannot gain greater payoff by unilaterally changing the number of nodes in any two loyal groups.

Decision at node $j \in M$:

When node j receives a message Y^i, it needs to decide whether to relay it to its neighbors in N_j. Without loss of generality, suppose the true value of X is 1. For any node $u \in N_j$:

When $Y_i = 1$, If j relays the message to u, the number of K_u^1 may increase by 1 (if u never received that message from other nodes); if it chooses not to relay, the information stored by u will not change. Therefore, choosing not to relay is a dominant strategy to prevent node u from reaching a higher K_u^1. Since this strategy holds for all nodes in N_j, the final strategy of node j will be blocking any path $s \in \mathcal{Q}(M)$.

When $Y_i = 0$, if j relays the message to u, the number of K_u^0 may increase by 1 (if u never received that message from other nodes); if it chooses not to relay, the information stored by u will not change. Therefore, choosing to relay is a dominant strategy to promote node u to reach a higher K_u^0. Since this strategy holds for all nodes in N_j, the final strategy of node j will be passing any path $s \in \mathcal{Q}(M)$.

In this way, we have proven rule 1 and rule 2. Next, we consider how node j's choice of Y_j. Based on the proof for rule 1 and 2, we know that relaying an incorrect message to u is a dominant strategy. Since node j can decide the value of Y_j, it should choose to transmit a message with $X = 0$ to node u. Since this strategy holds for all nodes in N_j, the final strategy of node j will be $Y_j = 0$, i.e. choose the incorrect observation of X, which is the proof of rule 3. □

Based on Theorem 1, we can now state the probability $\Pr\{K_1 < K | K_2 = i\}$ by

$$\Pr\{K_1 < K | K_2 = i\} = \begin{cases} \mathbb{I}\{n-i \geq K\}, & m < 2a, \\ |\bigcap_{i=1}^{s} L_i^c| \binom{n-m}{i}^{-1}, & m \geq 2a, \end{cases} \tag{4}$$

which completes the expression of $\Pr\{\hat{X} = X\}$ in (2).

B. Equilibrium of zero-sum game

Under the best response of the attacker, we can characterize the optimal threshold K^* for consensus and thus study the structure of the NE.

Theorem 2: (Best response for operator). Under the dominant strategy for the attacker, the operator's best response σ_o^* is as follows.

1) If $m < l^*_{\min}$, then there exists a unique $K^* \in (m, l^*_{\min}]$ such that $\sigma_o^* = K^*$ and $\Pr\{\hat{X} = X\} > 0$.
2) If $m \geq l^*_{\min}$, then $\sigma_o^* = \{1, 2, ..., n\}$, with $\Pr\{\hat{X} = X\} = 0$.

Proof.

Without loss of generality, suppose the true value of X is 1. Due to the transmission rules loyal nodes and Theorem 1, each incorrect message can be received and stored by every node, resulting in each node having at least m signatures on $X = 0$, i.e. $K_i^0 \geq m,\ i \in V$. If K is set to a value $k \leq m$, each node will observe an incorrect k-consensus, i.e. $Z^0 = n$. However, due to Theorem 1, the Byzantine nodes will not store the correct messages of X, i.e. $\mathbb{I}\{|K_j^1| \geq K\} = 0,\ j \in M$. In this way, the maximum possible number of Z^1 is $n-m$, resulting $\hat{X} = 0 \neq X$, i.e. the operator unable to reach a correct estimation. Therefore, we have $\Pr\{\hat{X} = X\} = 0$ if $K \leq m$.

Due to Theorem 1, the Byzantine nodes won't transmit the correct messages of X. In this way, the maximum possible K_1 is $l^*_{\min}$, i.e. $K_1 \leq l^*_{\min}$. If K is set to a value $k > l^*_{\min}$, the system operator will be unable to achieve any correct k-consensus, i.e. $Z^1 = 0$ and thus unable to reach a correct estimation. Therefore, we have $\Pr\{\hat{X} = X\} = 0$ if $K > l^*_{\min}$.

Based on the reasoning above, if $m < l^*_{\min}$, we have $m < K^* \leq l^*_{\min}$, or the system operator can unilaterally change

the value of K for a better payoff; if $m \geq l^*_{\min}$, we have $\Pr\{\hat{X} = X\} = 0$ for any $1 \leq K \leq n$, where the system operator can choose any $1 \leq K \leq n$ without unilaterally deviating to receive a better payoff. □

Based on Theorem 2, we know that only when $m < l^*_{\min}$, can the system operator possibly obtain the correct estimation. We use m^* as the maximum number of Byzantine nodes allowed in the network to guarantee a positive $\Pr\{\hat{X} = X\}$. By substituting the expression of $l^*_{\min}$, we can solve m^* under different values of a:

Proposition 1: (Resiliency score). The minimal number m^* of Byzantine nodes that ensures $\Pr\{\hat{X} = X\} = 0$ is

$$m^* = \begin{cases} \lceil \sqrt{an} \rceil - 1, & a < n/4, \\ \lceil n/2 \rceil - 1, & n/4 \leq a < n/2. \end{cases}$$

Proof.

In the case of $a \geq n/4$, we have $l^* = n - m$ and $s = 1$ since $m < n/2 \leq 2a$.

$$\begin{aligned} m &< l^*_{\min} = n - m \\ m &< n/2. \end{aligned}$$

That is to say, if the connectivity a of the ring is sufficiently large, the network can guarantee a positive $\Pr\{\hat{X} = X\}$ when the number of Byzantine nodes is less than half, i.e. $m^* = \lceil n/2 \rceil - 1$.

In the case of $a < n/4$:

If $m < 2a$, we have $l^* = n - m$ and $s = 1$. In this way, a positive $\Pr\{\hat{X} = X\}$ is guaranteed because $m < 2a < n/2 < l^*_{\min} = n - m$.

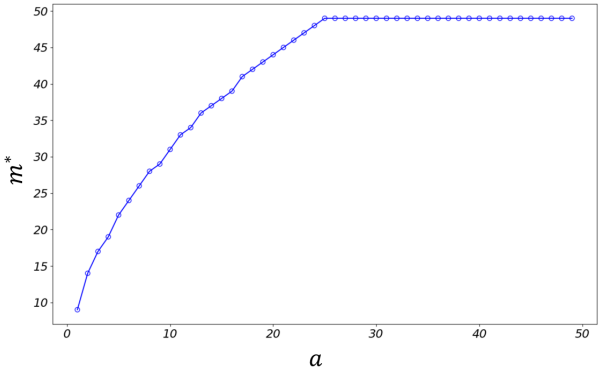
If $m \geq 2a$, we have $s = \lfloor m/a \rfloor$ and $l^*_{\min} = \lceil (n-m)/s \rceil$. In such case,

$$\begin{aligned} m &< l^*_{\min} = \lceil (n-m)/s \rceil \\ m + 1 &\leq \lceil (n-m)/s \rceil < (n-m)/s + 1 \\ m &< (n-m)/\lfloor m/a \rfloor < (n-m)/(m/a - 1) \\ m^2/a - m &< n - m \\ m &< \sqrt{an} \end{aligned}$$

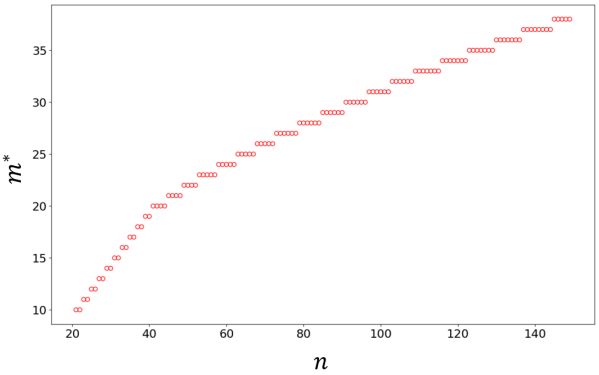
which gives an upper bound of m when $a < n/4$. In such case, we have $m^* = \lceil \sqrt{an} \rceil - 1$ □

We describe the resiliency of the ring against Byzantine nodes by the value of m^*. From Proposition 1, we find that as a increases, the resiliency of the system improves, i.e. it can accommodate a greater number of Byzantine nodes while guaranteeing a positive $\Pr\{\hat{X} = X\}$. The numerical simulation results are shown in Fig. 3. In reality, connectivity a is influenced by a variety of factors, including budget constraints, technological limitations, distances, white noise, disturbances, and other factors that prevent a from increasing freely. Therefore, there exists a tradeoff between resiliency and cost.

According to Theorem 1, we can derive the attacker's optimal strategy σ^*_a under any $1 \leq K \leq n$; according to Theorem 2, we can obtain the range of optimal strategy $\sigma^*_o = K^*$ for the system operator. For any k within that range, we can obtain the value of $\Pr\{\hat{X} = X; (k, \sigma^*_a)\}$ through (2). The maximum of these probabilities is the Nash equilibrium of the model under fixed values of n, m, and a, where a unilateral deviation by either side will not be profitable. In other words, for any given $R_{n,a}$, the strategy set (σ^*_o, σ^*_a) will form a pure strategy Nash Equilibrium.



(a) m^* under different connectivity a when $n = 100$.



(b) m^* under different n when $a = 10$.

Fig. 3: m^* under different n and a

IV. Conclusion and Future Work

In this paper, we present a zero-sum game model for a ring lattice sensing network under Byzantine attacks. We analyze the Nash equilibrium of the game and utilize its equilibrium structure to evaluate the network's resiliency. Our findings offer valuable insights into designing more robust distributed systems and enhancing network security.

Moving forward, we plan to expand our research by examining the equilibria of the original game model in more complex network structures, such as general regular networks and ad hoc networks. Investigating the existence of Nash equilibrium and assessing the network's resiliency in these structures will then be important research topics. We will also expand the conclusions on binary state estimation to multi-ary or continuous states to fit in more situations. Besides, we will investigate dynamic models where the set of Byzantine nodes can change over time, which could better capture the evolving cyber threats.

Acknowledgments

The authors appreciate the valuable inputs from the anonymous reviewers and the editor. Yufan Wu at SJTU also

contributed to the modeling part.

REFERENCES

[1] L. Bakule, "Decentralized control: An overview," *Annual reviews in control*, vol. 32, no. 1, pp. 87–98, 2008.

[2] P. D. Hines, S. Blumsack, and M. Schläpfer, "Centralized versus decentralized infrastructure networks," *arXiv preprint arXiv:1510.08792*, 2015.

[3] S. Y. Nikouei, R. Xu, Y. Chen, A. Aved, and E. Blasch, "Decentralized smart surveillance through microservices platform," in *Sensors and Systems for Space Applications XII*, vol. 11017. SPIE, 2019, pp. 160–175.

[4] D. Kingston, R. W. Beard, and R. S. Holt, "Decentralized perimeter surveillance using a team of uavs," *IEEE Transactions on Robotics*, vol. 24, no. 6, pp. 1394–1404, 2008.

[5] M. Castro, P. Druschel, A.-M. Kermarrec, and A. I. Rowstron, "Scribe: A large-scale and decentralized application-level multicast infrastructure," *IEEE Journal on Selected Areas in communications*, vol. 20, no. 8, pp. 1489–1499, 2002.

[6] Y.-J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information infrastructure for smart grid," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 58–65, 2010.

[7] G. G. Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. Reiter, D.-A. Seredinschi, O. Tamir, and A. Tomescu, "SBFT: A scalable and decentralized trust infrastructure," in *2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)*. IEEE, 2019, pp. 568–580.

[8] A. Y. Chen and F. Peña-Mora, "Decentralized approach considering spatial attributes for equipment utilization in civil engineering disaster response," *Journal of computing in civil engineering*, vol. 25, no. 6, pp. 457–470, 2011.

[9] Y. Bae, Y.-M. Joo, and S.-Y. Won, "Decentralization and collaborative disaster governance: Evidence from south korea," *Habitat international*, vol. 52, pp. 50–56, 2016.

[10] A. Beg, A. R. Qureshi, T. Sheltami, and A. Yasar, "Uav-enabled intelligent traffic policing and emergency response handling system for the smart city," *Personal and Ubiquitous Computing*, vol. 25, pp. 33–50, 2021.

[11] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[12] B. Awerbuch, R. Curtmola, D. Holmer, and C. Nita-rotaru, "Mitigating byzantine attacks in ad hoc wireless networks," 07 2004.

[13] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *Concurrency: the works of leslie lamport*, 2019, pp. 203–226.

[14] G. S. Veronese, M. Correia, A. N. Bessani, L. C. Lung, and P. Verissimo, "Efficient byzantine fault-tolerance," *IEEE Transactions on Computers*, vol. 62, no. 1, pp. 16–30, 2011.

[15] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-scalable byzantine fault-tolerant services," *ACM SIGOPS Operating Systems Review*, vol. 39, no. 5, pp. 59–74, 2005.

[16] L. Su and S. Shahrampour, "Finite-time guarantees for byzantine-resilient distributed state estimation with noisy measurements," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3758–3771, 2019.

[17] ——, "Finite-time guarantees for byzantine-resilient distributed state estimation with noisy measurements," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3758–3771, 2019.

[18] Y. Wu and X. He, "Secure consensus control for multiagent systems with attacks and communication delays," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 136–142, 2017.

[19] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3209–3223, 2014.

[20] Y. Chen, S. Kar, and J. M. Moura, "Resilient distributed estimation: Sensor attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3772–3779, 2018.

[21] 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, 2011.

[22] C. Litsas, A. T. Pagourtzis, and D. Sakavalas, "The byzantine generals problem in generic and wireless networks," *Applications of Mathematics and Informatics in Science and Engineering*, pp. 405–415, 2014.

[23] N. H. Vaidya, "Iterative byzantine vector consensus in incomplete graphs," in *Distributed Computing and Networking: 15th International Conference, ICDCN 2014, Coimbatore, India, January 4-7, 2014. Proceedings 15*. Springer, 2014, pp. 14–28.

[24] B. Kailkhura, S. Brahma, and P. K. Varshney, "Data falsification attacks on consensus-based detection systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 145–158, 2016.

[25] A. Mitra and S. Sundaram, "Byzantine-resilient distributed observers for lti systems," *Automatica*, vol. 108, p. 108487, 2019.

[26] Y. Li and C. Yu, "Game of the byzantine generals on time-varying graphs," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 16 958–16 963, 2020.