A Decentralized Multi-ruling Arbiter for Cyberspace Mimicry Defense

Congqi Shen*
cyberspace security
Zhejiang Lab
Hangzhou 310027, China
shencq@zhejianglab.com

Shuangxi Chen
Polytechnic Institute
Zhejiang University
Hangzhou 310027, China
abelchen@zju.edu.cn

Chunimng Wu
Computer Science and
Technology
Zhejjiang University
Hangzhou, 310027, China
wuchunming@zju.edu.cn

***Abstract*—Cyberspace Mimicry Defense (CMD) has been widely used to achieve intrusion prevention against unknown system vulnerabilities or backdoors. The multi-ruling arbiter is a key part in CMD. This paper focuses on the problem of multi-ruling arbiter under data injection attack from the perspective of attacker and defender. We build a decentralized multi-ruling arbiter model for arbitration and introduced a standard iteration process to achieve consensus without attackers. We describe two data injection attack models for decentralized multi-ruling arbiter, namely random data injection attack and stealthy data injection attack. Further, we characterize the negative effect of the data injection attack on the performance of multi-ruling correctness. In order to mitigate the negative effect of random data injection attack, we propose a reliable multi-ruling arbitration approach based on adaptive threshold. By cutting future communication with the malicious neighbor, the decentralized multi-ruling arbiter is robust against random data injection attacks. Simulation results show that the proposed arbitration approach can effectively defend against random data injection attacks.**

Keywords—mimic defense; multi-ruling arbitration; data injection attacks

I. INTRODUCTION

The cyberspace of industrial networks is vulnerable to many kinds of malicious attacks, especially in the case of an insider attacker. Since the cyberspace of industrial network is increasingly open, no one can guarantee that cyberspace is absolutely secure. The key infrastructure may contain malicious code, which leads to attacks using backdoors and holes in the network. Therefore, it is significant to research the security threats and its mitigations in the cyberspace of industrial networks [1].

A. A prior art on DHR and multi-ruling arbiter in Cyberspace Mimicry Defense (CMD)

Current defense systems are based on specific characteristics of threats, such as attack sources, manners, and techniques. These defense systems are effective only for known kinds of attacks because they are static and determinate without diversity. Therefore, Dynamic Heterogeneous Redundancy(DHR) is proposed to construct a dynamic architecture [2].

Based on the DHR theory, some researchers come up with CMD to deal with the threats of unknown cyberattacks[3-5]. By constructing dynamic, random, and diverse heterogeneous components, CMD can effectively resist unknown system vulnerabilities and backdoors. A mimicry defense system generates dynamic scheduling policies and arbitration strategies. An input agent selects heterogeneous functional equivalents to respond independently to the external requests according to the dynamic scheduling policy. The heterogeneous functional equivalents send the results to the multi-ruling arbiter and the arbiter computes a final result using arbitration strategy. Generally speaking, multi-ruling arbiter is prominent for a CMD system.

Some researchers have studied multi-ruling arbiter in recent years. The framework of DHR and the basic concept of mimicry defense was introduced in [6]. From the perspective of theoretical analysis, the defensive performance of CMD was analyzed in [7] and the redundancy based ruling performance was investigated using Markov chain in [8]. Authors in [9] proposed mimicry Markov model to research the relation among different states and the reliability of the system. From the perspective of engineering applications, the vulnerability of the grid was studied using petri network in [10]. Similar work is also implemented in [11,12]. To the best of our knowledge, the attack and its mitigation of multi-ruling arbiter are not addressed in current work.

In current mimicry system, only one arbiter is implemented and is achieved through software, so the whole system will be compromised if the arbiter is attacked. One can conclude that the current mimicry system is effective under a strong assumption that the arbiter will not be attacked.

In this paper, we study the problem of multi-ruling arbiter under data injection attack from the perspective of attacker and defender. The main contributions of this paper is summarized as follows:

First, a decentralized multi-ruling arbiter model for arbitration is constructed, where sub-arbiters exchange their local results with its neighbors and the target of the

This work was partly supported by Major Scientific Project of Zhejiang Lab (No. 2018FD0ZX01), National Key Research and Development Program of China(2016YFB0800102, 2016YFB0800201，2017YFB0803205), the Key Research and Development Program of Zhejiang Province (2017C01064, 2018C03052), and the Fundamental Research Funds for the Central.

978-1-7281-1244-2/19/$31.00 ©2019 IEEE

decentralized multi-ruling arbiter is to converge to a consistent global result after several iterations. We prefer a decentralized construction as it requires a lower cost compared with a centralized one.

Second, we describe two data injection attack models for decentralized multi-ruling arbiter, namely random data injection attack and stealthy data injection attack. Further, we characterize the negative effect of the data injection attack on the performance of multi-ruling correctness.

Third, a reliable multi-ruling arbitration approach based on adaptive threshold is proposed to defend against random data injection attacks. A sub-arbiter will determine the type of its neighbor (normal or malicious) by comparing the local result of itself and its neighbor with an adaptive threshold which is adjusted according to the local results of its neighbors. By cutting future communication with the malicious neighbor, the multi-ruling arbiter is robust against random data injection attacks.

The remainder of this paper is organized as follows. The system model and decentralized multi-ruling arbiter model are introduced in Section II. A standard iteration process without attackers is also introduced in this section. In Section III, two data injection attack models and the negative effect of the data injection attack are addressed. To defend against random data injection attack, a reliable multi-ruling arbitration approach based on adaptive threshold is proposed in Section IV. Numerical results and discussions are given in Section V. Section VI concludes the paper.

II. PRELIMINARIES

A. System model

As shown in Fig. 1, a typical industrial network includes remote controller, gateway and some actuators, etc. The actuators in the lowest layer gather data, make a local decision and pass the decision to the higher layer. In order to guarantee the security of the actuators, we construct heterogeneous functional equivalent executor to make a local result independently and send to an arbiter. The arbiter computes a global result.

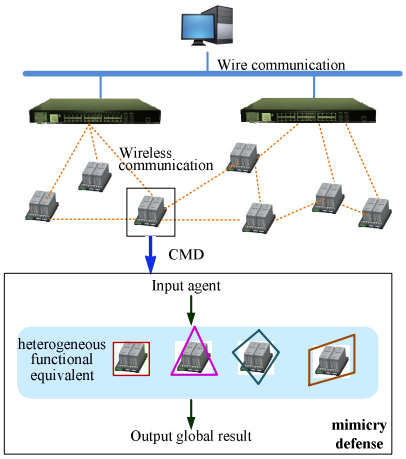


Fig. 1. A typical industrial network.

Since the probability of heterogeneous executors is independent to each other and the logical architecture and code is totally different, the probability of producing commonality vulnerabilities and defects can be assumed as zero. This is based on the theory introduce in [6].

B. Decentralized multi-ruling arbiter model

As shown in Fig. 2, a typical mimicry defense model consists of input agent, heterogeneous execution set, and a multi-ruling arbiter. Heterogeneous execution set consists of M heterogeneous executors with functional equivalent but different algorithms implementation. The decentralized multi-ruling arbiter model proposed in this work is shown in Fig. 3. M heterogeneous executors, namely E_1, E_2, E_3,…, E_M , receive input data and make local results independently. The decentralized multi-ruling arbiter can be regarded as undirected graph and consists of N sub-arbiters. Two connected sub-arbiters can exchange data with each other. The working process of decentralized multi-ruling arbiter can be described as follows. First, sub-arbiters collect all the results from heterogeneous execution set. Second, sub-arbiters operate own ruling algorithm and obtain local results. Third, sub-arbiters exchange local results between directly connected ones and converge to a global consistent result after several iterations.

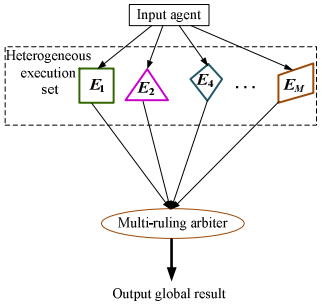


Fig. 2. A typical mimicry defense model.

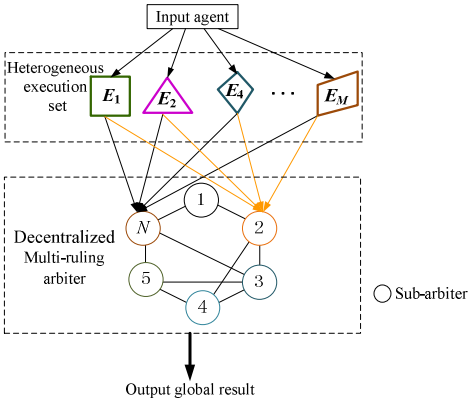


Fig. 3. Decentralized multi-ruling arbiter model.

Let $\mathcal{G}=(\mathcal{N},\mathcal{E})$ be the construction of the decentralized multi-ruling arbiter, where $\mathcal{N}=\{i|i=1,2,\ldots,N\}(N\geq 3)$ denotes the set of all the sub-arbiters, $\mathcal{E}\in\mathcal{N}\times\mathcal{N}$ denotes the set of all the edges. In a multi-ruling arbiter, any two sub-arbiters

can be connected through a path. A path is a sequence of the number of sub-arbiters 1,2,…,*q*,…,*Q* ($Q \geq 3$),satisfying $(q,q+1) \in \mathcal{E}$. Only those sub-arbiters connected directly can exchange current local results. Sub-arbiter *i* and *j* is considered as connected directly if they satisfy $(i,j) \in \mathcal{E}$ and $i \neq j$. The set of neighbors of sub-arbiter is denoted as $\mathcal{N}_i = \{j \mid (i,j) \in \mathcal{E}\} \subset \mathcal{N}$ and $|\mathcal{N}_i|$ is the size of set $\mathcal{N}_i$. Let $\mathcal{L}$ be the Laplacian matrix of graph $\mathcal{G}$ and the *i*th row *j*th column element of the matrix is denoted as

$$l_{ij} = \begin{cases} |\mathcal{N}_i| & i = j \\ -1 & i \neq j, j \in \mathcal{N}_i \\ 0 & otherwise \end{cases} \quad (1)$$

A sub-arbiter first collects the local results of heterogeneous executor and obtain an initial local results according to the loaded local ruling algorithm. Second, the sub-arbiter exchanges its current local results with all the neighbors. Third, the sub-arbiter updates its local result. Let $x_i(k)$ be the local result of sub-arbiter *i* at *k*th iteration. At *k*th (*k*=1,2,3,…) iteration, the update process of sub-arbiter *i* is written as

$$x_i(k) = w_{ii} x_i(k-1) + \sum_{j \in \mathcal{N}_i} w_{ij} x_j(k-1) \quad (2)$$

where *i*,*j*=1,2,…,*N*, w_{ij} are some weight and remains same during the iteration process.

Similarly, all the sub-arbiters exchange their own results with their neighbors and obtain the results of neighbors to update their own local results. At the next iteration, sub-arbiters exchange results again and obtain the information two hops far from themselves. After several iterations, all sub-arbiters reaches the same results and the decentralized multi-ruling arbiter is converged and satisfies $\bar{x}_1 = \bar{x}_2 = ... = \bar{x}_i = ... = \bar{x}_N$, where $\bar{x}_i$ is the global results. Let $\mathbf{x}(k) = \left[x_1(k), x_2(k), ..., x_N(k)\right]^T$ be the results vector at *k*th iteration. The standard iteration process described above can be written in a matrix manner as

$$\mathbf{x}(k) = \mathbf{W}\mathbf{x}(k-1) \quad (3)$$

III. Attack Strategy for the Decentralized Multi-Ruling Arbiter

In this paper, we consider data injection attacks. An attacker may either modify a local result at update step, or inject a fabricated value at exchange step, or the attack may happen in both the updating step or exchange step. This attack may be dangerous because it can cause long-term impact on the decentralized multi-ruling arbiter. Only one attacker that transmits a constant value at one iteration can make the whole network diverge or converge to a falsified value.

In this paper, we assume that the decentralized multi-ruling arbiter is not dominated by the malicious sub-arbiters and the communication link is reliable. We also assume that the network topology remains unchanged during the iteration process. Data injection attacker injects random values into its neighbors at each time-step as long as it can lead the decentralized multi-ruling arbiter to a wrong global results. Let $e_i(k)$ be the additive malicious data injected to sub-arbiter *i* at time-step *k*. Sub-arbiter *i* is said to be malicious if $e_i(k)$ is nonzero for at least one time-step *k*. When the decentralized multi-ruling arbiter contains attackers, the iteration process can be written as

$$x_i(k) = e_i(k-1) + w_{ii} x_i(k-1) + \sum_{j \in \mathcal{N}_i} w_{ij} x_j(k-1) \quad (4)$$

Let $\mathbf{e}(k) = \left[e_1(k), e_2(k), ..., e_N(k)\right]^T$ be the vector composed by the additive malicious data. Then we get the iteration algorithm with some malicious sub-arbiters

$$\mathbf{x}(k) = \mathbf{W}\mathbf{x}(k-1) + \mathbf{e}(k) \quad (5)$$

Attackers can choose any nonzero vector as $\mathbf{e}(k)$ and $\mathbf{e}(k)$ is named as attack vector.

Theorem 1: Malicious arbiter inject a nonzero attack vector will cause arbiter diverge or converge to a wrong global result.

Proof: If no attacker invaded in the decentralized multi-ruling arbiter, the global result can be written as

$$\mathbf{x}(k) = \mathbf{W}\mathbf{x}(k-1) = \mathbf{W}^2\mathbf{x}(k-2) = ... = \mathbf{W}^k\mathbf{x}(0)$$

When the decentralized multi-ruling arbiter suffers data injection attacks, at time-step *k*, using (5), the global result can be written as

$$\mathbf{x}(k) = \mathbf{W}\mathbf{x}(k-1) + \mathbf{e}(k)$$

The equation above can be rewritten as

$$\mathbf{x}(k) = \mathbf{W}^k\mathbf{x}(0) + \sum_{i=0}^{k-1} \mathbf{W}^i\mathbf{e}(k-i) \quad (6)$$

It is clear that two cases exist in (6). We analyze each case in detail as follows.

Case 1: the attack vector $\mathbf{e}(k)$ satisfies $\mathbf{e}(k) = \begin{cases} \mathbf{W}\mathbf{c}(1) & k = 1 \\ \mathbf{0} & k \neq 1 \end{cases}$, where $\mathbf{c}(1)$ is a nonzero vector.

In this case, (6) can be rewritten as

$$\mathbf{x}(k) = \mathbf{W}^k\left[\mathbf{x}(0) + \mathbf{e}(1)\right] \quad (7)$$

This means the arbiter is converged to a wrong consensus value and the global result is dominated by attacker.

Case 2: the attack vector $\mathbf{e}(k)$ dose not satisfy $\mathbf{e}(k) = \begin{cases} \mathbf{W}\mathbf{c}(1) & k = 1 \\ \mathbf{0} & k \neq 1 \end{cases}$.

We can know from (6), the arbiter can not converge to a consistent result.

Above all, when the decentralized multi-ruling arbiter suffers attacks, it may not converge normally or converge to a wrong global results. According to the discussion above, we introduce two attack models as follows.

Attack model 1: Random data injection attack model:

Attackers have no prior knowledge of the decentralized multi-ruling arbiter and inject random attack vector to cause a divergence.

Attack model 2: Stealthy data injection attack model:

Attackers know the construction of multi-ruling arbiter and inject a designed attack vector to cause a converged global result dominated by the attackers.

IV. A RELIABLE MULTI-RULING ARBITRATION APPROACH BASED ON ADAPTIVE THRESHOLD

For a decentralized multi-ruling arbiter, it is important to identify the type of sub-arbiter and exclude the malicious sub-arbiters from the iteration process. Hence, we mainly focus on the malicious sub-arbiter identification method in this section.

We propose a malicious sub-arbiter detection method based on adaptive local threshold. A sub-arbiter can identify the type of its neighbors (normal or malicious) using an adaptive threshold. According to the standard iteration process, the maximum state of the network is decreasing while the minimum state is increasing until reaching consensus, so the difference among a normal sub-arbiter and its normal neighbors will shrink to zero. As for a malicious sub-arbiter, the gap between its local result and its neighbors' results will become larger until the multi-ruling arbiter cannot converge.

The main idea of the detection algorithm is to design a threshold at each sub-arbiter. However, it is likely to mistakenly judge a normal sub-arbiter with a relatively large deviation using a over strictly threshold. To avoid mistaking the normal sub-arbiter with large deviation, we enlarge the threshold and adapt the threshold with diminishing difference. We now detail the detection algorithm as follows.

Sub-arbiter i computes the differences between result of itself and its neighbors $\left|x_j(k)-x_i(k)\right|$ at each time-step to identify the nature of its neighbors. At the first time-step, the sub-arbiter calculates the threshold as follows which will allow all the neighbors participate in the iteration.

$$\lambda_i(1)=\max_{j\in\mathcal{N}_i}\left|x_i(1)-x_j(1)\right|$$

At the following iteration step k ($k\geq 2$), in order to adapt the detection threshold according to the shrinking difference between the neighbors, the estimates of the threshold value $\lambda_i(k)$ can be calculated below

$$\lambda_i(k)=\frac{\sum_{j\in\mathcal{N}_i}\left|x_j(k)-x_i(k)\right|}{\sum_{j\in\mathcal{N}_i}\left|x_j(k-1)-x_i(k-1)\right|}\lambda_i(k-1)$$

Sub-arbiter i calculates $\left|x_j(k)-x_i(k)\right|$ ($j\in\mathcal{N}$)using the results exchanged with neighbors and compare $\left|x_j(k)-x_i(k)\right|$ ($j\in\mathcal{N}$) with $\lambda_i(k)$. A neighbor j is said to be malicious if $\left|x_j(k)-x_i(k)\right|>\lambda_i(k)$. The adaptive threshold based defense technique is given in algorithm 1.

Algorithm1 The multi-ruling arbitration approach based on adaptive threshold

Input: initial number of sub-arbiters N, the decentralized multi-ruling arbiter $\mathcal{G}=(\mathcal{N},\mathcal{E})$

(1) **for** i=1:N **do**

(2) $\lambda_i(1)=\max_{j\in\mathcal{N}_i}\left|x_i(1)-x_j(1)\right|$

(3) **end for**

(4) **while** $\mathbf{x}(k)$ do not reach a consensus

(5) **for** i=1:N **do**

(6) $\lambda_i(k)=\frac{\sum_{j\in\mathcal{N}_i}\left|x_j(k)-x_i(k)\right|}{\sum_{j\in\mathcal{N}_i}\left|x_j(k-1)-x_i(k-1)\right|}\lambda_i(k-1)$

(7) **for** $j\in\mathcal{N}_i$

(8) **if** $\left|x_j(k)-x_i(k)\right|>\lambda_i(k)$

(9) $w_{ij}=0$

(10) **end if**

(11) **end for**

(12) $x_i(k)=w_{ii}x_i(k-1)+\sum_{j\in\mathcal{N}_i}w_{ij}x_j(k-1)$

(13) **end for**

(14) **end while**

Output: $\mathbf{x}(k)$

According to the consensus algorithm, the maximum state of the network is monotonically decreasing while the minimum state is monotonically increasing. The difference between a normal sub-arbiter and its neighbors gradually decreases to zero, so the threshold gradually decreases to zero. A neighbor is assumed to be a malicious one and will be eliminated if the difference is too large.

V. SIMULATION RESULTS

In this section, we present a numerical example to validate the performance of two attack models presented in Section III and the reliable arbitration approach proposed in Section IV by comparing with standard iteration process.

We consider the decentralized multi-ruling arbiter is attacked by random data injection attack described in Section III, and then perform the standard iteration process and our scheme to the decentralized multi-ruling arbiter. The reliability of the proposed multi-ruling arbitration approach based on adaptive threshold is validated by contracting the results under two circumstances.

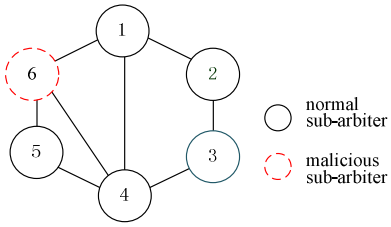
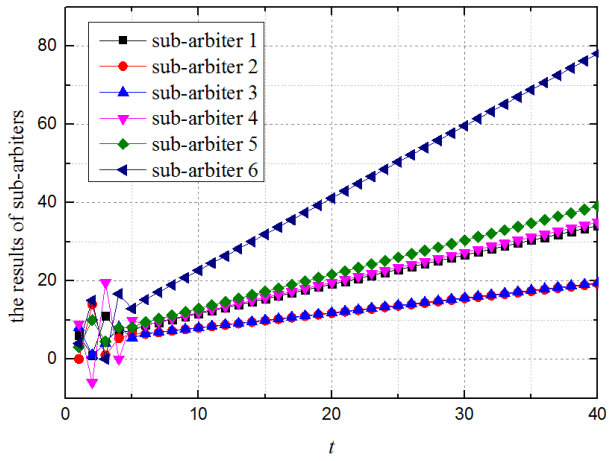
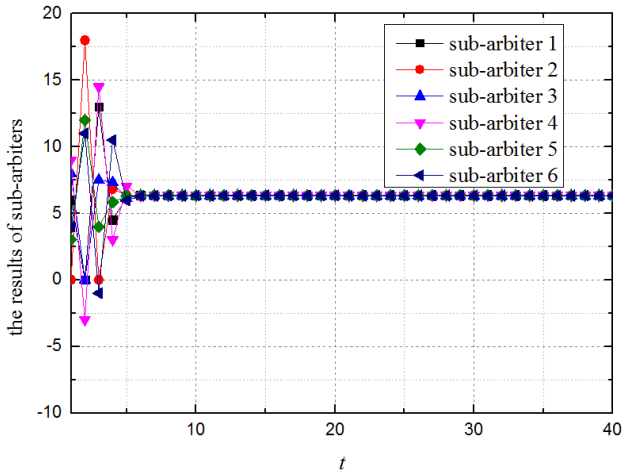


Fig. 4. A decentralized multi-ruling arbiter composed of five normal sub-arbiters and one malicious sub-arbiter

The construction of the decentralized multi-ruling arbiter considered in our simulation is shown in Fig. 4 where 6 sub-arbiters are doing multi-ruling arbitration. The sub-arbiter set is $\mathcal{N}=\{1,2,\ldots,6\}$ and the initial value $\mathbf{x}(0)=\{6,0,8,9,3,4\}$. The decentralized multi-ruling arbiter will converge to 5 if there is no attacker.



(a) sub-arbiter 6 suffers random data injection attack



(b) sub-arbiter 6 suffers stealthy data injection attack

Fig. 5. The local results of 6 sub-arbiters over time when sub-arbiter suffers data injection attack

Fig. 5 shows the negative effect of data injection attack. Fig. 5(a) and (b) shows the local results of sub-arbiters over time when sub-arbiter 6 suffers random data injection attack and stealthy data injection attack, respectively. One can find from Fig. 5(a) that when random data injection attack happens, the local results of all the sub-arbiters become larger and larger and the local results of sub-arbiter 6 increases fastest. The malicious data injected by sub-arbiter 6 is transmitted to its neighbors and the negative effect is spread throughout the network. This also shows that it is feasible to use the difference between a sub-arbiter and its neighbor as an indicator to show the type of a sub-arbiter. From Fig. 5(b), we observe that when stealthy data injection attack happens, all the sub-arbiters converge to a consensus, but to a wrong global result. One can find that a carefully designed malicious data may lead to a wrong consensus designed by attackers.

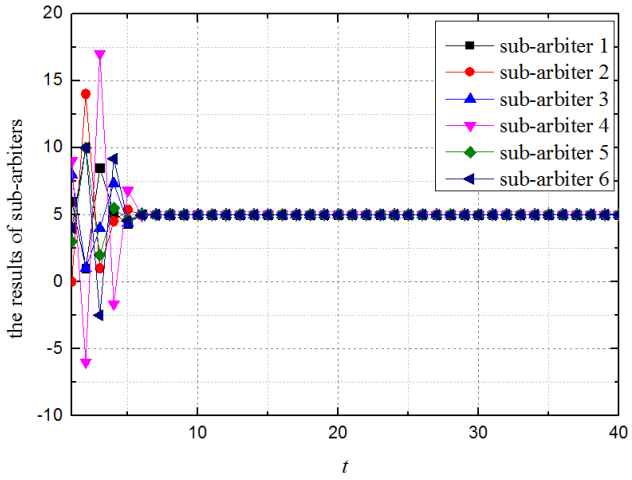
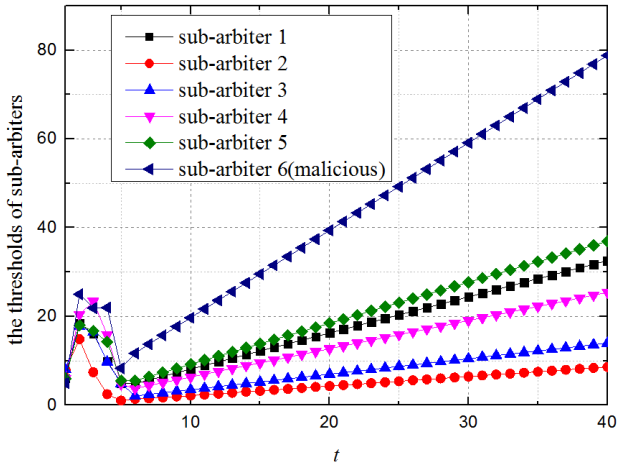
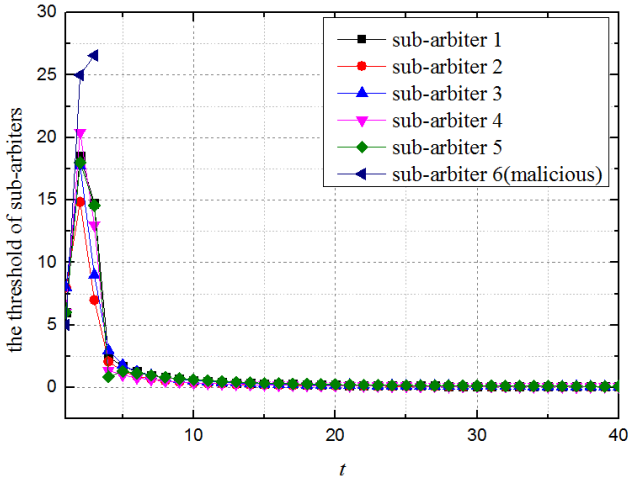


Fig. 6. The local results of 6 sub-arbiters over time under random data injection attack when the algorithm 1 is used suffers data injection attack

Fig. 6 shows the local results of sub-arbiters over time under random data injection attack when the algorithm 1 is used. One can find that all the sub-arbiters converge to the correct global result though sub-arbiter 6 is attacked by random data injection attacks.



(a) sub-arbiter 6 suffers random data injection attack



(b) the reliable multi-ruling arbitration approach based on adaptive threshold is used

Fig. 7. The thresholds of 6 sub-arbiters over time under different circumstances

Fig. 7 shows the thresholds of 6 sub-arbiters over time when random data injection attack happens and when algorithm 1 is used, respectively. One can find from Fig. 7(a) that when random data injection attack happens, the threshold of all the sub-arbiters increases and sub-arbiter 6 increases fastest This agrees with Fig. 5(a). By using Algorithm 1, sub-arbiter 6 is judged as a malicious one and it is eliminated after around 4 iterations. From Fig. 7(b), we observe that after malicious sub-arbiter is eliminated, the thresholds of all the sub-arbiters converge to zero, which is consistent to the theoretical analysis in Section IV.

VI. CONCLUSION

In this paper, we studied the problem of multi-ruling arbiter under data injection attack from the perspective of attacker and defender. We built a decentralized multi-ruling arbiter model for arbitration and introduced a consensus algorithm without attackers. we described two data injection attack models for decentralized multi-ruling arbiter, namely random data injection attack and stealthy data injection attack. Further, we characterized the negative effect of the data injection attack on the performance of multi-ruling correctness. In order to mitigate the negative effect of data injection attack, we proposed a reliable multi-ruling arbitration approach based on adaptive threshold. By cutting future communication with the malicious neighbor, the multi-ruling arbiter is robust against random data injection attacks.

In the future, we will investigate multi-ruling arbitration under stealthy data injection attack. An effective way should be addressed to mitigate the negative effect of stealthy data injection attack since it will lead the arbiter to a wrong result dominated by attackers.

ACKNOWLEDGMENT

This work was partly supported by Major Scientific Project of Zhejiang Lab (No. 2018FD0ZX01)，the Key Research and Development Program of Zhejiang Province(2017C01064，2018C03052), and the Fundamental Research Funds for the Central.

REFERENCES

[1] A. B. Berhe, and K. Kim, Industrial Control System Security Framework for Ethiopia, *ICUFN 2017*, Milan Italy, pp. 814-817, Jul. 2017.

[2] B. Ma, Z. Zhang, Security Research of Redundancy in Mimic Defense System, *2017 3rd IEEE International Conference on Computer and Communications*, Chengdu, China, pp. 2910-2914, Dec. 2017.

[3] J. Wu, Cyber Mimic Security Defense, *secrecy science and technology*, vol. 34, no. 10, pp. 4-9, Oct. 2014.

[4] X. Si, W. Wang, J. Zeng, B. Yang, G. Li, C. Yuan, F. Zhang, A Review of the Basic Theory of Mimic Defense, *Strategic Study of CAE*, vol. 18 no. 6, pp.1-7, Nov. 2016.

[5] X. Luo, Q. Tong, Z. Zhang, J. Wu, Mimic Defense Technology, *Strategic Study of Chinese Academy of Engineering*, vol. 18, no. 6, pp. 69-73, Dec. 2016.

[6] J. Wu, Research on Cyber Mimic Defense, *Journal of Cyber Security*, vol. 1, no. 4, pp. 1-10, Apr. 2016.

[7] Q. Ren, L. Xie, and J. Wu, Analysis of different anti-interference system models based on discrete time Markov chain, *Chinese Journal of Network and Information Security*, vol. 4, no. 4, pp. 30-37, Apr. 2018.

[8] W. Li, Z. Zhang, L. Wang, and J. Wu, The Modeling and Risk Assessment on Redundancy Adjudication of Mimic Defense, Journal of Cyber Security, vol. 3, no. 5, pp. 64-74, May 2018.

[9] X. Zhang, Z. Gu, S. Wei, and J. Shen, Markov game modeling of mimic defense and defense strategy determination, Journal on Communications, vol. 39, no. 10, Oct. 2018.

[10] X. Min, Y. Wu, and Y. Yan. Power System Fault Diagnosis Based on Improved Dynamic Adaptive Fuzzy Petri Nets and Back Propagation Algorithm. *Proceedings of the Csee*, vol. 35, no. 12, pp. 3008-2017, Dec. 2015

[11] G. Cai, B. Wang, and Y. Luo. A Model for Evaluating and Comparing Moving Target Defense Techniques Based on Generalized Stochastic Petri Net. Advanced Computer Architecture. *Springer Singapore*, vol. 10, no. 10, pp. 184-197, Oct. 2016

[12] S. Jian, Y. Meng, and S. Wang. Reliability and safety analysis of redundant vehicle management computer system. *Chinese Journal of Aeronautics*, vol. 26, no.5, pp. 1290-1302, May 2013.