Treat Detection based on System Credibility by Logging Analysis and Visualization

Wei Qiao, Youjun Bu, Yao Chen, Xiaoxiao Jiang, Bingbing Jiang

Purple Mountain Laboratories, China

Contact Email: jiangbingbing@pmlabs.com.cn

紫金山实验室
Purple Mountain Laboratories

IARIA

Biography

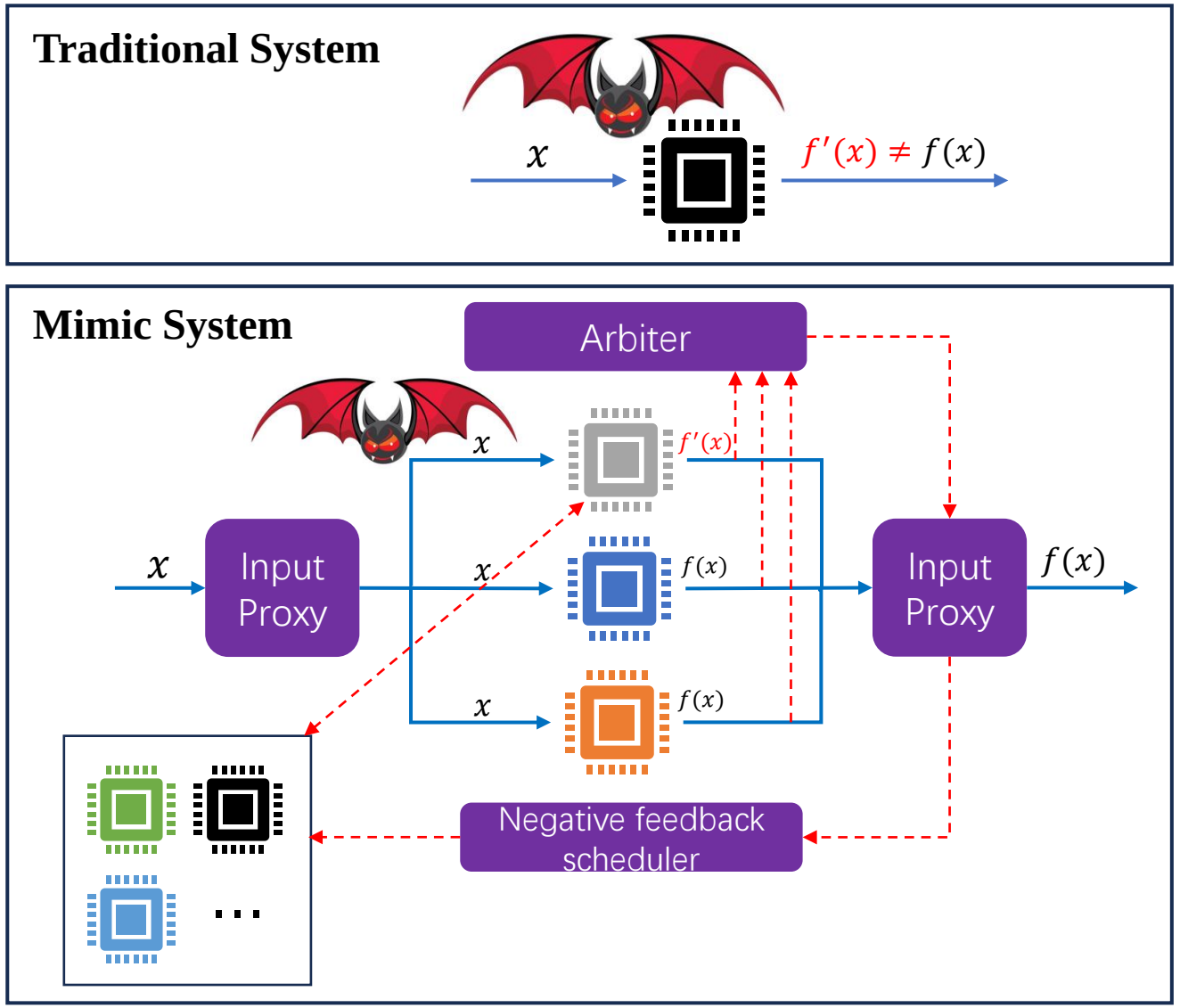
Bingbing Jiang received the PhD in computer science and technology from Nanjing University in 2021. He is currently a cybersecurity researcher in the department of endogenous safety and security, Purple Mountain laboratories.

His research interests include cybersecurity, endogenous safety and security, cyber resiliency and cryptography. A particular focus is homomorphic encryption (scheme-design and applications) and mimic defense (theoretical modeling and applications).

1. Aims and Contributions

- Aims of our paper:
  - Design a reasonable log analysis algorithm to enhance the credibility of outputs of mimic systems.
- Contributions of our paper:
  - A log analysis algorithm for credibility assessment through associating the suffered threat perturbations of systems with the credibility of their outputs.
  - Mitigation of unknown threats through combining our log analysis algorithm with the dynamic, heterogeneous and redundant properties of the system architecture.
  - A practical implementation of the log analysis algorithm on our developing mimic log cloud management system to verify the feasibility and effectiveness of the proposed approach.

2. Question

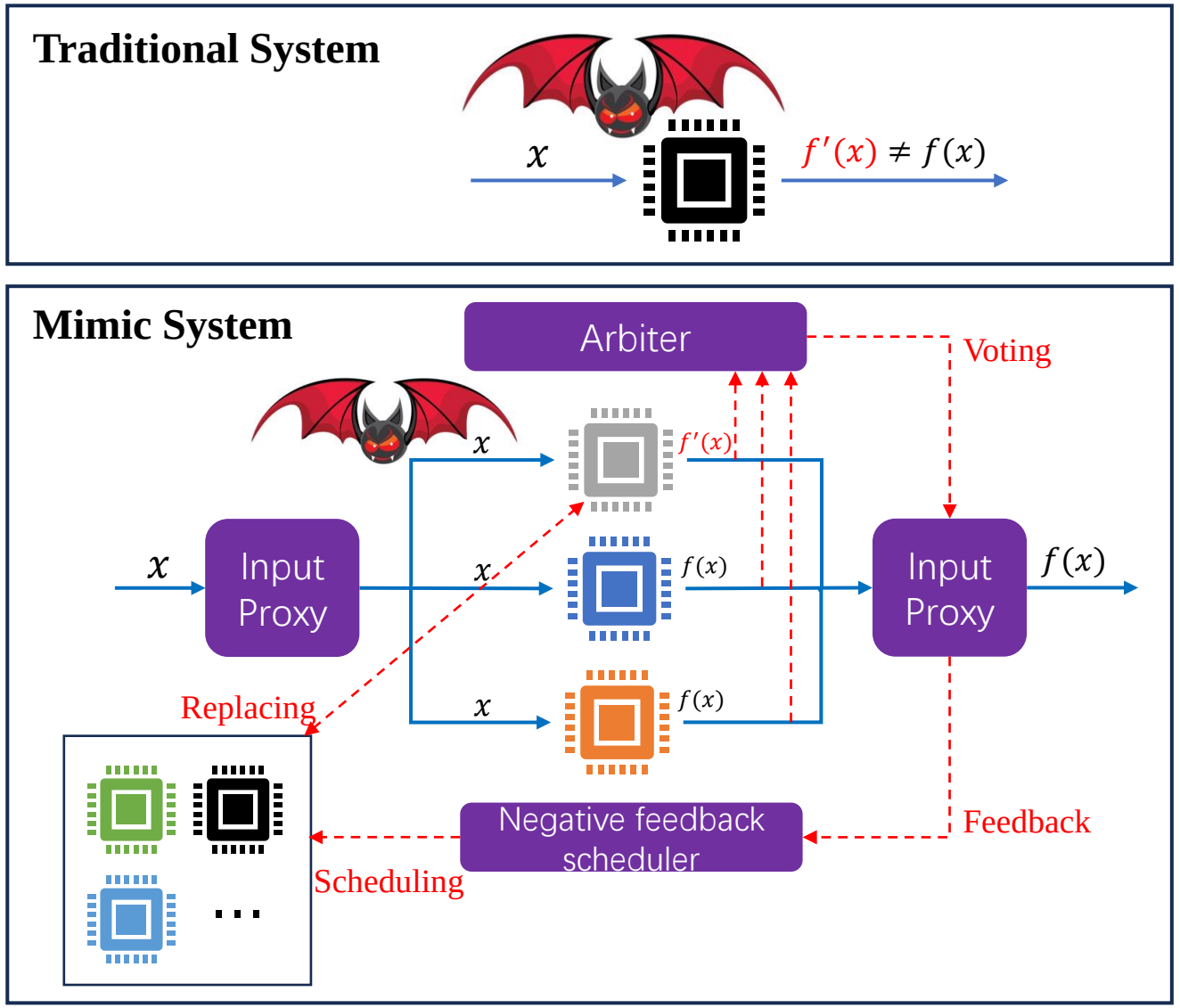


If adversaries find or acquire some vulnerabilities of / threats to the traditional system, it is easier to compromise.

Even if adversaries find or acquire some vulnerabilities of / threats to the mimic system, the vulnerabilities or threats are not possible to valid for all executors at the same time. Because these executors are heterogeneous and functionally equivalent.

However, ...

2. Question



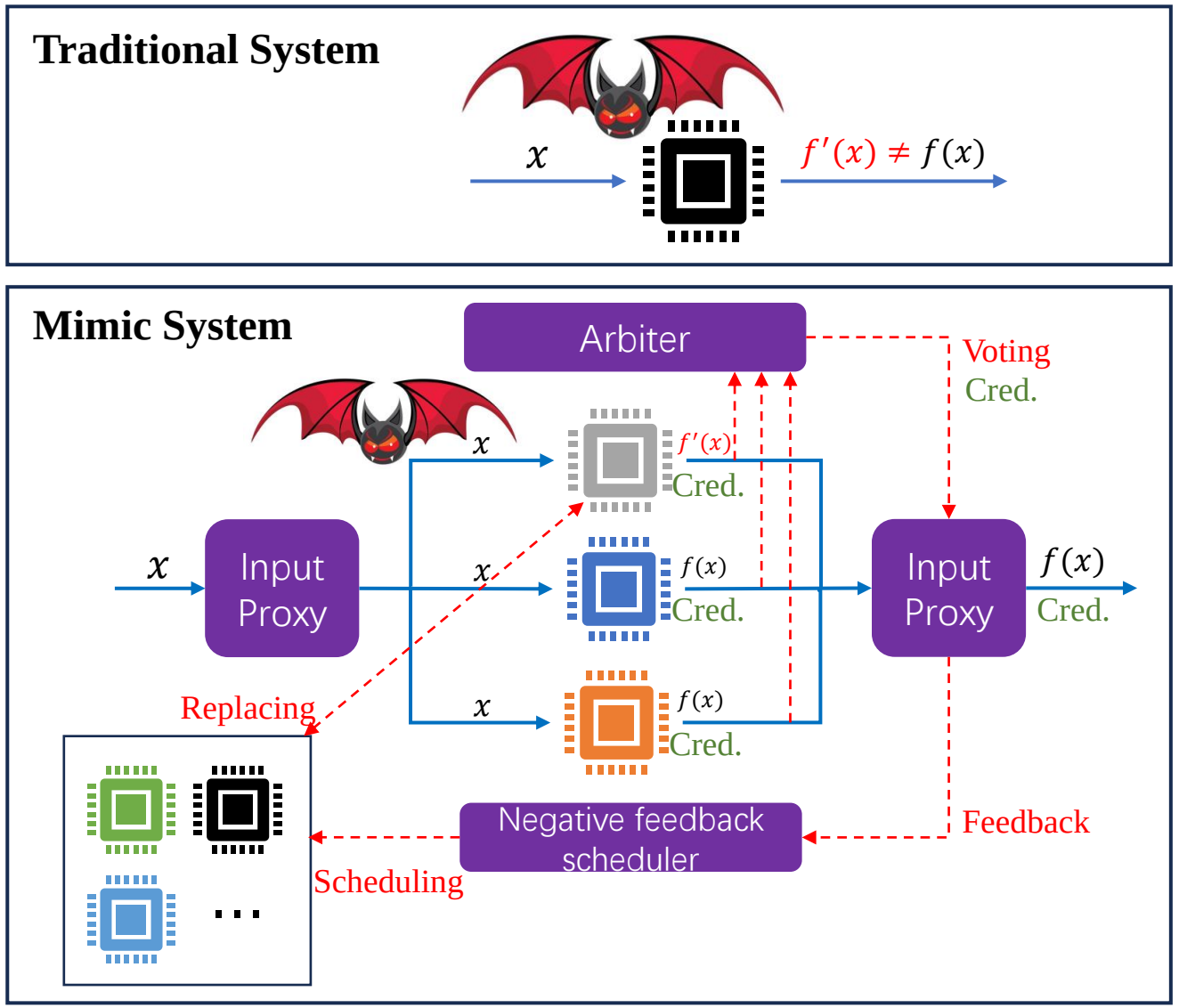
If adversaries find or acquire some vulnerabilities of / threats to the traditional system, it is easier to compromise.

This effect requires a credible adjudication algorithm to support because the output of the arbiter has a great impact on the final result.

Currently, the most used adjudication algorithm is majority voting.

Therefore, ...

2. Question



If adversaries find or acquire some vulnerabilities of / threats to the traditional system, it is easier to compromise.

Judging the system credibility can be reduced to judge the credibility of the output of arbiter. And, the latter also can be reduced to judge the credibility of the output of each executor.

So, ***how to assess the executor credibility and calculate the arbiter credibility from it***, is our studied question.

3. Method

Executor Credibility

Influencing Factors:

- **Disturbance Event History**: Whether the executor has been *disturbed before*?
- **Disturbance Factors**: Whether *the cause* of this disturbance has occurred *before*?
- **Disturbance Numbers**: *The number of disturbances* that have been *previously* experienced.
- **One-time Service Runtime Duration**: Whether this service runtime is *beyond the normal range*?

Calculation Sketch:

- Initialize the credibility of the executor as one, denoted $E.cred = 1$;
- If disturbed before, $E.cred = E.cred - \alpha_h$ (α_h is the weight of the historical disturbance);
- If the cause occurred before, $E.cred = E.cred - \alpha_f$ (α_f is the weight of the disturbed factors);
- If the number is more than the threshold, $E.cred = E.cred - \alpha_n$ (α_n is the weight of the disturbed times);
- If beyond the range of the normal service runtime, $E.cred = E.cred - \alpha_t$ (α_t is the weight of the runtime);

3. Method

Arbiter Credibility

Calculation Formula:

- Denoted the credibility of the arbiter $V.cred$;

$$V.cred = \frac{1}{m}\sum_{E \in R.set} E.cred + \sum_{i \in \{h,f,n,t\}} \Delta_i(R) \cdots\cdots\cdots (1)$$

where

$$\Delta_i(R) = \begin{cases} \frac{Count_i(R)}{m} \times \alpha_i & ,if\ j < k; \\ \frac{1}{2m} \times Norm_i(R) \times \alpha_i & ,if\ j = k; \\ -\frac{m-j}{m} \times \alpha_i & ,otherwise. \end{cases} \cdots\cdots (2)$$

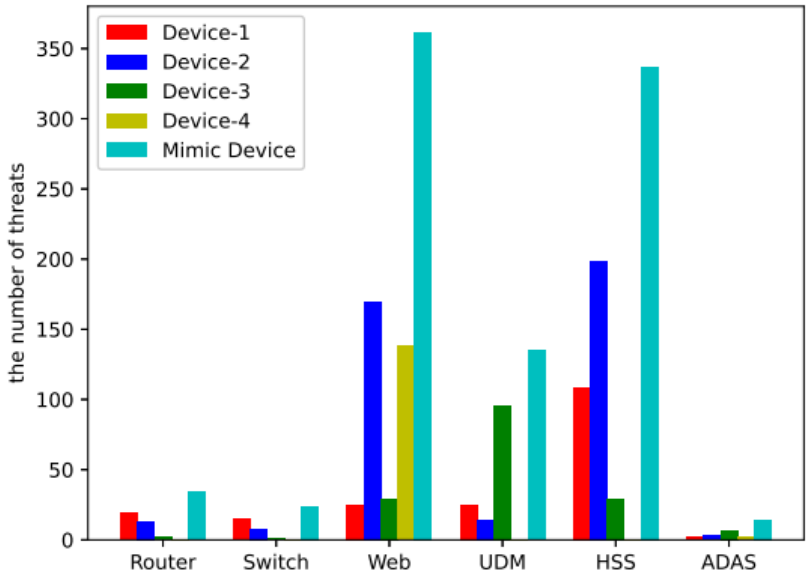
$$Count_i(R) = \sum_{E \in R.set} isFactor_i(E) \cdots\cdots (3)$$

$$Norm_i(R) = \begin{cases} 1 & ,if\ R.abnorm \notin R.set(i); \\ 0 & ,otherwise. \end{cases} \cdots\cdots (4)$$

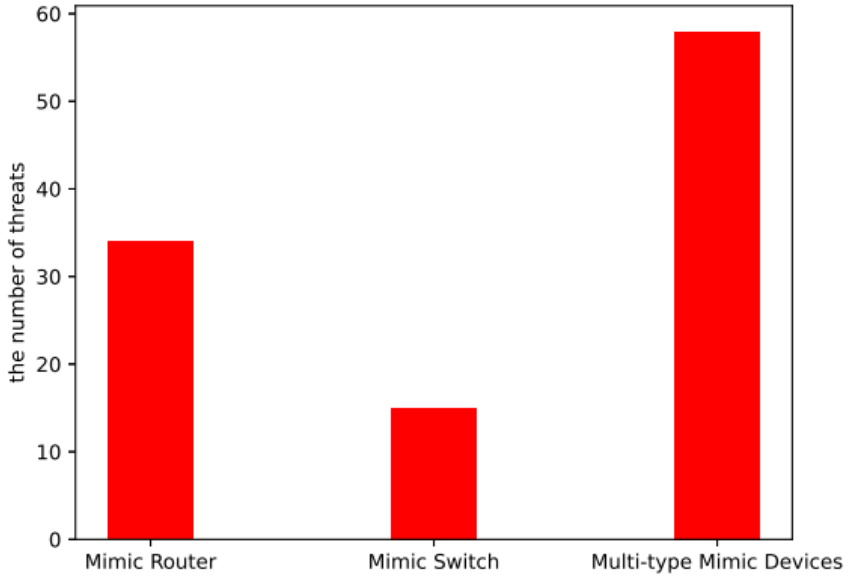
$$isFactor_i(E) = \begin{cases} 1 & ,if\ E\ has\ the\ factor\ i; \\ 0 & ,otherwise. \end{cases} \cdots\cdots (5)$$

$i \in \{h,f,n,t\}$ represents the four influencing factors, E is an executor, R is the current adjudication log record, $R.set$ is the set of online executors contained in R, $R.set(i)$ is the set of online executors in R satisfying the factor i, $R.abnorm$ is the abnormal executors in R, Δ_i stands for the tuning parameter of the corresponding factor.

4. Evaluation



The greater the number of heterogeneous and functionally equivalent devices, the greater the reliability and confidence in the verdict results, as well as enhanced threat detection capability.



Threat detection capability of a combination of different types of mimic devices is stronger than that of a single mimic device.

In the experiment, we set the scoring threshold as 0.85. We calculate our model's accuracy as 0.768 and precision as 0.894 which shows it can effectively perceive threats.

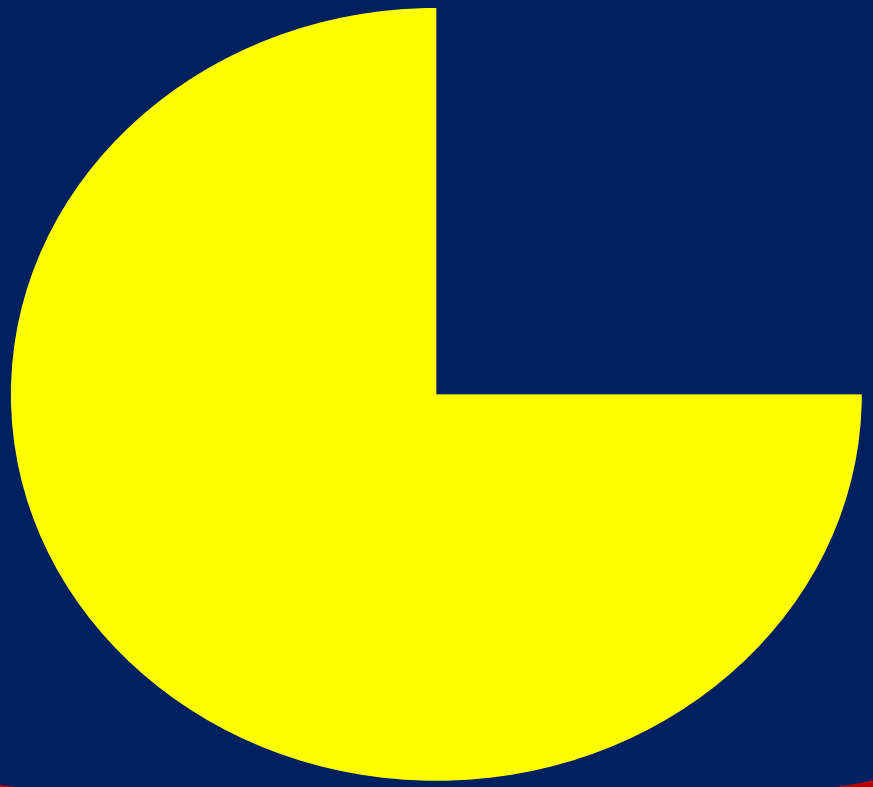
5. Conclusion & Future Work

Conclusion:

- An executor credibility algorithm assessing each online executor's previously disturbed information and currently running state information;
- A system credibility algorithm based on the executor credibility;
- A threat detection model based on system credibility is proposed to enhance the network defense capabilities of the entire mimic network.

Future Work:

- Consider more influencing factors in calculating the executor credibility, and design a more accurate algorithm;
- Except the executor credibility, take multidimensional mimic architecture information in consideration when calculating the system credibility.



Thanks !