ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

ЗАЩИТА ИНФОРМАЦИИ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

К. А. Акула

Белорусский государственный университет, Минск;
Ksenea1@gmail.com;
науч. рук. – А. В. Сидоренко, д-р техн. наук, проф.

Термин кибер-физическая система (CPS) относится к относительно новому поколению роботизированных систем, которые объединяют кибер-аспект вычислений и взаимосвязи с физикой процессов. Мультиагатные CPS состоят из набора динамических систем или агентов, которые взаимодействуют друг с другом по сети передачи для достижения скоординированной работы. В работе представлены механизмы анализа, обнаружения и ослабления атак в распределенных мультиагатных CPS в линейном представлении. Показано, что ошибки отслеживания агентов в локальной окрестности сходятся к нулю независимо от действия атаки. Это происходит, когда собственные значения динамической матрицы сигнала атаки являются подмножеством собственных значений согласованной матрицы. Атаки такого типа атаками, основаны на использовании внутренней модели (IMP атаки). Для обнаружения атак вводится критерий расхождения Кульбака-Либлера (КЛ). Результаты могут быть использованы при разработке нового поколения роботизированных систем.

Ключевые слова: мультиагатные системы; атаки; механизмы обнаружения атак; критерий расхождения Кульбака-Либлера.

ОПИСАНИЕ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ

Предположим, что мультиагентная система, состоящая из N агентов, описывается следующим образом:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) \\ y_i(t) = C_i x_i(t) \end{cases}, \; i = 1,\ldots,N, \qquad (1)$$

где $x_i \in \mathbb{R}^{ni}$, $u_i \in \mathbb{R}^{mi}$ и $y_i \in \mathbb{R}^{p}$ обозначают соответственно состояние, управляющий вход и выход агента. Матрицы $A_i \in \mathbb{R}^{ni \times ni}$, $B_i \in \mathbb{R}^{ni \times mi}$ и $C_i \in \mathbb{R}^{p \times ni}$ соответственно являются матрицами динамики дрейфа, входа и выхода.

МЕХАНИЗМ ОБНАРУЖЕНИЯ АТАКИ

В этом разделе разрабатываются подходы к обнаружению атак и смягчению последствий атак основе критерий расхождения Кульбака-Либлера для атак как на основе IMP, так и других.

Расхождение Кульбака-Либлера является неотрицательной мерой относительной энтропии между двумя вероятностными распределениями, которая определяется следующим образом.

Пусть X и Z две случайные последовательности, имеющие плотности вероятности P_X и P_Z соответственно. Мера расхождения Кульбака-Либлера между P_X и P_Z определяется в работе [1]

$$D_{KL}\left(X\|Z\right)=\int P_X\left(\theta\right)\log\left(\frac{P_X\left(\theta\right)}{P_Z\left(\theta\right)}\right)d\theta \tag{2}$$

со следующими свойствами:

1. $D_{KL}\ (P_X \| P_Z) > 0$
2. $D_{KL}\ (P_X \| P_Z) = 0$ тогда и только тогда, когда $P_X = P_Z$
3. $D_{KL}\ (P_X \| P_Z) \neq D_{KL}\ (P_Z \| P_X)$

Ошибки τ_i и ϕ_i для агента i определяются на основе только локальной обменной информации

$$\tau_i=\left\|\sum_{j\in N_i}a_{ij}\left(h_j-h_i\right)+\omega_i+f_i^d\right\|, \tag{3}$$

$$\varphi_i=\left\|\sum_{j\in N_i}a_{ij}\left(h_j-h_i\right)+a_{ij}\left(\omega_{ij}+f_i^d\right)\right\|, \tag{4}$$

где $\omega_i \sim N(0, \Sigma\omega_i)$ представляет собой гауссов шум ω_{ij} (от агента j к агенту i), h_i, h_j – данные, которыми обмениваются агенты; $f_i^d=\sum_{j\in N_i}a_{ij}f_j^d$, где f_j^d – генерируемый атакующий сигнал.

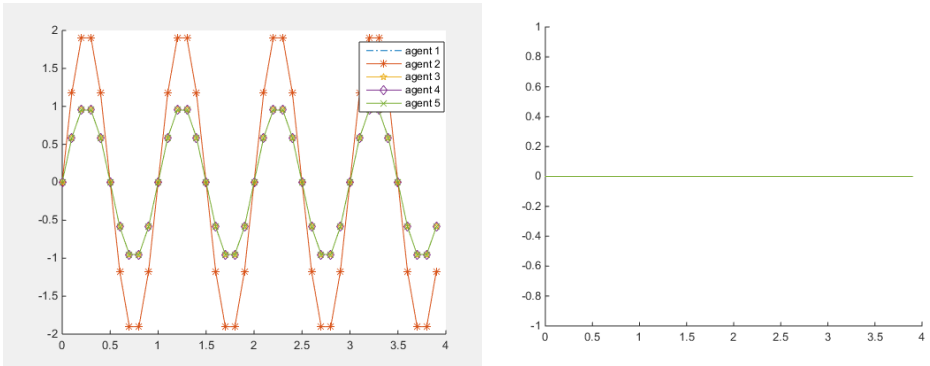
Для обнаружения атаки используются следующие выражения:

$$\begin{cases}\frac{1}{T}\int_k^{k+T-1}D_{KL}\left(\varphi_i\|\tau_i\right)dk<\gamma_i:H_0\\ \frac{1}{T}\int_k^{k+T-1}D_{KL}\left(\varphi_i\|\tau_i\right)dk\geq\gamma_i:H_1\end{cases}, \tag{5}$$

где γ_i – рассчитываемый порог обнаружения: гипотезы H_0 и H_1 обозначают исходный режим работы агента и компрометированный режим. T – размер окна.

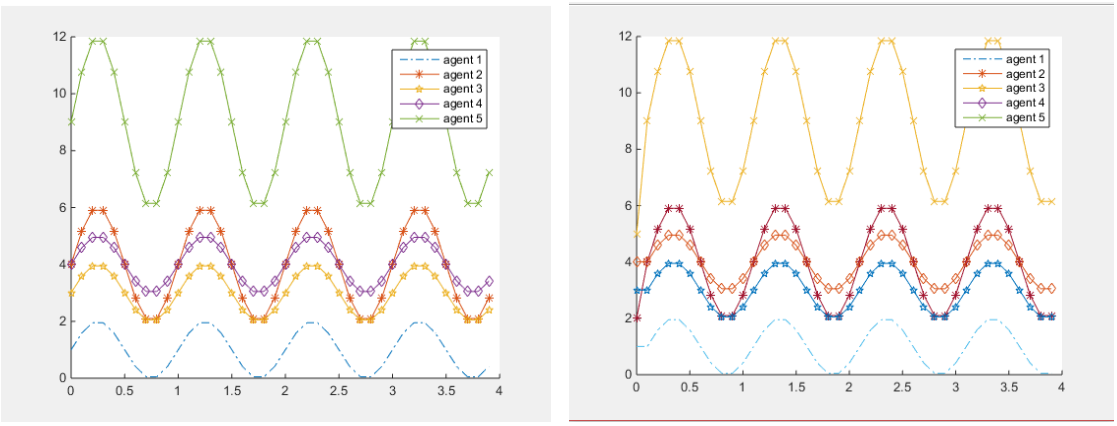
РЕЗУЛЬТАТЫ

На рисунках 1, 2 и 3 представлены результаты.



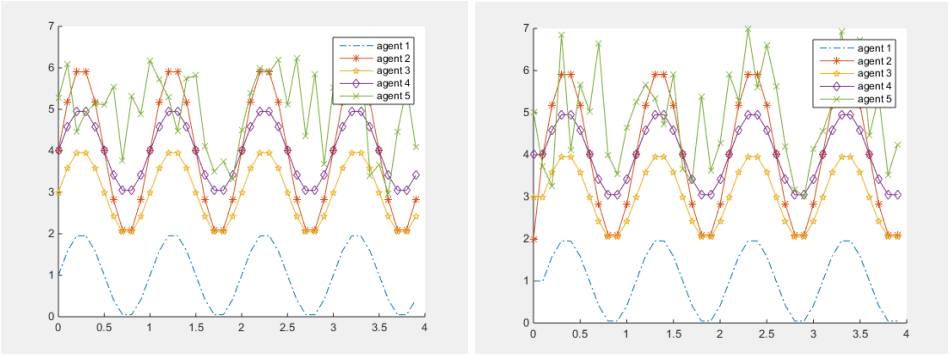
а) б)

Рис. 1. Иллюстрация работы мультиагентной системы:
а) изменение позиции агента при получении им команды;
б) ошибка перемещения агента при подаче ему команды



а) б)

Рис. 2. Иллюстрация работы мультиагентной системы при воздействии ошибки на один агент:
а) изменение позиции агента при получении им команды;
б) ошибка перемещения агента при подаче ему команды



а) б)

Рис. 3. Иллюстрация работы мультиагентной системы при воздействии белого гауссова шума на один агент:
а) изменение позиции агента при получении им команды;
б) ошибка перемещения агента при подаче ему команды

ЗАКЛЮЧЕНИЕ

Таким образом, рассмотренный метод может применятся при обнаружении ошибок при работе мультиагентных систем, что отразится на надежности мультиагентных систем.

Библиографические ссылки

1. Resilient Synchronization of Heterogeneous Multi-agent Systems under Cyber-Physical Attacks [Electronic resource] / H. Modares [et al.]. URL: https://arxiv.org/abs/1807.02856v4 (date of access: 30.05.2019).