УНИВЕРСИТЕТ ИТМО

SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2022 Vol. 22 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2022 Том 22 Номер 1

doi: 10.17586/2226-1494-2022-22-1-47-59

A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms

Ilia I. Viksnin[1]✉, Egor D. Marinenkov[2], Sergey S. Chuprov[3]

[1] Saint Petersburg Electrotechnical University “LETI”, Saint Petersburg, 197022, Russian Federation
[2,3] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] wixnin@mail.ru✉, https://orcid.org/0000-0001-6240-0390
[2] egormarinenkov@gmail.com, https://orcid.org/0000-0001-9895-239X
[3] drmyscull@gmail.com, https://orcid.org/0000-0001-7081-8797

Abstract

Cyber-physical systems’ security and safety assurance is a challenging research problem for Smart City concept development. Technical faults or malicious attacks over communication between its elements can jeopardize the whole system and its users. Reputation systems implementation is an effective measure to detect such malicious agents. Each agent in the group has its indicator, which reflects how trustworthy it is to the other agents. However, in the scenario when it is not possible to calculate the Reputation indicator based on objective characteristics, malicious or defective agents can negatively affect the system’s performance. In this paper, we propose an approach based on Game Theory to address the Reputation and Trust initial values calculation challenge. We introduced a mixed strategies game concept and a probability indicator. The possible outcomes of using different strategies by the system agents are represented with a payoff matrix. To evaluate the approach effectiveness, an empirical study using a software simulation environment was conducted. As a Cyber-physical system implementation scenario, we considered an intersection management system with a group of unmanned autonomous vehicles, the aim of which is to perform conflict-free optimal intersection traversal. To simulate the attack scenario, some vehicles were able to transmit incorrect data to other traffic participants. The obtained results showed that the Game Theory approach allowed us to increase the number of detected intruders compared to the conventional Reputation and Trust model.

Keywords

Game Theory, reputation, trust; security, safety, cyber-physical systems

Acknowledgements

This work was supported by the Ministry of Science and Higher Education of the Russian Federation (Project ‘Goszadanie’ No. 075-01024-21-02 from 29.09.2021).

For citation: Viksnin I.I., Marinenkov E.D., Chuprov S.S. A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 1, pp. 47–59. doi: 10.17586/2226-1494-2022-22-1-47-59

УДК 004.896

Применение теории игр для обеспечения безопасности коммуникации киберфизической системы с использованием механизмов репутации и доверия

Илья Игоревич Викснин[1]✉, Егор Денисович Мариненков[2], Сергей Сергеевич Чупров[3]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова, Санкт-Петербург, 197022, Российская Федерация
[2,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] wixnin@mail.ru✉, https://orcid.org/0000-0001-6240-0390
[2] egormarinenkov@gmail.com, https://orcid.org/0000-0001-9895-239X
[3] drmyscull@gmail.com, https://orcid.org/0000-0001-7081-8797

© Viksnin I.I., Marinenkov E.D., Chuprov S.S., 2022

Аннотация

Предмет исследования. Обеспечение безопасности и надежности киберфизических систем является сложной исследовательской проблемой для разработки концепции «умного города». Технические неполадки или злонамеренные атаки на коммуникации между элементами системы могут поставить под угрозу всю систему и ее пользователей. Реализация репутационных систем — эффективная мера для обнаружения таких вредоносных агентов. Каждый агент в группе имеет свой показатель, который отражает, насколько он заслуживает доверия других агентов. Вместе с тем в сценарии, когда невозможно рассчитать показатель репутации на основе объективных характеристик, вредоносные или дефектные агенты негативно влияют на работу системы. **Метод.** Предложен подход, основанный на теории игр, для решения проблемы расчета начальных значений репутации и доверия. Введены концепция игры со смешанными стратегиями и индикатор вероятности. Возможные результаты использования различных стратегий агентами системы представлены с помощью матрицы выплат. **Основные результаты.** Для оценки эффективности подхода выполнено эмпирическое исследование с использованием программной среды моделирования. В качестве сценария реализации киберфизической системы рассмотрена система управления перекрестком с группой беспилотных автономных транспортных средств, цель которой бесконфликтное оптимальное прохождение перекрестка. Для имитации сценария атаки часть транспортных средств может передавать неверные данные другим участникам движения. Полученные результаты показали, что подход теории игр позволил увеличить количество обнаруживаемых нарушителей по сравнению с необработанной моделью репутации и доверия.

Ключевые слова

теория игр, репутация, доверие, информационная безопасность, функциональная безопасность, киберфизические системы

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации (проект «Госзадание» № 075-01024-21-02 от 29.09.2021).

Ссылка для цитирования: Викснин И.И., Мариненков Е.Д., Чупров С.С. Применение теории игр для обеспечения безопасности коммуникации киберфизической системы с использованием механизмов репутации и доверия // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 47–59 (на агл. яз.). doi: 10.17586/2226-1494-2022-22-1-47-59

Introduction

Striking development of information, communication and automation technologies over the past few decades has had a tremendous impact on various areas of human life. The endeavor to optimize various routine processes and make our life more convenient have led to the emergence of such concepts as Smart Home, Smart City and Smart Manufacturing [1, 2]. These approaches are based on the communication (most often, wireless) between the informational and physical components, the combination of which became known as Cyber-physical systems (CPSs) [3]. The aims of physical elements are to interact with the environment, in which they are located, and collect and/or measure its characteristics. For example, it can be light brightness, humidity, or temperature sensors, which measure the characteristics at predetermined time intervals and transmit the collected data to the informational elements. Informational elements perform computational operations, and, according to predetermined algorithms, generate decisions based on the data received. For instance, if the light brightness level has fallen to a certain threshold, the system needs to turn on the lights.

The implementation of unmanned autonomous vehicles (AVs) is a vital direction for future transportation systems and the Smart City concept development and modernization [4]. Such AVs can be terrestrial, aerial, water or underwater, and can also be described as a set of CPS elements. At the present development stage, AVs are widely available on the market and are actively used in various spheres to perform different work, including those that could previously be performed by highly qualified specialists, e.g. aircraft pilots or train drivers. However, there are tasks that can be performed more effectively by AVs group than using individuals, for instance, territory surveillance or people search during rescue operations. To coordinate group actions, AVs have to use one of the control strategies: centralized or decentralized. They both have their advantages and drawbacks, and the choice depends on such factors as group participants number, task types, or system requirements.

A more detailed review of their properties and an example of practical application can be found in [5, 6]. In the present work, we use a decentralized agent control strategy, as it is more reliable and fault-tolerant from the safety perspective.

CPSs, like any information systems, are exposed to various cybersecurity threats. Conventional security methods, such as authentication, authorization, or cryptography mechanisms are effective to counter or mitigate most information attacks. However, there are so-called “soft” types of attacks that cannot be identified by conventional security mechanisms. These attacks can be aimed at unauthorized changes in the contextual integrity of data transmitted between group members. Moreover, such attacks can be both intentional and unintentional. For instance, in the event when the legitimate agent’s hardware or software components fail, and it starts broadcasting false data about its current location. To combat “soft” attacks, the mechanism based on the agents’ Reputation and Trust was proposed. Group member’s Reputation level is based on their behavior and calculated according to the other group members’ opinions. However, this method has a drawback: since the Reputation is a retrospective indicator, it cannot be calculated at the initial system functioning moment, or at the moment when a new member joins the group.

Earlier in our study [7], we proposed and physically implemented the Reputation and Trust-based approach for AVs security and safety assurance in the intersection management system. To address the initial Reputation value calculation challenge, in [8] we provided the mechanism based on Game Theory fundamentals, which allowed us to calculate this value relying on objective indicators. The major contribution of this paper is twofold. First, we provided an improved and more rigorous approach formalization, with a novel dynamical hybrid decision-making strategy and a probability indicator. In addition, we developed our custom software simulator, that can be found in public access1, and conducted an empirical study with multiple robotic devices able to communicate with each other under "soft" attacks conditions. The results showed that the Game Theory approach implementation allows one to reduce probability of classification intruders as legitimate agents and to increase accuracy of their detection, compared with using classical Reputation and Trust metrics, provided in [7].

The paper contains the definition and description of the terms "Trust" and "Reputation", and a brief discussion of the documents that offer security mechanisms based on this approach. A description of the use of the game theory approach for computer system security is presented, with a brief discussion of the research that followed this concept. The CPS model, information interaction between agents, and group goal optimization problem were formalized. A solution to the problem of transmitting false data by agents and its impact on the work and security of the entire group was proposed. The calculation of trust and reputation was introduced, and the issue of the initial reputation value calculation was discussed for cases where it is impossible to assign this value due to the lack of historical data on the agent behavior. The classification of data transmitted between agents and the formalization of the costs are presented. The concept of the game between two agents, payoff matrix, possible mixed strategies, and their outcomes for the case when the agent does not have enough data to calculate the current reputation value are defined. An approach to the effectiveness evaluation of the proposed model, a modeling scheme and metrics, and a discussion of the obtained result interpretation are considered.

Literature review

Trust and Reputation

In some social networks, online stores, and e-commerce applications, user reputation rating systems have gained popularity. The presence of a reputation indicator implies the existence of certain generally accepted norms and behavior rules on a resource. Violation of such rules and norms by the user leads to a decrease in his reputation indicator, as well as to a decreasing trust to him from other users. For instance, if one of the online store's sellers sells a product with characteristics different from the declared ones, or the delivery time is not corresponding to the expected, it is less likely that buyers want to buy goods from him if there are other more trustworthy sellers.

Depending on the sources, interpretations of Trust and Reputation may vary. The content of these concepts goes deep into antiquity, with the advent of the first people communities and the interaction between them. Those concepts can now be described as Trust and Reputation. Study [9] defines trust as an open and positive relationship between people, containing confidence in decency and goodwill. If we move away from the human relationship and describe the trust between some agents in a computer system, in [10] trust described as a subjective expectation of agent A of certain behavior from agent B based on the history of the interaction. It follows from the definition that trust allows us to assume what kind of expected action or inaction might come from the agent. From the same definition we can trace the subjectivity of trust in relation to one or another object of relationships.

Reputation is defined as an opinion about the intentions and norms of a particular agent, based on his behavior retrospective and interactions with him [10]. Quantification can be calculated based on the opinions or observations of other group members. Unlike subjective trust (relying on one's own experience and other factors), reputation allows reflecting a public measure of the agent's reliability based on group members' observations or assessments.

To use the Trust and Reputation-based approach in information systems, it is necessary to formalize and consider quantitative Reputation and Trust indicators, and data on observations and assessments. This can be especially relevant in decentralized networks, where there is a lack of network infrastructure and the nodes interact directly with each other. Such networks became known as peer-to-peer (P2P) networks [11]. P2P networks have gained widespread popularity with the advent of the Internet of Things (IoT) concept [12], vehicular (VANETs) and mobile (MANETs) ad-hoc networks [13]. P2P allows to transfer and process large amounts of information, at a cost lower than using a centralized infrastructure network [14]. However, due to the decentralized architecture, presence of heterogeneous elements, and specific features, such networks are subject to "soft" attacks aimed at the contextual integrity of the transmitted data. "Conventional" cybersecurity methods, such as authentication or cryptography, are ineffective against such attacks.

In the AVs case, VANETs allow transmitting data from one vehicle to another and to the transport infrastructure objects. Such data transfer can be used by the Intelligent Transport System (ITS) to build optimal routes, generate informational and emergency messages warning of bad weather conditions, construction and maintenance road works, and etc. Papers studying Reputation-based data security techniques may offer different approaches to calculate these metrics. In [15], the authors suggest calculating the trust indicator in the range from –1 to 1, as in [7], we proposed to calculate the Reputation and Trust indicators in the range from 0 to 1. In the present paper, we use the calculus described in [7] and improve it with the Game Theory-based approach.

In [16], Starub et al. proposed a multi-level intrusion detection system (IDS) to protect self-driving vehicles from malicious attacks. The system is based on the method of determining nodes' reputation value. The system contains shared knowledge generated by all communication participants. The reputation level depends on the nodes' retrospective behavior. Despite the interesting system's architecture proposed by the authors, it is difficult to evaluate the effectiveness of their solution. The work lacks both reputation level calculus and the solution effectiveness validation and comparison with other existing Trust and Reputation-based mechanisms.

In [17], Kim and Viksnin proposed a method for calculating Trust and Reputation indicators, which is based on the loan theory to ensure communication of security flying drones. The main idea of the approach is that it would be unprofitable for intruders to perform a destructive informational impact on the group. In case when the agent transmits incorrect information, its indebtedness increases. The experiment results showed that the intruder transmitting incorrect data was blocked in 90.2 % cases.

To verify the data reliability, two approaches are proposed [18]: objective and subjective. In the second case, the nodes rely on the opinion of other nodes to calculate the trust indicator. The authors addressed the data privacy problem when calculating nodes' trust indicators, and proposed a framework that allowed them to find a balance between trust and privacy in the system. Experiments conducted using the ONE network simulator showed that the application of the proposed linkability protocol allowed increasing transmitted data privacy by using pseudonyms for nodes and offered more flexibility than the standard secure broadcast authentication protocol utilized in the ONE network simulator.

One of the main challenges in existing Reputation and Trust-based approaches is generating the initial value for the system agents, based on their retrospective behavior. Moreover, this issue is actual when a new agent joins the group, and other participants need to decide, how trustworthy it is. In this paper, we proposed a novel dynamic approach for initializing the Reputation value, which depends on particular situations and considers current agents' conditions. In Table 1, we summarize and compare the main characteristics of the related literature in the context of this challenge.

As can be seen from Table 1, we outlined a number of important characteristics that are necessary for evaluating further potential and implementation of the proposed mechanisms. We compared the approach, proposed in this paper, with our previous research [7] and other four studies, related to Reputation and Trust-based security methods. According to the presented Table, only our approach provides dynamic Reputation value initialization for self-driving vehicles, which is vital to reduce the negative influence of malicious or defective agents on the system, when their Reputation value cannot be determined on the basis of retrospective behavior. Moreover, our plans include implementing of this Game-Theory approach on the physical testing ground, demonstrated in [19] and conducting real-world performance evaluation.

Game Theory

Game theory is a branch of mathematical economics that studies the resolution of conflicts between players and the optimality of their strategies. It is widely used in various fields of human activity, such as economics and management, industry and agriculture, military and construction, trade and transport, communications, etc [20].

One of the Game Theory implementation tasks in the cybersecurity area is to optimize security administrators' actions in network systems. In the Game Theory context, this task can be formalized as follows: there are two coalitions: defenders (administrators) and attackers; the goal of administrators is to minimize the damage to the system by optimal tasks distribution among themselves, and the goal of the attackers is to compromise the system. Considering different attackers' behaviors, it is possible to identify such strategies for the administrators' behavior (both for a coalition and for each administrator), in which the system's damage is minimized, regardless of the attackers' strategy. One of the approaches is described in [21]. The authors proposed a strategy, in which Nash equilibrium can be achieved, which guarantees an optimal solution to the defending side regardless of the attackers' decisions. The authors conducted a comparative approach analysis to ensure Game Theory-based safety circuit and common sense decision algorithms. To verify the developed model, real statistics were used.

Table 1. Reputation and Trust-based approaches characteristics comparison

Characteristics	Reviewed Studies					Our approach
	[7]	[15]	[16]	[17]	[18]	
Implementation scenario	Self-driving vehicles	Cloud computing	VANETs	Unmanned aerial vehicles (UAV)	VANETs	Self-driving vehicles
Reputation (or Trust) initial value	Constant (0.5)	Constant (0)	Constant (0)	Constant (0)	Constant (not specified)	Dynamic (depends on situation)
Behavior evaluation	Collective	Individual and collective	Individual and collective	Collective	Collective	Collective
Calculus	Provided	Provided	Not provided	Provided	Provided	Provided
Soft attacks	Addressed	Not addressed	Addressed (lack of details)	Addressed	Addressed	Addressed
Empirical study	Software, physical	No	No	Software	Software	Software

In [22], Roy et al. provided an overview of the Game-Theoretic models' application for network security assurance. The authors reviewed static games and divided them into complete imperfect information and incomplete imperfect information games. In the former game type, the authors cited the example of an information war and a quantitative risk assessment for effective investment decisions in the cybersecurity area. The latter gave examples of games in the framework to counter DDoS and intrusions in ad-hoc networks. Moreover, the authors analyzed dynamic games and subdivided them into 4 types: complete perfect information, complete imperfect information, incomplete perfect information, and incomplete imperfect information games. The first game type is used for risk analysis in computer networks, where, as a rule, there are only two participants: a network administrator and an attacker. Implementation of Game Theory allows determining the optimal strategy for several iterations, which helps to optimally distribute resources for long time periods. For the second type, an IDS and several scenarios, based on the attackers' knowledge completeness on the system were considered. This approach determines the optimal players' strategies, which can subsequently be applied as a deciding rule when implementing or modifying the system. The third type described a game, in which network participants reduce worm-attack propagation speed, which allows scanning a system for important and valuable information. In the fourth type, games like admin-attacker are also considered.

In [23], Game Theory is used for security assurance in e-commerce applications. The authors described the security game model using the penalty parameter, calculated replicator dynamics and analyzed the evolutionarily stable strategy of the game model. As a result, the authors concluded that investment cost reduction leads to the stimulation of investment in cybersecurity. With an increase in investment costs, the penalty parameter saves the incentive for investments. The described papers on Game Theory approaches show the expediency of applying such approaches in the areas related to distributed networks and automated systems. However, there still is a challenge of initial value calculation for Trust and Reputation indicators, and our Game Theory-based approach allows estimating the behavior of elements within a distributed system. Thus, we propose our Game Theory-based approach to address this challenge.

Cyber-physical system model formalization

As mentioned above, we consider the CPS with a decentralized group control strategy. In addition, we assume that all group participants are homogeneous. Then, CPS can be formalized as a set of homogeneous agents with the cardinality of n: $CPS = \{e_i | i = \overline{1, n}\}$. Let us assume that agent e_i is a dynamic object and is able to move. Moreover, CPS agents possess the following characteristics:

- agent's current location;
- maximum possible distance to perform informational interaction (II) with other group members;
- on-board sensors' maximum possible distance to perform surroundings monitoring.

The agents are able to perform the tasks assigned to them. Tasks are distributed between group participants via collective task-allocation auction. All tasks are aimed to reach the common CPS's group goal. Generally, this goal can be interpreted as an optimization problem: the group needs to complete maximum tasks with the minimum costs, where costs can be understood as time, energy or other characteristics. In the task execution process, every action performed by agents increases the group costs for goal reaching, therefore, these actions need to be optimal. To perform optimal action, agents are necessary to analyze the data circulating inside the CPS and decide which action to perform on the basis of these data. The data circulating in CPS at the discrete time t can be classified in the following way:

- data on e_i current technical state TS_{ei}^t which include hardware and software components condition, current location and velocity and other agent's characteristics;
- data on e_i current status S_{ei}^t, which can be interpreted as "occupied" or "unoccupied" with a task at a current moment;
- data on e_i current surroundings condition E_{ei}^t, which is obtained by agent's on-board sensors;
- other agent's e_i useful data O_{ei}^t, which are relevant for reaching the CPS goal;
- data on other group participant $I_{ei}^t = \{I_{e_ie_j} | i \neq j, j = \overline{1, m}\}$, that e_i possesses, where $I_{e_ie_j} = \{TS_{ej}, S_{ej}, E_{ej}, O_{ej}\}$ is a data on e_j obtained in t time or earlier, $m | m \leq n - 1$ is a number of elements, on which e_i has knowledge.

To calculate the task's completion costs, it is proposed to calculate actions' costs that need to be performed when completing this task. To perform this, we introduce a cost calculation function based on the selected action:

$$c_{ei}^t = costs(act(TS_{ei}^t, S_{ei}^t, E_{ei}^t, I_{ei}^t, O_{ei}^t)), \qquad (1)$$

where c_{ei}^t is the amount of resources spent to execute an action at the t time; *costs* is the function for calculating the costs amount; *act* is the function for e_i optimal action determining at the t time. The set of completed tasks T^d can be represented as a subset of all available tasks T with a cardinality of k: $\exists T^d \subseteq T$: $T = \{tsk_l | l = \overline{1, k}\}$, where tsk_l is a l'th task need to be performed by the group.

According to (1) and to the introduced task's subset, the CPS goal can be formalized as:

$$\begin{cases} \sum\limits_{s=0}^{t} \sum\limits_{i=0}^{n} costs(act(TS_{ei}^t, S_{ei}^t, E_{ei}^t, I_{ei}^t, O_{ei}^t)) \to 0 \\ |T^d| \to |T| \end{cases}.$$

Problem statement

The data transmitted by agents can be either correct or false. In the first case, the data reflects the actual (real) location and environment characteristics of the agent e_i at the time of transmission t_j. In the second case, the data is incorrect and does not reflect the real characteristics of the agent e_i at the time of the data transfer t_j. The data may be incorrect due to malfunction, sensors failure, or malicious interference with the software or hardware agent's e_i components.

To identify agents that transmit false data, earlier, we proposed the procedure based on Reputation and Trust indicators evaluation [7]. Each of the group agents has a Reputation indicator. The assessment is based on the transmitted data verification at each time *t* by group agents, which are able to perform this evaluation. To describe our approach, we introduced three indicators: Truth, Trust, and Reputation. A brief description of these indicators is provided below, and a more detailed explanation can be found in [7].

In [8], we applied pure strategies and obtained better results than using raw Reputation and Trust metrics. However, the pure strategies application did not show a considerable gain in effectiveness.

Therefore, in this study, we formulate the hypothesis that the *Truth* indicator calculation in the incomplete data conditions, based on the information impact on the CPS's aim assessment, allows us to improve false data providers detection accuracy compared to setting initial Reputation value as 0.5.

Reputation and Trust approach formalization

To perform the data correctness evaluation, we need to introduce three indicators: *Truth*, *Reputation* (*R*), and *Trust*.

Truth is an indicator that displays a subjective correctness assessment of the transferred data by other agents. Correctness is determined using the sensors of agents and can be described as:

$$Truth_t = f_{tr_t}(data),$$

where $Truth_t$ is the evaluation of data at the time *t*; *data* is the data to be evaluated; f_{tr_t} is the evaluation function of *Truth* at the *t* time.

Reputation (*R*) is an indicator based on a retrospective of the *Truth* indicator assessed by each group agent. It can be described as:

$$R_t = f_{r_t}(Truth_t) = f_{r_t}(f_{tr_t}(data)),$$

where R_t is the *R* value at the *t* time; f_{r_t} is the *R* evaluation function at the *t* time.

Trust is an indicator characterizing a subjective assessment of agent's behavior by other group members. It is calculated based on a *Truth* and *R* combination, and can be represented as:

$$Trust_t = f_{trust_t}(R_{t-1}, Truth_t) = f_{trust_t}(f_{r_{t-1}}(f_{tr_{t-1}}(data), f_{tr_t}(data)),$$

where $Trust_t$ is the indicator of *Trust* at the *t* time; f_{trust_t} is the function of evaluating *Trust* at the *t* time.

Reputation initial value calculating challenge

Existing Reputation-based models use indicators of Reputation and Trust to detect intruders on the basis of their behavior and the content of informational messages, transmitted by them [24–27]. However, during the system operation, situations may occur when none of the agents has the opportunity to assess the correctness of the data transmitted to them. For example, such a situation may arise at the t_0 time (initialization of the system), when agents are distributed over the area and do not have a retrospective assessment, or when a new agent joins the group. As a limitation, each of the above indicators is in the range of [0, 1]. In general, the initial *R* value is defined as 0.5 (as average value). Such an approach does not allow characterizing transmitted data as either correct or not, which leads to a further unpredictable agent's behavior assessment.

To address this issue, in [8], we provided an improved *Truth* calculating mechanism for the case of data incompleteness, based on the transmitted data impact evaluation on the task performance process. Considering the data incompleteness case in the Game Theory context, we formalized, implemented, and evaluated our approach via software simulations. The proposed model implementation allowed us to slightly increase malicious agents' detection accuracy and to decline false-negative errors by almost 8 times. However, false-positive errors increased by almost 12 times. These results were obtained using pure game strategies, which led to *Truth* = 0 assigning for both correct and incorrect data. Such obstacles encouraged us to evolve the approach's accuracy and reliability.

In this study, we suggest that in the data incompleteness case — when the agent is unable to assess data transmitted from another agent — a probabilistic data correctness assessment increases the malicious agents' detection accuracy. Such an approach can be implemented using Game Theory, namely a mixed game extension, in which an equilibrium situation always exists [28]. This mechanism allows calculating *Truth* indicator even in the data incompleteness cases. Moreover, the probabilistic nature of *Truth* indicator formation assumes obtaining a dynamic solution, using which it is possible to assess the optimal *Truth* value for various system's conditions.

False data identification model

False data impact on the group's performance

To verify our mechanism, we propose a calculus for assessing the false data impact on the group's performance during the goal achievement process. The information in the system can be divided by its relevance into the following categories: actual, less actual, and disinformation. The information relevance is substantiated by the combination of the information receiving time, and the time at which this information is used to determine the agent's further actions and is characterized by a linear costs increase. In this case, the costs are calculated according to:

$$c_{ei}^{t} = k \times (t - (t' - 1)) + c_{ei}^{t'-1}, \tag{2}$$

where *k* is a static coefficient that determines costs increasing rate using actual information; *t*′ is a moment of information reception.

In the less actual information case, the costs grow exponentially since the information becomes outdated in time. This can lead to various scenarios that maliciously affect agent's or whole CPS's operation. Let us introduce the information block *Inf* relevance indicator $a_{Inf} \in (0; 1)$, which characterizes the information obsolescence rate and the growth of costs, estimated by the agent e_i. The costs of using less relevant information are calculated according to:

$$c_{ei}^{t} = k \times a_{Inf}^{t'-1} \times (t - (t' - 1)) + c_{ei}^{t'-1}. \tag{3}$$

In the disinformation case, when the data is incorrect, costs grow faster than using actual and less actual information. Therefore, it is necessary to introduce the disinformation impact coefficient $a'_{Inf} \in (0; 1)$, which characterizes the damage caused by the false data. The costs are then calculated according to:

$$c_{ei}^{t} = k \times a_{Inf}^{\prime t'-1-t} \times (t - (t' - 1)) + c_{ei}^{t'-1}. \tag{4}$$

Game Theory approach formalization for data incompleteness case

To solve the problem stated in section "Problem Statement" and test the hypothesis, an approach to the formation of the *Truth* indicator based on Game Theory is proposed. Herein under the "game", we mean the process of assessing the information that an evaluating agent receives from another agent in the case when it is impossible to evaluate received data by his sensor devices or to rely on other agents' opinions. Therefore, two players have two strategies in this game. In the case of an evaluating agent, the strategy is the definition of the received data as correct, and its further processing or determination of these data as incorrect. In the case of the transmitting agent, there are strategies to transmit correct or incorrect data. Thus, the solution to the game is to find an equilibrium in a given situation. That is, for the evaluating agent, this is a strategy that gives it the maximum gain regardless of the transmitting agent. The payoff of the evaluating agent is the difference in the cost' growth rate for actions performance based on the evaluated data, received from the transmitting agent. In other words, the evaluating agent decides which information will lead to a smaller deviation in the cost' growth rate: less relevant information or disinformation.

In the previous study [8], we proposed to solve this game in pure strategies, which required to initialize the *Truth* indicator as a constant (0 in our case). The simulation results showed insufficient effectiveness (the *Accuracy* increased by only 1 %) since, in the case of *Truth* = 0, the effectiveness grows in proportion to the malicious agents in the system. To address this issue, we decided to solve the game in a mixed form, the outcome of which directly depends on the data obsolescence indicators, the cost' growth for disinformation, and the time of using these data. The solution of such a game gives the probability of choosing a particular strategy, which allows finding an equilibrium for games with different conditions and thereby gives a general solution to the problem.

To calculate the *Truth* indicator in the data incompleteness case, the process of information receiving is considered as a game with two players in normal form, where each agent has a finite number of possible strategies. The game can be characterized as [29]:

- discrete — the strategies set is discrete;
- finite — the strategies set is finite;
- strategic — the uncertainty comes from another player;
- in normal form — the payment matrix exists;
- antagonistic — the loss of one player is equal to the gain of the other.

Thus, let us define the game G according to the antagonistic game in normal form [28]:

$$G = (X, Y, K),$$

where X and Y are player's 1 and 2 strategies sets respectively; $K : X \times Y \rightarrow \mathbb{R}$ is player's 1 gain function. In this case, under player 1 e_T trusted agent that receives information is considered. Under player 2 e_U potential intruder agent that transmits information is meant. Table 2 represents agents' e_T and e_U strategies $x_i \in X$, $i \geq 1$ and $y_j \in Y, j \geq 1$, respectively.

Information correctness evaluation for data incompleteness case

To form a payoff matrix, we introduce the agent's e_T payoff function $K(x_i, y_j)$. Let there be a function for cost' growth rate calculating, which depends on the $H(x_i, y_j)$. Strategies, selected by the agents. According to the strategies outcomes, defined in Table 2, e_T's information is considered as: actual if agent e_T chooses 1st strategy and e_U — 2nd strategy $(x_1; y_2)$; less actual if e_T chooses 2nd strategy and e_U chooses 1st strategy $(x_2; y_1)$ or e_T chooses 2nd strategy and e_U also chooses 2nd strategy $(x_2; y_2)$; and disinformation if both e_T and e_U choose 1st strategy $(x_1; y_1)$. In the actual information and disinformation cases $t' = t$. Thus, determining the functions' (2), (3), and (4) first degree derivative, H is determined according to:

$$H(x_i, y_i) = \\ = \begin{cases} \begin{cases} k \times (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1), j = 1, i = 1 \\ k, j = 2 \end{cases} \\ k \times (a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1), i = 2 \end{cases}. \tag{5}$$

Let us introduce the function for determining agent's e_T optimal strategy, which depends on the strategy chosen by e_U agent: $opt(y_j) = x_{j mod 2+1}$. Then the payoff function $K(x_i, y_j)$ can be defined as the difference between the cost growth rate in the case when e_T knows e_U's strategy and the cost growth rate, which depends on the strategies selected by the agents:

$$K(x_i, y_j) = H(opt(y_j), y_j) - H(x_i, y_j). \tag{6}$$

According to the (5) and (6) equations, the generated payoff matrix is presented in Table 3.

As one can see from Table 3, situations (x_1, y_1) and (x_2, y_2) defined for the general case, and maximin cannot be defined. However, as the calculation of these functions results strictly less than zero, then *maximin* ≠ *minimax*, *minimax* = 0. Therefore, it is not possible to solve the game in pure strategies and mixed strategies should be used. According to the book [28], $\exists \chi_i$: $\sum_{i=1}^{|X|} \chi_i = 1$, $1 \leq i \leq |X|$ is the

Table 2. Agents' strategies

Strategy counter l	x_l	y_l
1	To estimate information as a correct	To send incorrect information
2	To estimate information as an incorrect	To send correct information

Table 3. Payoff matrix

		e_U	
		y_1	y_2
e_T	x_1	$k \times \left((a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)\right)$	0
	x_2	0	$k \times \left(1 - (a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}\right)$

pure strategy χ_i selection probability, and $\exists\gamma_j$: $\sum_{j=1}^{|Y|}\gamma_j = 1$, $1 \le j \le |Y|$ be the pure strategy y_j selection probability.

Then $\overline{X} = (\chi_1, \ldots, \chi_{|X|})$ and $\overline{Y} = (\gamma_1, \ldots, \gamma_{|Y|})$ are agents' e_T and e_U mixed strategies, respectively. Therefore, it is possible to define mixed strategies using the following equation systems:

$$\begin{cases} K(x_1, y_1) \times \chi_1 + K(x_2, y_1) \times \chi_2 = v_\Gamma \\ K(x_1, y_2) \times \chi_1 + K(x_2, y_2) \times \chi_2 = v_\Gamma \\ \chi_1 + \chi_2 = 1 \end{cases}$$

$$\Rightarrow \begin{cases} \left((a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)\right) \times \chi_1 = \\ = \left(1 - (a_{Inf})^{\,t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}\right) \times \chi_2, \\ \chi_2 = 1 - \chi_1 \end{cases}$$

$$\begin{cases} K(x_1, y_1) \times \gamma_1 + K(x_1, y_2) \times \gamma_2 = v_\Gamma \\ K(x_2, y_1) \times \gamma_1 + K(x_2, y_2) \times \gamma_2 = v_\Gamma \\ \gamma_1 + \gamma_2 = 1 \end{cases}$$

$$\Rightarrow \begin{cases} \left((a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)\right) \times \gamma_1 = \\ = \left(1 - (a_{Inf})^{\,t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}\right) \times \gamma_2, \\ \gamma_2 = 1 - \gamma_1 \end{cases}$$

where v_Γ is game value. As one could see these equation systems looking similar, so, we will solve the equation system only for the $\overline{X}$:

$$\begin{cases} \left((a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)\right) \times \chi_1 = \\ = \left(1 - (a_{Inf})^{\,t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}\right) \times \chi_2, \\ \chi_2 = 1 - \chi_1 \end{cases} \Rightarrow$$

$$\Rightarrow \left((a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)\right) \times \chi_1 =$$

$$= \left(1 - (a_{Inf})^{t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}\right) \times (1 - \chi_1) \Rightarrow$$

$$\Rightarrow \chi_1 = \frac{1 - (a_{Inf})^{\,t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}}}{1 - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)} \Rightarrow$$

$$\Rightarrow \chi_2 = \frac{(a_{Inf})^{\,t'-t} \times \ln \frac{e}{(a_{Inf})^{t'-t+1}} - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)}{1 - (a'_{Inf})^{-1} \times \ln\left(\frac{e}{a'_{Inf}}\right)}.$$

The equation system for the $\overline{Y}$ are solving the same, therefore, $\chi_1 = \gamma_1$ and $\chi_2 = \gamma_2$.

As a result of solving the game, the obtained mixed strategies can be formalized according to:

$$\overline{X} = \left(\frac{1 - (a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1)}{1 - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}, \right.$$
$$\frac{(a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1) - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}{1 - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}$$

$$\overline{Y} = \left(\frac{(1 - (a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1))}{1 - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}, \right.$$
$$\frac{(a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1) - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}{1 - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}.$$

On the basis of agent's e_T strategies, defined in Table 2, the *Truth* indicator directly depends on the probability of evaluating the information as correct. Therefore, *Truth* = χ_1, and in the data incompleteness case the *Truth* indicator is calculated according to:

$$Truth = \frac{(1 - (a_{Inf})^{t'-t} \times (-\ln a_{Inf} \times (t - (t' - 1)) + 1))}{1 - (a'_{Inf})^{-1} \times (-\ln a'_{Inf} + 1)}.$$

Since the *Truth* indicator can be greater than 1 in this case, we assume that all values greater than 1 is equated to 1: *Truth* > 1 → *Truth* = 1.

Empirical study

Simulation setup

To evaluate the effectiveness of the proposed model, we conducted an empirical study using a custom software simulator. As one of the CPS's possible implementations, we considered the simulation of the intersection management system with multiple unmanned autonomous vehicles, which need to perform conflict-free optimal intersection traversal with minimal costs [7]. In the present study, costs are represented as a number of sectors that agent overcomes to reach its path's finish point.

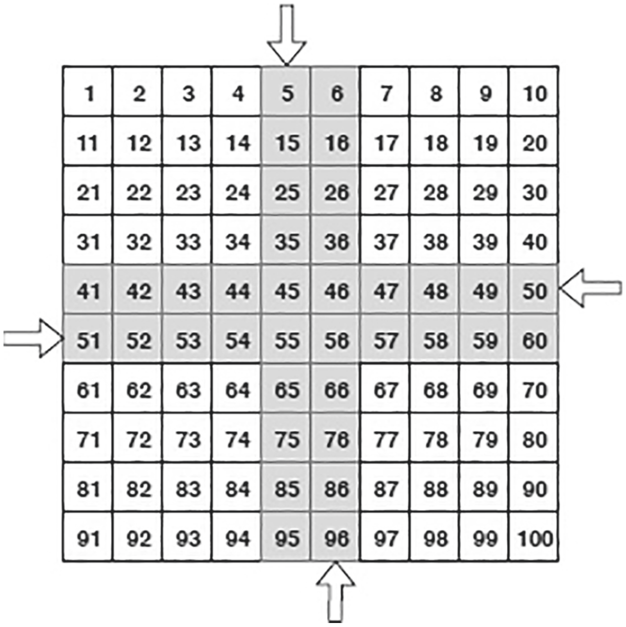

Fig. 1. Model of intersection and schematic representation of the vehicles' driving direction

The intersection scheme is represented in Fig. 1. It has the following properties:

- software testing ground is divided into equal sectors, and each sector has its unique number;
- software testing ground size: 10 × 10 sectors;
- software testing ground has 4 roads: two vertical (oncoming and passing) and two horizontal (oncoming and passing) ones.

As an assumption, we initially set the number of agents, which provide false data (intruders). During the system operation process, intruders implement on-off attack [30]. The purpose of this attack is to compromise Reputation mechanism and decrease system's effectiveness via the alternating transmission of correct and false data. In our experiments, on-off attack cycle is 2-on, and 1-off, i.e. intruders transmit false data during 2 discrete time moments and correct data during the next 1 discrete time moment.

To detect intruders, agents transmit and evaluate information about their current location. For such an assessment, they use their sensor devices, which can obtain data from the surroundings within a radius of 1 sector, that is, in 8 sectors around the agent. Moreover, the agent can request the assessment of other agents in case when it is not able to evaluate the data received. The radius of information interaction between agents is 9 sectors. All agents located on the software testing ground have the ability to interact.

Experiments were performed using raw Reputation and Trust indicators and using the proposed Game Theory approach. In each group of the experiment series, 1000 simulations were conducted with the various intruders percentage: 10, 20, 30, and 40 % from 1000 agents in a group. To evaluate the approach effectiveness, we introduced the following metrics:

- False Positive (FP) — the ratio of legitimate agents, that were incorrectly identified as intruders (relatively to all agents in a group);
- False Negative (FN) — the ratio of intruders, that were incorrectly identified as legitimate agents;
- Accuracy — the ratio of agents, that were correctly identified as legitimate agents or saboteurs;
- Precision — the ratio of intruders, that were correctly identified as false data providers relative to all agents identified as intruders;
- Recall — the ratio of intruders, that were correctly identified as false data provides relative to all agents in the group;
- F0.5 — weighted harmonic mean of Precision and Recall metrics, when $\beta = 0.5$;
- F1 — harmonic mean of Precision and Recall metrics, when $\beta = 1$;
- F2 — harmonic mean of Precision and Recall metrics, when $\beta = 2$.

During the simulation process, Accuracy, Recall, FP and FN error metrics were defined and employed in the following way:

- FN error occurred when the agent provides false data and is perceived by the rest of the group as legitimate. The likelihood of collision increases in this case;
- FP error occurred when the agent provides correct data and is perceived by the rest of the group as an intruder, which results in a system's effectiveness decrease;
- True Negative (TN) case is occurred when the incorrect information transmitted by the intruder is perceived by the rest of the group as incorrect;
- True Positive (TP) case is occurred when the correct information transmitted by the legitimate agent is perceived by the rest of the group as correct;
- $\text{Accuracy} = \dfrac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$;
- $\text{Recall} = \dfrac{\text{TP}}{\text{TP} + \text{FN}}$.

Simulation results

Fig. 2 demonstrates the obtained results for 10, 20, 30, and 40 % intruders in the group. Averaged indicators' values are presented in Fig. 3. TP and TN values are not presented in the figures, although they were used for Accuracy and Recall calculation.

Fig. 2 demonstrates that the proposed Game Theory-based approach seems to be more sensible in relation to intruders detection, i.e., more elements are likely to be identified as intruders if their behavior deviates from "normal". Thus, the basic approach is more characterized by "skipping" intruders to increase the number of elements involved in the system. In addition, Game Theory-based approach did not show a significant change in the efficiency of legitimate agents' identification. This is evidenced by the values of $F(\beta = 0.5)$, $F(\beta = 1)$ and $F(\beta = 2)$.

Comparing the results presented in Fig. 2, one can observe that the values of Accuracy, $F(\beta = 0.5)$, and $F(\beta = 1)$ tend to the values obtained with $R = 0.5$ as the intruders proportion in the group increases. According to Fig. 3, the Accuracy of intruder identification increased by 15 % on average. Moreover, FN errors decreased by an average of 3 times, and FP errors increased by 1.7 times, which also decreased the average value of the Precision metric. As

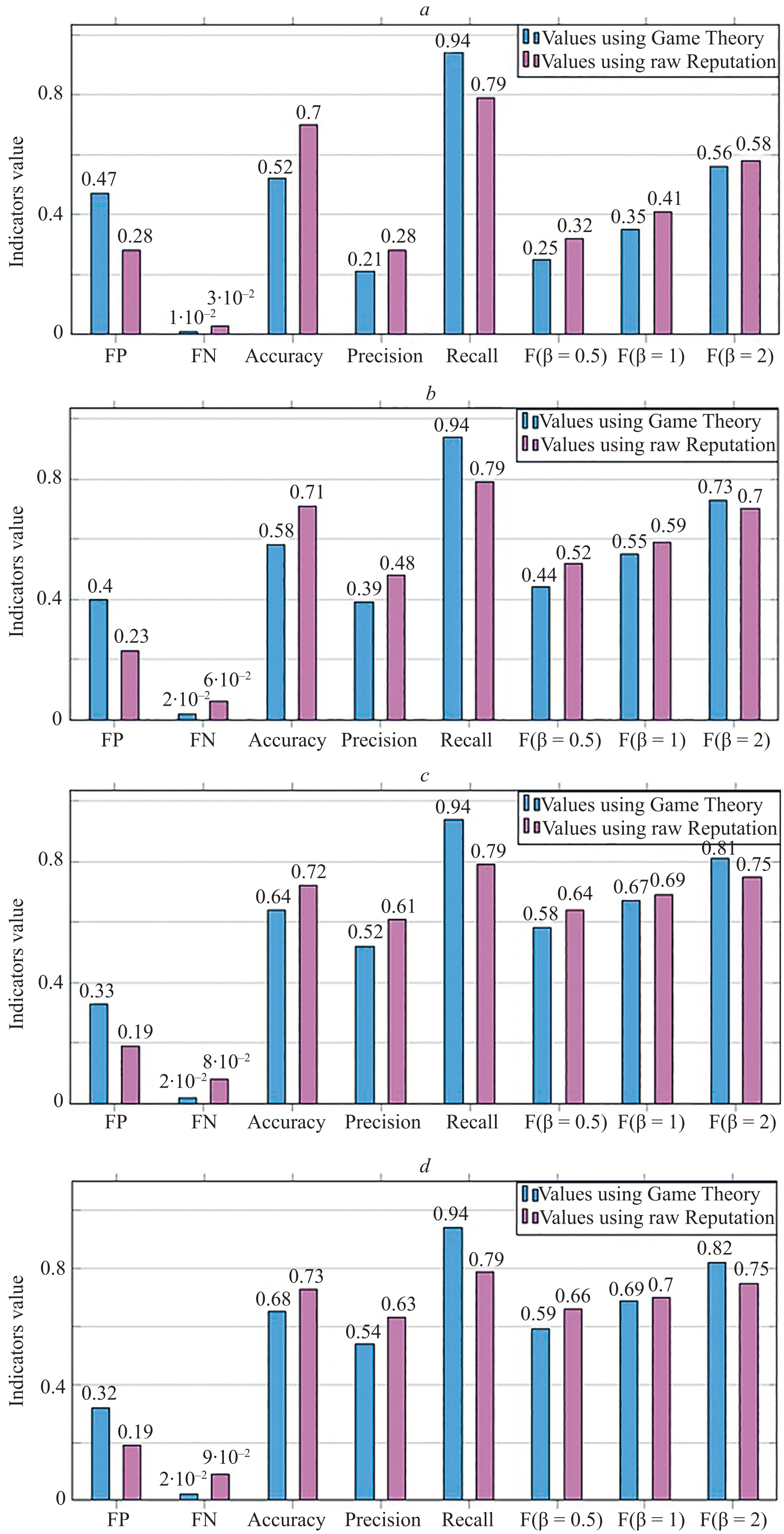

Fig. 2. FP, FN, Accuracy, Precision, Recall, and F-measure values, averaged on 1000 agents classification experiments, with and without Game Theory approach, for the case with: 10 % (*a*); 20 % (*b*); 30 % (*c*); 40 % (*d*) of intruders in the group

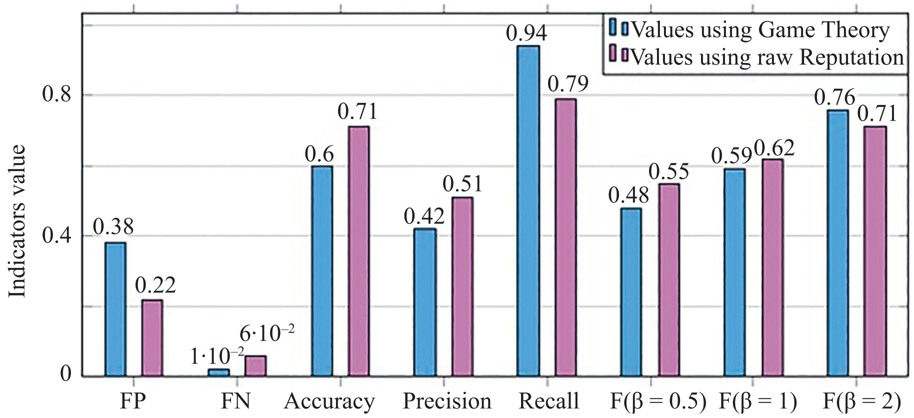

Fig. 3. Averaged FP, FN, Accuracy, Precision, Recall, and F-measure values for all experiment series (10–40 % of intruders), with and without Game Theory approach

a result of modeling the developed approach, the Recall metric had been increased. As the Recall shows the ratio of detected intruders, the developed model demonstrates a better result than proposed in previous studies. Given the larger number of elements functioning in "normal" mode, we can say that despite the use of the proposed approach may reduce the performance of the system (speed of task execution, cost of task execution, etc.), it can also increase the probability of successful tasks' execution. The implementation of the proposed approach can be practically appropriate in case of cyber-physical systems supposed to work in an aggressive environment, for instance, in the group of UAV designed for environmental monitoring tasks [31]. The use of the proposed approach allows one to organize the verification of sensitive information and, as an example, can increase the chance of human rescue in case of emergency rescue operations.

Further work will be aimed at improving the results on other indicators. Compared to previous work [8], the results obtained in this study are more reliable, as during the experiments, the number of agents in the group was increased, and various intruders ratio were simulated. The advantage of the presented improved approach is the dynamic calculation of the Truth value. In the earlier work, such an indicator was constant in cases when it was not possible to obtain the data on the agent's preceding behavior. The advancement of the presented approach allows us to make the Truth indicator more flexible and to adjust it to the conditions of the system. In addition, further research will focus on the implementation of the proposed approach in real UAV groups designed for ground objects detection purposes.

Conclusion

In this paper, we proposed the enhanced Reputation, Trust, and Game Theory-based model to improve cyber-physical system elements' security and safety. To address the Reputation initial value calculation challenge, we described the intruders identification procedure in terms of Game Theory, applied the game concept between intruders and legitimate agents, and formalized group members strategies. The possible outcomes of using different strategies are represented with a payoff matrix. To verify our enhanced approach, we conducted an empirical study using a custom software simulator. Multiple experiments were performed with a group of agents able to interact with each other. Cases with a 10–40 % of intruders from the whole agents' group were simulated. Despite the fact that the probability to incorrectly classify a legitimate agent as an intruder increased, which also reduced the Precision metric, results analysis showed that our model implementation allowed us to significantly increase intruders detection Accuracy and to reduce the intruders incorrect classification probability compared with raw Reputation and Trust model. This specific characteristic can be vital in systems, which are not tolerant of the high risk of damage acceptance.

Our further research plans include implementation and assessing the proposed model on a developed intersection management physical testing ground, with models of autonomous vehicles, presented by us in [7]. As the previous study has shown, Reputation and Trust approach's practical implementation allows one to effectively detect "soft" attacks in the intersection management system, organized by the agents that transmit incorrect data. We assume that implementation of the proposed Game Theory mechanisms on real physical models will allow increasing "soft" attacks detection accuracy, including the cases when agents do not have retrospective data, on the basis of which they can calculate the Reputation value.

References

1. Bastos D., Shackleton M., El-Moussa F. Internet of Things: A survey of technologies and security risks in smart home and city environments. *IET Conference Publications*, 2018, vol. 2018, no. CP740. https://doi.org/10.1049/cp.2018.0030
2. Kang H.S., Lee J.Y., Choi S., Kim H., Park J.H., Son J.Y., Kim B.H., Do Noh S. Smart manufacturing: Past research, present findings, and future directions. *International Journal of Precision Engineering and Manufacturing — Green Technology*, 2016, vol. 3, no. 1, pp. 111–128. https://doi.org/10.1007/s40684-016-0015-5
3. Wolf W. Cyber-physical systems. *Computer*, 2009, vol. 42, no. 3, pp. 88–89. https://doi.org/10.1109/MC.2009.81
4. Tokody D., Albini A., Ady L., Rajnai Z., Pongrácz F. Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. *Interdisciplinary Description of Complex Systems*, 2018, vol. 16, no. 3, pp. 384–396. https://doi.org/10.7906/indecs.16.3.11
5. Kalyaev I., Gaiduk A., Kapustyan S. *Models and Algorithms of the Collective Control of Robots Group*. Moscow, Fizmatlit Publ., 2009, 278 p. (in Russian)
6. Furno L., Nielsen M.C., Blanke M. Centralised versus decentralised control reconfiguration for collaborating underwater robots. *IFAC-PapersOnLine*, 2015, vol. 48, no. 21, pp. 732–739. https://doi.org/10.1016/j.ifacol.2015.09.614
7. Chuprov S., Viksnin I., Kim I., Marinenkov E., Usova M., Lazarev E., Melnikov T., Zakoldaev D. Reputation and trust approach for security and safety assurance in intersection management system. *Energies*, 2019, vol. 12, no. 23, pp. 4527. https://doi.org/10.3390/en12234527
8. Marinenkov E., Chuprov S., Viksnin I., Kim I. Empirical study on trust, reputation, and game theory approach to secure communication in a group of unmanned vehicles. *CEUR Workshop Proceedings*, 2019, vol. 2590.
9. Gibb J.R. Trust: *A New View of Personal and Organizational Development*. Guild of Tutors Press, 1978. 320 p.
10. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation. *Proc. of the 35th Annual Hawaii International Conference on System Sciences*, 2002, pp. 2431–2439. https://doi.org/10.1109/HICSS.2002.994181
11. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proc. of the 1st International Conference on Peer-to-Peer Computing (P2P)*, 2001, pp. 101–102. https://doi.org/10.1109/P2P.2001.990434
12. *Sector S. Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Next generation networks – frameworks and functional architecture models*: Recommendation ITU-T Y 2012 / International Telecommunication Union. Switzerland, Geneva, P. 2060.
13. Singh A., Kumar M., Rishi R., Madan D. A relative study of MANET and VANET: Its applications, broadcasting approaches and challenging issues. *Communications in Computer and Information Science*, 2011, vol. 132 CCIS, part 2, pp. 627–632. https://doi.org/10.1007/978-3-642-17878-8_63
14. Chmaj G., Walkowiak K. A P2P computing system for overlay networks. *Future Generation Computer Systems*, 2013, vol. 29, no. 1, pp. 242–249. https://doi.org/10.1016/j.future.2010.11.009
15. Nojoumian M., Stinson D.R. Social secret sharing in cloud computing using a new trust function. *Proc. of the 10th Annual International Conference on Privacy, Security and Trust (PST)*, 2012, pp. 161–167. https://doi.org/10.1109/PST.2012.6297936
16. Straub J., McMillan J., Yaniero B., Schumacher M., Almosalami A., Boatey K., Hartman J. CyberSecurity considerations for an interconnected self-driving car system of systems. *Proc. of the 12th System of Systems Engineering Conference (SoSE)*, 2017, pp. 7994973. https://doi.org/10.1109/SYSOSE.2017.7994973
17. Kim I., Viksnin I. Secure information interaction within a group of unmanned aerial vehicles based on economic approach. *Advances in Intelligent Systems and Computing*, 2019, vol. 997, pp. 59–72. https://doi.org/10.1007/978-3-030-22871-2_5
18. Pham T.N.D., Yeo C.K. Adaptive trust and privacy management framework for vehicular networks. *Vehicular Communications*, 2018, vol. 13, pp. 1–12. https://doi.org/10.1016/j.vehcom.2018.04.006
19. Chuprov S., Viksnin I., Kim I., Nedosekin G. Optimization of autonomous vehicles movement in urban intersection management system. *Proc. of the 24th Conference of Open Innovations Association (FRUCT)*, 2019, pp. 60–66. https://doi.org/10.23919/FRUCT.2019.8711967

Литература

1. Bastos D., Shackleton M., El-Moussa F. Internet of Things: A survey of technologies and security risks in smart home and city environments // IET Conference Publications. 2018. V. 2018. N CP740. https://doi.org/10.1049/cp.2018.0030
2. Kang H.S., Lee J.Y., Choi S., Kim H., Park J.H., Son J.Y., Kim B.H., Do Noh S. Smart manufacturing: Past research, present findings, and future directions // International Journal of Precision Engineering and Manufacturing – Green Technology. 2016. V. 3. N 1. P. 111–128. https://doi.org/10.1007/s40684-016-0015-5
3. Wolf W. Cyber-physical systems // Computer. 2009. V. 42. N 3. P. 88–89. https://doi.org/10.1109/MC.2009.81
4. Tokody D., Albini A., Ady L., Rajnai Z., Pongrácz F. Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city // Interdisciplinary Description of Complex Systems. 2018. V. 16. N 3. P. 384–396. https://doi.org/10.7906/indecs.16.3.11
5. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: Физматлит, 2009. 278 с.
6. Furno L., Nielsen M.C., Blanke M. Centralised versus decentralised control reconfiguration for collaborating underwater robots // IFAC-PapersOnLine. 2015. V. 48. N 21. P. 732–739. https://doi.org/10.1016/j.ifacol.2015.09.614
7. Chuprov S., Viksnin I., Kim I., Marinenkov E., Usova M., Lazarev E., Melnikov T., Zakoldaev D. Reputation and trust approach for security and safety assurance in intersection management system // Energies. 2019. V. 12. N 23. P. 4527. https://doi.org/10.3390/en12234527
8. Marinenkov E., Chuprov S., Viksnin I., Kim I. Empirical study on trust, reputation, and game theory approach to secure communication in a group of unmanned vehicles // CEUR Workshop Proceedings. 2019. V. 2590.
9. Gibb J.R. Trust: A New View of Personal and Organizational Development. Guild of Tutors Press, 1978. 320 p.
10. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // Proc. of the 35th Annual Hawaii International Conference on System Sciences. 2002. P. 2431–2439. https://doi.org/10.1109/HICSS.2002.994181
11. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications // Proc. of the 1st International Conference on Peer-to-Peer Computing (P2P). 2001. P. 101–102. https://doi.org/10.1109/P2P.2001.990434
12. Sector S. Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Next generation networks – frameworks and functional architecture models: Recommendation ITU-T Y 2012 / International Telecommunication Union. Switzerland, Geneva. P. 2060.
13. Singh A., Kumar M., Rishi R., Madan D. A relative study of MANET and VANET: Its applications, broadcasting approaches and challenging issues // Communications in Computer and Information Science. 2011. V. 132 CCIS. Part 2. P. 627–632. https://doi.org/10.1007/978-3-642-17878-8_63
14. Chmaj G., Walkowiak K. A P2P computing system for overlay networks // Future Generation Computer Systems. 2013. V. 29. N 1. P. 242–249. https://doi.org/10.1016/j.future.2010.11.009
15. Nojoumian M., Stinson D.R. Social secret sharing in cloud computing using a new trust function // Proc. of the 10th Annual International Conference on Privacy, Security and Trust (PST). 2012. P. 161–167. https://doi.org/10.1109/PST.2012.6297936
16. Straub J., McMillan J., Yaniero B., Schumacher M., Almosalami A., Boatey K., Hartman J. CyberSecurity considerations for an interconnected self-driving car system of systems // Proc. of the 12th System of Systems Engineering Conference (SoSE). 2017. P. 7994973. https://doi.org/10.1109/SYSOSE.2017.7994973
17. Kim I., Viksnin I. Secure information interaction within a group of unmanned aerial vehicles based on economic approach // Advances in Intelligent Systems and Computing. 2019. V. 997. P. 59–72. https://doi.org/10.1007/978-3-030-22871-2_5
18. Pham T.N.D., Yeo C.K. Adaptive trust and privacy management framework for vehicular networks // Vehicular Communications. 2018. V. 13. P. 1–12. https://doi.org/10.1016/j.vehcom.2018.04.006
19. Chuprov S., Viksnin I., Kim I., Nedosekin G. Optimization of autonomous vehicles movement in urban intersection management system // Proc. of the 24th Conference of Open Innovations Association (FRUCT). 2019. P. 60–66. https://doi.org/10.23919/FRUCT.2019.8711967

20. Basar T., Zaccour G. *Handbook of Dynamic Game Theory*. Springer, 2018.
21. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Game theory meets information security management. *IFIP Advances in Information and Communication Technology*, 2014, vol. 428, pp. 15–29. https://doi.org/10.1007/978-3-642-55415-5_2
22. Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. A survey of game theory as applied to network security. *Proc. of the 43rd Hawaii International Conference on System Sciences (HICSS-43)*, 2010, pp. 5428673. https://doi.org/10.1109/HICSS.2010.35
23. Sun W., Kong X., He D., You X. Information security problem research based on game theory. *Proc. of the International Symposium on Electronic Commerce and Security (ISECS)*, 2008, pp. 554–557. https://doi.org/10.1109/ISECS.2008.147
24. Guo J., Chen R. A classification of trust computation models for service-oriented internet of things systems. *Proc. of the IEEE International Conference on Services Computing*, 2015, pp. 324–331. https://doi.org/10.1109/SCC.2015.52
25. Bankovic Z., Vallejo J.C., Fraga D., Moya J.M. Detecting false testimonies in reputation systems using self-organizing maps. *Logic Journal of the IGPL*, 2013, vol. 21, no. 4, pp. 549–559. https://doi.org/10.1093/jigpal/jzs028
26. Li W., Song H., Zeng F. Policy-based secure and trustworthy sensing for internet of things in smart cities. *IEEE Internet of Things Journal*, 2018, vol. 5, no. 2, pp. 716–723. https://doi.org/10.1109/JIOT.2017.2720635
27. Rawat D.B., Yan G., Bista B.B., Weigle M.C. Trust on the security of wireless vehicular Ad-hoc Networking. *Ad-Hoc and Sensor Wireless Networks*, 2015, vol. 24, no. 3-4, pp. 283–305.
28. Petrosian L.A., Zenkevich N.A., Shevkoplias E.V. *Game Theory*. St. Petersburg, BHV-Peterburg, 2012, 432 p. (in Russian)
29. Kuzin L. *Foundations of Cybernetics*. In 2 vol. Moscow, Energia Publ., 1979. (in Russian)
30. Perrone L.F., Nelson S.C. A study of on-off attack models for wireless ad hoc networks. *Proc. of the 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm)*, 2006, pp. 4138221. https://doi.org/10.1109/WOACN.2006.337180
31. Baker C.A.B., Ramchurn S., Teacy W.T.L., Jennings N.R. Planning search and rescue missions for UAV teams. *Frontiers in Artificial Intelligence and Applications*, 2016, vol. 285, pp. 1777–1778. https://doi.org/10.3233/978-1-61499-672-9-1777

20. Basar T., Zaccour G. Handbook of Dynamic Game Theory. Springer, 2018.
21. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Game theory meets information security management // IFIP Advances in Information and Communication Technology. 2014. V. 428. P. 15–29. https://doi.org/10.1007/978-3-642-55415-5_2
22. Roy S., Ellis C., Shiva S., Dasgupta D., Shandilya V., Wu Q. A survey of game theory as applied to network security // Proc. of the 43rd Hawaii International Conference on System Sciences (HICSS-43). 2010. P. 5428673. https://doi.org/10.1109/HICSS.2010.35
23. Sun W., Kong X., He D., You X. Information security problem research based on game theory // Proc. of the International Symposium on Electronic Commerce and Security (ISECS). 2008. P. 554–557. https://doi.org/10.1109/ISECS.2008.147
24. Guo J., Chen R. A classification of trust computation models for service-oriented internet of things systems // Proc. of the IEEE International Conference on Services Computing. 2015. P. 324–331. https://doi.org/10.1109/SCC.2015.52
25. Bankovic Z., Vallejo J.C., Fraga D., Moya J.M. Detecting false testimonies in reputation systems using self-organizing maps // Logic Journal of the IGPL. 2013. V. 21. N 4. P. 549–559. https://doi.org/10.1093/jigpal/jzs028
26. Li W., Song H., Zeng F. Policy-based secure and trustworthy sensing for internet of things in smart cities // IEEE Internet of Things Journal. 2018. V. 5. N 2. P. 716–723. https://doi.org/10.1109/JIOT.2017.2720635
27. Rawat D.B., Yan G., Bista B.B., Weigle M.C. Trust on the security of wireless vehicular Ad-hoc Networking // Ad-Hoc and Sensor Wireless Networks. 2015. V. 24. N 3-4. P. 283–305.
28. Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В. Теория игр. СПб.: БХВ-Петербург, 2012. 432 с.
29. Кузин Л.Т. Основы кибернетики. В 2 т. М.: Энергия, 1979.
30. Perrone L.F., Nelson S.C. A study of on-off attack models for wireless ad hoc networks // Proc. of the 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm). 2006. P. 4138221. https://doi.org/10.1109/WOACN.2006.337180
31. Baker C.A.B., Ramchurn S., Teacy W.T.L., Jennings N.R. Planning search and rescue missions for UAV teams // Frontiers in Artificial Intelligence and Applications. 2016. V. 285. P. 1777–1778. https://doi.org/10.3233/978-1-61499-672-9-1777

Authors

Ilia I. Viksnin — PhD, Associate Professor, Saint Petersburg Electrotechnical University “LETI”, Saint Petersburg, 197022, Russian Federation, SC 57191359693, https://orcid.org/0000-0001-6240-0390, wixnin@mail.ru

Egor D. Marinenkov — Scientific Researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57212198065, https://orcid.org/0000-0001-9895-239X, egormarinenkov@gmail.com

Sergey S. Chuprov — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57208318420, https://orcid.org/0000-0001-7081-8797, drmyscull@gmail.com

Авторы

Викснин Илья Игоревич — кандидат технических наук, доцент, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова, Санкт-Петербург, 197022, Российская Федерация, SC 57191359693, https://orcid.org/0000-0001-6240-0390, wixnin@mail.ru

Мариненков Егор Денисович — научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57212198065, https://orcid.org/0000-0001-9895-239X, egormarinenkov@gmail.com

Чупров Сергей Сергеевич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57208318420, https://orcid.org/0000-0001-7081-8797, drmyscull@gmail.com

Received 10.11.2021
Approved after reviewing 21.12.2021
Accepted 29.01.2022

Статья поступила в редакцию 10.11.2021
Одобрена после рецензирования 21.12.2021
Принята к печати 29.01.2022

Работа доступна по лицензии
Creative Commons
«Attribution-NonCommercial»