ВЕСТНИК ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

2022 Управление, вычислительная техника и информатика № 61

Tomsk State University Journal of Control and Computer Science

Original article
doi: 10.17223/19988605/61/11

Improving reputation and trust-based approach with reliability indicators for autonomous vehicles intergroup communication

Timofey Y. Melnikov[1], Sergey S. Chuprov[2], Eduard A. Lazarev[3], Ruslan I. Gataullin[4], Ilia I. Viksnin[5]

[1] ITMO University, St. Petersburg, Russian Federation
[2, 3, 4, 5] Electrotechnical University "LETI", St. Petersburg, Russian Federation
[1] tim_melnikov@mail.ru
[2] drmyscull@gmail.com
[3] lazarev.eduard00@gmail.com
[4] rusfiner@mail.ru
[5] wixnin@mail.ru

Abstract. Reputation and Trust models have successfully been implemented to ensure security and maintain nodes' trustworthiness in decentralized networks, including autonomous vehicles (AVs). However, the implementations of these models usually lack of objective parameters to calculate the initial Reputation values. In this study, we employ reliability-based approach to evaluate the initial Reputation value.

Keywords: Reputation; trust; reliability; autonomous vehicles; communication

***Acknowledgments*:** The work was supported by the Ministry of Science and Higher Education of the Russian Federation "Goszadanie" №075-01024-21-02 from 29.09.2021 (project FSEE-2021-0014).

***For citation*:** Melnikov, T.Y., Chuprov, S.S., Lazarev, E.A., Gataullin, R.I., Viksnin, I.I. (2022) Improving reputation and trust-based approach with reliability indicators for autonomous vehicles intergroup communication. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitelnaja tehnika i informatika – Tomsk State University Journal of Control and Computer Science*. 61. pp. 108–116. doi: 10.17223/19988605/61/11

Научная статья
УДК 519-7
doi: 10.17223/19988605/61/11

Улучшение модели репутации и доверия путем внедрения индикаторов надежности для внутригрупповой коммуникации между автономными транспортными средствами

Тимофей Юрьевич Мельников[1], Сергей Сергеевич Чупров[2], Эдуард Артемович Лазарев[3], Руслан Ильнурович Гатауллин[4], Илья Игоревич Викснин[5]

[1] Университет ИТМО, Санкт-Петербург, Россия
[2, 3, 4, 5] Государственный электротехнический университет «ЛЭТИ», Санкт-Петербург, Россия
[1] tim_melnikov@mail.ru
[2] drmyscull@gmail.com
[3] lazarev.eduard00@gmail.com
[4] rusfiner@mail.ru
[5] wixnin@mail.ru

Аннотация. Модели репутации и доверия успешно применяются для обеспечения безопасности и поддержания надежности узлов в децентрализованных сетях, включая автономные транспортные средства. Однако в реализациях этих моделей обычно отсутствуют объективные параметры для расчета начальных значе-

ний репутации. В данном исследовании предлагается подход, основанный на теории надежности, для оценки исходного значения репутации участников группы автономных транспортных средств.

Ключевые слова: репутация; доверие; надежность; автономные транспортные средства; коммуникация

***Благодарности*:** Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации «Госзадание» № 075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0014).

***Для цитирования*:** Мельников Т.Ю., Чупров С.С., Лазарев Е.А., Гатауллин Р.И., Викснин И.И. Улучшение подхода, основанного на доверии и репутации, с помощью индикаторов надежности для межгрупповой коммуникации автономными транспортными средствами // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2022. № 61. С. 108–116. doi: 10.17223/19988605/61/11

The evolution of Information and Communication technology over the past few decades has resulted in the emergence of Internet of Things (IoT) and Smart Everything concepts. These concepts are generally based on the integration of physical and information components, and on the interconnections between them. Such an integration became known as Cyber-Physical Systems (CPSs) [1]. An example of a CPS is an autonomous monitoring system that has a sensor component (e.g., camera) and a video processing component (e.g., Machine Learning classifier) that performs video classification and pattern recognition operations.

Reputation and Trust models usually find their application in the systems whose elements communicate directly with each other and are essentially decentralized. An example of such systems is peer-to-peer (P2P) computer networks, where there no central server and the nodes communicate directly with each other [2]. For the nodes of P2P networks, it can be extremely important to evaluate the information received from others in order to choose their further actions within the network (e.g., packets forwarding towards a final destination). In VANETs, the communication between AVs and infrastructure roadside units are also decentralized, and can be considered as a P2P network [3]. There are various models for man aging such networks and practical examples of their application [4].

Reputation and Trust indicators can be implemented and calculated in different ways in the context of computer systems. Generally, most of them define some quantitative indicators to evaluate how trustworthy is the agent by the other agents. Mui, Mohtashemi, and Halberstadt define Reputation as an indicator that an agent creates through their previous actions [5]. The Trust indicator, in this case, is a subjective expectation one agent has about another agent's future actions based on the history of their interactions.

The application of Reputation and Trust-based approach to AVs intergroup communication allows to improve its security and safety [6, 7]. However, Reputation and Trust approach has a substantial drawback. Let us consider two cases: AV's group initialization moment, when the agents do not have any information on the previous actions of each other; and when a new agent joins to an already existing AVs group, and the group participants also do not have any information about the new agent's previous actions. In these two cases, the initial Reputation indicator value cannot be calculated based on the previous actions or "correctness" of the transmitted data be the agents. In these scenarios, the Reputation initial value is initialized as a constant (e.g., 0.5 in [6]). This initial constant initialization allows the potential adversarial or failed agent to transmit "incorrect" before their Reputation will drop below the acceptable threshold.

To address this drawback, an approach based on Data Quality (DQ) concept was proposed [8]. This solution allows to use such data source's characteristics as accuracy and security to calculate the initial Reputation value. This solution allows to rely on not only subjective evaluation of the agent's Reputation by the other agents, but also on the objective parameters based on the agent's hardware components. Agents DQ value depends on how "well" their sensors and devices are working at the evaluation moments: if there any failures or deviations from normal, the DQ value will be decreased [8]. However, the methods on deriving these data source's parameters to calculate DQ value are highly scenario-specific and under-researched [9]. An approach partially related to evaluating of the robotic device's hardware characteristics was presented in [10]. The authors proposed to consider various probability-dependent parameters in the robotic device's control strategy, for example, a failure rate of the robotic device's subsystem. Such an approach has motivated us to investigate and develop probability-dependent parameters based on AV's device characteristics to calculate

DQ values. We base our metrics on the reliability theory [11], which considers the probability of the system's components operation failures. We assume that the "correctness" of the data transmitted by the agents is related to this probability. The less reliable the agent's components, the lower its Reputation value should be initialized, and otherwise. This approach allows us to obtain objective basis for the initial Reputation calculation, which previous models lack [6, 12].

We incorporate the terms of failure, time between failure, and probability of failure-free operation into the initial Reputation value calculus. We incorporate these terms into the previously developed Reputation and Trust approach to calculate the initial Reputation value based on AV's hardware reliability characteristics. This solution allows to rely real physical AVs characteristics with the probability of "incorrect" data production and transmission. To test the proposed approach, we verify it on a well-known real-world hardware IoT components. The contribution of this paper is twofold. First, we provide a theoretical reliability based approach to calculate the AV's initial Reputation value. The approach allows to rely the hardware characteristics and the data produced by an AV model based on these hardware. In addition, we verify the proposed approach implementation on the intersection management problem with a software simulation. The initial Reputation values for the software simulation are based on the real-world device collected hardware characteristics.

1. Initial Reputation Calculus

1.1. System Description

Let us define a group of AVs represented by the agents of decentralized network. The agents are able to communicate directly with each other according to the P2P network communication model [2]. The data agents exchange consist of their final destination and agent's current condition (e.g., current location, energy resource, etc.). The main objective of the agents' group is to safely traverse the intersection [6, 13].

We assume, that each agent's architecture includes several sub-systems, the failure of which affect the reliability agent's reliability. Such sub-systems depend on the agent's functionality and architecture. Below we provide some examples of such sub-systems.

– Communication sub-system. If an agent is disconnected from the communication channel or its communication sub-system fails, it becomes unable to update or transmit "correct" information to other agents.

– The agent's computing sub-system is responsible for the agent's decision-making. If it fails, the information transmitted by the agent cannot be considered as reliable.

– Sensing sub-system for obtaining data from the environment (e.g., camera, radar, or other sensors). Failure of this sub-system leads to the obtaining of "incorrect" data from the environment and its transmission to other agents.

Based on the probabilities of these sub-systems' failure, we propose to evaluate the agent's initial Reputation value. To formalize these probabilities, we employ the exponential distribution law [11. P. 86]. In our case, we assume that the sub-systems' failures are constantly distributed, can occurred in a random manner, and are not caused by the deterioration or aging of the agent's parts. If the agent's components are deteriorated, it will be necessary to use a different distribution, but the basic calculation principle will not change.

1.2. Initial Reputation Calculus

Here we define failure probabilities and other terms according to [11]. Probability of failure during the sub-system operation time t can be defined as (1).

$$F(t) = 1 - e^{\lambda * t}, \tag{1}$$

where λ is a constant failure rate, and e is an exponential distribution.

From (1) we can derive the equation for failure-free operation during time t (2)

$$P(t) = 1 - F(t) = e^{\lambda * t}. \tag{2}$$

The parameter λ can be calculated according to (3)

$$\lambda = \frac{1}{T_0}, \tag{3}$$

where T_0 is the mean time between failures. It is calculated as (4).

$$T_0 = \frac{\sum_{i=1}^{N} t_i}{\sum_{i=1}^{N} m_i}, \tag{4}$$

where:

– N is the total number of sub-system's components for which the indicator is calculated;

– t_i is the operating time of the i-th sub-system's element;

– m_i is the number of failures of the i-th sub-system's element for the entire operation period.

For the *i*-th agent, as the initial Reputation value R_{0ei}, we consider the probability of its non-failure operation P_{ei}. Let each i-th agent is composed of a set of sub-systems: $S_{ei} = \{s_1, \ldots, s_m\}$, and $P_{ij}(t)$ is the probability of non-failure operation of the *j*-th subsystem of the i-th agent during the time *t*, which can be calculated as (5).

$$P_{ij}(t) = e^{t*\lambda_{ij}}, \tag{5}$$

where λ_{ij} is the corresponding parameter of the *i*-th agent's *j*-th sub-system. According to (3) failure rate for (5) can be calculated according to (6).

$$\lambda_{ij} = \frac{1}{T_{0_{ij}}}, \tag{6}$$

where $T_{0_{ij}}$ is the mean time between failures of the *i*-th agent's *j*-th subsystem. Further, according to the [11. P. 120–124], we need to calculate the probability of failure-free operation for the combination of these sub-systems, which is an entire agent. To do this, we need to consider how the agent sub-systems are interrelated in terms of failures. If the sub-systems are connected in such a way, that the failure of any of them leads to the failure of the entire system, then it can be referred to a serial connection. In another case, the sub-systems are connected in a parallel manner. For such a connection, the probability of failure-free operation during the required time t_0 considering (6) can be calculated as (7).

$$P_{e_i} = \prod_{j=1}^{m} P_{ij}(t_0), \tag{7}$$

where m is the total number of the agent's sub-systems; and t_0 is the required operating time.

After that, the value calculated as (7)) can be incorporated into the Reputation calculus instead of R_0 value, described in [6]. The modified initial Reputation value can be calculated as (8):

$$R_t = \begin{cases} \prod_{j=1}^{m} P_{ij}(t_0) + \sum_{k=1}^{t} I_k, I_k > 0{,}5 \\ \prod_{j=1}^{m} P_{ij}(t_0) + \sum_{k=1}^{t} I_k - (R_{t-1} - e^{-(1-I_t)*t}), I_k < 0{,}5, \end{cases} \tag{8}$$

– $\sum_{k=1}^{t} I_k$, is the sum of Truth values for the previous iterations [6];

– R_{t-1} is the Reputation value on previous iteration;

– I_t is the Truth value on current iteration.

From the developed calculus, the following points can be derived.

1) Every Reputation model has its penalty system, when the agents with low reputation are punished in some way. Usually they are excluded from further group communication [6]. If any of the agent's sub-system is initially considered faulty (the probability of its failure-free operation is close or equal to zero), then the agent's Reputation will also be close to 0. Therefore, this agent will be excluded from the group communication after the first Reputation evaluation round. Such a scenario is true only if the sub-systems are connected serially. This means that if the key agent's sub-systems fail, the agent is excluded from the group communication.

2) The proposed initial Reputation value calculation approach sets a specified quality bar for all agent's sub-systems and their components. So, for example, if we have three serially connected sub-systems,

then to obtain an initial Reputation value of 0,5, the reliability indicators of the sub-systems should be about 0,8. With the increase in the sub-systems number, the requirements for these indicators will increase too.

3) The values obtained with (8) are always in the [0, 1] interval, as the probability of a random event is also lies in this interval.

One can see that the initial Reputation value is based on the sub-system's uptime, as we are considering the probability of uptime for a certain time *t*. This is justified by the fact that when the system is required to work longer, we will obviously impose higher requirements on the agents' reliability. Let us suppose that we have a group of agents, each of which with a high probability will not fail for an hour of real time. Then, we can employ these agents in a system that should run for half an hour. However, these agents are not enough reliable for a system that needs to run for 6 hours, for example. This fact allows us to clarify the value of the initial agent's Reputation of agents, depending on the user and/or application requirements.

2. Empirical Study

2.1. Experimental setup

To verify the proposed reliability-based Reputation calculation approach, we conduct an empirical study. First, we employ real hardware components of the AV's models developed for our previous study [6] to calculate their reliability values. Then, we integrate the developed reliability-based calculus in our intersection management simulation environment, and compare the effectiveness with the traditional constant Reputation value initialization.

Each agent has the following subsystems:

– Computing sub-system, which is a small on-board computer used by the agent for decision-making and evaluation of the received information.

– The controller sub-system, which is used to provide connectivity between the computing and other sub-systems.

– The communication sub-system, used by an agent to transmit and receive information from other group participants.

– The ultrasonic rangefinder (URF) sub-system, which is used to avoid obstacles while driving.

– The vision sub-system (on-board camera), that the agent needs for localization and mapping.

Each of these sub-systems has its reliability indicator, which depends on the probability of failure-free operation for a given time. Let us assume that the agent should work without failures within 30 minutes. Such a minor time interval is chosen in the consideration of the widely available and cheap hardware components, employed in this study. We assume, that each of the defined sub-system's depends on a particular hardware component that corresponding to this sub-system. The employed AV model's hardware components are listed below.

1) Raspberry Pi 3 single-board computer, which serves as the computing sub system. It directly receives the data from an on-board camera, and from the communication sub-system via Arduino Nano;

2) Arduino Nano is connected to the URF and communication sub-system, and serves as a controller sub-system;

3) NRF24L01 serves as a communication sub-system. It is connected to Arduino Nano via SPI;

4) URF sub-system is connected to the Arduino Nano digital outputs;

5) RaspiCam is chosen as the AV's on-board camera, and it serves as the vision sub-system. It is connected with the computing sub-system, which processes the obtained image via OpenCV.

In Fig. 1 connection between hardware components is presented.

For this empirical study, we use two previously developed AV's models with two single sets of components, listed above. We ran these two models to drive through the intersections on our testbed [6] for 30 minutes, and monitored their sub-system's failures. Usually, it is possible to determine quite accurately that one of the agent's sub-systems has failed, as, depending on the subsystem, the agent can start to transmit meaningless data or stops updating information about their actions. According to the obtained results, we

calculated the reliability indicators for both sets, which are presented in Table 1. Based on the 7 and 8, and assuming that all sub-systems are connected in series, we calculated the new initial Reputation value for two sets of sub-systems. These values are also presented in Table 1.

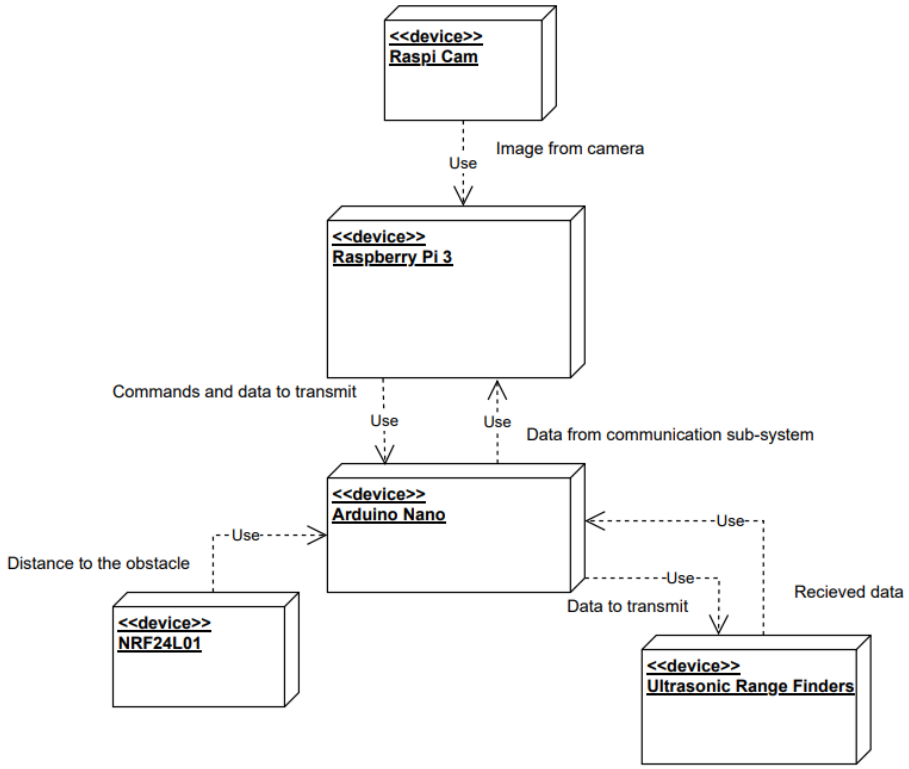

Fig. 1. Hardware connection UML-diagram

Table 1

Reliability values for the studied real hardware components

Hardware component	First set	Second set
Raspberry Pi 3	0,98	0,95
NRF24L01	0,94	0,90
Arduino Nano	0,82	0,70
Camera	0,97	0,89
Rangefinders	0,94	0,85
Reliability value	0,68	0,45

2.2. Software Simulation Assumptions

Since we have a limited number of AVs models, we leveraged the software simulator for the AVs intersection management system [14]. We used the Reputation values obtained with the hardware components to initialize agents' Reputation indicators. Let us assume that about half of the agents in the system have subsystems' reliability indicators higher than 0,5, and the other half have lower than 0,5.

The simulation parameters can be represented as follows.

1) Two groups of experiments were conducted: with the constant Reputation initialization (0,5); and based on the calculated reliability characteristics.

2) In both experiment groups, there were two sub-groups: for each values calculated based on the studied hardware set.

3) A group of 20 agents operates in the system. The main objective of the agent is to safely and optimally traverse the intersection. Detailed simulation environment description is provided in [14, 15].

4) 1000 iterations of the simulation are conducted for each sub-group.

5) Initially agents in the group have different reliability indicators for their sub systems. To avoid setting the same reliability values for different agents, we took values from Table 1 and randomly distribute it over the agents. As we studied two hardware sets, we divided our agents into two sub-groups of 10 participants: with initially more reliable components, and with less reliable ones. The reliability values are initialized in the range of 0,65 – 0,72 for the first sub-group, and in the range of 0,42 – 0,45 for the second set.

6) Agents' sub-systems can fail in the operation process with a probability corresponding to the exponential distribution law. The parameter λ for a given distribution law is obtained from the reliability indicators of agent sub-systems. After sub-system fails agent starts transmitting "incorrect" data. Data is considered "incorrect" when it does not represent the real condition of the agent or surrounding environment.

7) Agents are able to determine when one of their subsystem fails.

8) The assumed uptime for all agent's subsystems is set to 30 minutes, and every 30 seconds agents communicate with each other and perform one round of the Reputation values calculation.

9) When agent's Reputation drops below the 0,3 threshold, they are excluded from the group communication.

2.3. Results

As an evaluation criteria, we considered the following ones: average time T_{avg} and its standard deviation σ_T of the agents' operation during the experiment; and the average time required to exclude failed agent from the group communication T_{err_avg} and its standard deviation σ_{T_err}. Moreover, to investigate the effect of reliability-based Reputation indicators affect the operation time of the agents. To address this question, we calculate the linear correlation coefficient between the time spent by agents in the system and their initial reputation value r_{trep}. The empirical study results are represented in Table 2.

Table 2

Empirical study results

Initial Reputation calculus	Components' set	T_{avg}, sec	σ_T, sec	T_{err_avg}, sec	σ_{T_err}, sec
Realibility-based	First set	1453	387	827	701
	Second set	1030	395	602	554
Constant-based (0,5)	First set	1374	417	787	744
	Second set	1081	431	643	600

In Fig. 2 The relationship between the agent's initial Reputation value and the time of agent's operation in the system is presented.

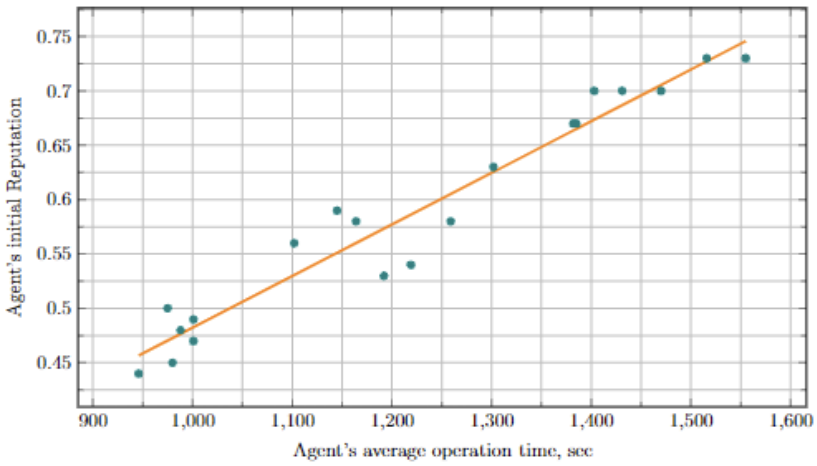

Fig. 2. The relationship between the agent's initial Reputation value and the time of agent's operation in the system (dots – initial Reputation and time values, orange line – linear regression)

As one can see from the obtained results, the employment of reliability indicators allows to slightly decrease average time to exclude agents that provide "incorrect" data due to sub-systems failures. The linear

correlation coefficient between the overall average agent's operation time (calculated based on both sub-groups), and initial reliability indicator is r_{trep} = 0,97, which can be interpreted as a strong relationship between the initial reliability indicators and the agent's operation time. Moreover, it can be seen that in all cases with reliability indicators, the standard deviation de creases. This can be interpreted by the fact that all agents are initially divided into two groups according to the initialized Reputation values. Thus, the spread of values both for the time spent in the system and for the agent's exclusion from the group communication decreased.

The results on correlation allows us to say that with reliability indicators it becomes possible to predict the average time of how long the agent with a specified reliability value will operate in the system. With the traditional Reputation initialization approach, such prediction is impossible, as there is no objective indicators can be used. In addition, reliability-based approach allows to reduce the time to exclude a failed agent from the group communication.

Conclusion

In this paper, we proposed to integrate reliability indicators to improve Reputation and Trust-based approach for AVs intergroup communication. Reputation and Trust models have found its implementation to enhance security in VANETs. However, these models has a substantial security gap – they rely on retrospective actions of the agent, and the initial Reputation value are usually set as a constant. In our preliminary research, we developed various approaches to address this issue [8, 12], but the direct relationships between the "correctness" of the data produced by the AVs and its hardware components were not considered in those studies. In this study, we employ reliability indicators to assess the AVs hardware parameters and to use these parameters to define initial Reputation value. We lever aged terms and models from the reliability theory and integrated them into the initial Reputation value calculus. Furthermore, to verify the reliability-based approach, we conducted an empirical study, We employed two real-world AVs models, developed in our preliminary intersection management research, and used its hardware components to empirically obtain reliability indicators. Furthermore, we conducted a set of software simulations to investigate the effect of the developed calculus against tradition Reputation initialization. The results showed that in the reliability-based approach the initial reliability indicator and the agents operation time are strongly correlated with each other (0,94). In addition, the approach allowed to decrease the time for exclusion failed agents' from the intergroup communication.

References

1. Wolf, W. (2009) Cyber-physical systems. *Computer.* 42(03). pp. 88–89.
2. Schollmeier, R. (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE. pp. 101–102.
3. Verma, A., Raghavendra, P., Arun, P. & Rajeev, T. (2018) Information retrieval in two-tier VANET/P2P using RSU as a super-peer. *Wireless Communication Technology*. 2(1). pp. 1–9.
4. Kalyaev, I.A., Gaiduk, A.R. & Kapustyan, S.G. (2009) *Models and Algorithms of Collective Control in Groups of Robots.* Moscow: Fizmatlit.
5. Lik, M., Mohtashemi, M. & Halberstadt, A. (2002) A computational model of trust and reputation. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. pp. 2431–2439. DOI:10.1109/HICSS.2002.994181
6. Chuprov, S.S., Viksnin, I.I., Kim I.V., Marinenkov, E.D., Usova, M., Lazarev, E.A., Melnikov, T.Y. & Zakoldaev, D. (2019) Reputation and trust approach for security and safety assurance in intersection management system. *Energies*. 12(23). 4527. pp. 1–19.
7. Viksnin, I.I., Iureva, R.A., Komarov, I.I. & Drannik, A.L. (2016) Assessment of stability of algorithms based on trust and reputation model. *2016 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT)*. IEEE. pp. 364–369.
8. Chuprov, S., Viksnin, I., Kim, I., Resnikand, L. & Khokhlov, I. (2020) Reputation and trust models with data quality metrics for improving autonomous vehicles traffic security and safety. *2020 IEEE systems security symposium (SSS)*. pp. 1–8. DOI: 10.1109/SSS47320.2020.9174269
9. Pipino, L.L., Lee, Y.W. & Wang, R.Y. (2002) Data Quality Assessment. *Communications of the ACM*. 45(4). pp. 211–218. DOI: https://doi.org/10.1145/505248.506010
10. Thrun, S., Burgard, W. & Fox, D. (2005) *Probabilistic Robotics*. 492 p. [Online] Available from: https://docs.ufpr.br/~danielsantos/ProbabilisticRobotics.pdf

11. Gnedenko, B.V., Belyaev, Yu.K. & Solovyev, A.D. (2014) *Mathematical Methods of Reliability Theory*. Academic Press.
12. Marinenkov, E., Chuprov, S., Viksnin, I. & Kim, I. (2020) Empirical study on trust, reputation, and game theory approach to secure communication in a group of unmanned vehicles. *CEUR Workshop Proceedings.* 2590. Paper 28. pp. 1–12.
13. Dresner, K. & Stone, P. (2008) A multiagent approach to autonomous intersection management. *Journal of Artificial Intelligence Research*. 31. pp. 591–656.
14. Chuprov, S., Viksnin, I., Kim, I. & Nedosekin, G. (2019) Optimization of autonomous vehicles movement in urban intersection management system. *Proceedings of the 24th Conference of Fruct Association.* St. Petersburg, Russia. pp. 60–66.
15. Chuprov, S., Viksnin, I., Kim, I., Tursukov, N. & Nedosekin, G. (2020) Empirical study on discrete modeling of urban intersection management system. *International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*. 11(2). pp. 16–38. DOI: 10.4018/IJERTCS.2020040102

***Information about the authors*:**
Melnikov Timofei Yu. (Student of the Faculty of Secure Information Technologies of the National Research University ITMO, St. Petersburg, Russian Federation). E-mail: tim_melnikov@mail.ru
Chuprov Sergey S. (Software Developer in MIS Laboratory, The Institute of A.S. Popov, Electrotechnical University "LETI", St. Petersburg, Russian Federation). E-mail: drmyscull@gmail.com
Lazarev Eduard A. (Technician in MIS Laboratory, The Institute of A.S. Popov, Electrotechnical University "LETI", St. Petersburg, Russian Federation). E-mail: lazarev.eduard00@gmail.com
Gataullin Ruslan I. (Software Developer in MIS Laboratory, The Institute of A.S. Popov, Electrotechnical University "LETI", St. Petersburg, Russian Federation). E-mail: rusfiner@mail.ru
Viksnin Ilia I. (Candidate of Technical Science, Researcher in MIS Laboratory, The Institute of A.S. Popov, Electrotechnical University "LETI", St. Petersburg, Russian Federation). E-mail: wixnin@mail.ru

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

***Информация об авторах*:**
Мельников Тимофей Юрьевич – студент факультета безопасности информационных технологий Национального исследовательского Университета ИТМО (Санкт-Петербург, Россия). E-mail: suncheture@gmail.com
Чупров Сергей Сергеевич – программист лаборатории МИС Института им. А.С. Попова Санкт-Петербургского государственного электро-технического университета «ЛЭТИ» (Санкт-Петербург, Россия). E-mail: drmyscull@gmail.com
Лазарев Эдуард Артемович – техник лаборатории МИС Института им. А.С. Попова Санкт-Петербургского государственного электро-технического университета «ЛЭТИ» (Санкт-Петербург, Россия). E-mail: lazarev.eduard00@gmail.com
Гатауллин Руслан Ильнурович – программист лаборатории МИС Института им. А.С. Попова Санкт-Петербургского государственного электро-технического университета «ЛЭТИ» (Санкт-Петербург, Россия). E-mail: rusfiner@mail.ru
Викснин Илья Игоревич – кандидат технических наук, научный сотрудник лаборатории МИС Института им. А.С. Попова Санкт-Петербургского государственного электро-технического университета «ЛЭТИ» (Санкт-Петербург, Россия). E-mail: wixnin@mail.ru

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Received 24.05.2022; accepted for publication 29.11.2022

Поступила в редакцию 24.05.2022; принята к публикации 29.11.2022