Empirical Study on Trust, Reputation, and Game Theory Approach to Secure Communication in a Group of Unmanned Vehicles

Egor Marinenkov[0000−0001−9895−239X], Sergey Chuprov[0000−0001−7081−8797], Ilya Viksnin[0000−0002−3071−6937], and Iuliia Kim[0000−0002−6951−1875]

ITMO University, Saint-Petersburg, Russia
egormarinenkov@gmail.com, chuprov@itmo.ru, wixnin@mail.ru, yulia1344@gmail.com

Abstract. The paper presents an approach based on a combination of Reputation, Trust, and Game Theory to ensure secure data transfer in distributed networks of unmanned autonomous vehicles. Trust and Reputation-based approaches have gained popularity in computer networks to improve their security. The existence of "soft" attacks, when the initiator of the attack is a legitimate agent, and traditional means of protecting information are powerless, it is possible to use methods based on trust. Using Game Theory approaches in cybersecurity allows optimizing intrusion detection and network security systems. In this paper, we reviewed the foundations of Trust and Reputation-based models, and Game Theory approaches in computer systems and attempts of its implementations in distributed network security and communication protocols. We described the operating conditions of a group of AVs, elaborated an apparatus for calculating the indicators of Trust and Reputation, and presented an approach based on a combination of Game Theory with Trust and Reputation. To validate the effectiveness of the proposed approach a custom software simulator was developed. Experiments with a group of AVs driving through the intersection was conducted. The results showed that a combination of Trust, Reputation and Game Theory allows more effective detection of bogus data, transmitted by the agents in a system.

Keywords: Trust · Reputation · Game Theory · Multi-agent System

1 Introduction

With the development of global technological progress, robotic systems are beginning to be applied in various areas of human life. Auto manufacturers are actively researching the development and integration of AVs on the roads of our

cities. Small unmanned aerial vehicles (drones) have become widespread in everyday life and can be used for a variety of purposes: from searching for missing people to farming. One of the main advantages of AVs is the ability to perform complex, dangerous and monotonous for humans' organism tasks. To perform some tasks, it is more promising to use groups of fully autonomous robots capable of functioning without a human-operator and more efficiently performing tasks distributed in the area.

Each robotic device can be represented as a combination of physical and information components, called the cyber-physical system [8]. To study groups of autonomous robotic devices, a multi-agent approach has gained popularity [1]. In this approach, all robots are represented by a set of agents capable of interacting with each other and performing common, group tasks. For optimal planning of group actions, they can use the data obtained with the sensors from the environment and transmit them to each other via a wireless communication channel. However, as with any network, the transmitted data between elements may be subject to security threats.

2 Literature Review

2.1 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 rules of behavior on a resource. Violation of such rules and norms by the user will lead to a decrease in the indicator of his reputation, as well as to a decreasing trust to him from other users. For example, if one of the sellers of the online store selling a product that has characteristics different from the declared ones, or the delivery time did not correspond to the expected one, it is less likely that buyers will want to buy goods from him if there are other sellers who are more trustworthy.

Depending on the sources, interpretations of Trust and Reputation (T&R) may vary slightly. The content of these concepts goes deep into antiquity, with the advent of the first groups of people and the interaction between them, those concepts also appeared that can now be described as T&R. The work [6] 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 a history of interactions. 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 follows 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 the history of his behavior 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 observations or assessments of group members.

To use the approach based on T&R in information systems, it is necessary to formalize and take into account quantitative indicators of T&R 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 are called peer-to-peer (P2P) networks [15]. P2P networks have gained widespread popularity with the advent of the Internet of Things (IoT) concept [16] and vehicular (VANETs) and mobile (MANETs) ad-hoc networks [17]. P2P allows to transfer and process large amounts of information, at a cost lower than using a centralized infrastructure network [3]. However, due to the decentralized structure, the presence of heterogeneous elements and specific features, such networks are subject to "soft" attacks aimed at the contextual integrity of the transmitted data between nodes. "Traditional" cybersecurity methods, such as authentication or cryptography, are not effective against such attacks.

In the case of AVs, 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 offering T&R-based data security techniques may offer different approaches to calculating these metrics. For example, the authors of [11] suggest calculating the trust indicator in the range from -1 to 1, when, as in [4], it is proposed to calculate the T&R indicators in the range from 0 to 1. It is worth noting that in the present paper we use the calculus described in [4] and complement it with an approach based on Game Theory.

In [18] Starub et al. proposed a multi-level intrusion detection system (IDS) to protect self-driving vehicles from malicious attacks, as well as false data. The system is based on the method of determining the reputation of nodes. The system contains shared knowledge generated by all communication participants. The level of reputation depends on the history of the behavior of one or another node. Despite the interesting system architecture proposed by the authors, it is difficult to evaluate the effectiveness of the proposed solution. The work lacks both calculus to calculate the reputation level, as well as validation of the effectiveness of the solution and comparison with other existing T&R-based approaches.

Kim and Viksnin in [7] proposed a method for calculating T&R, based on the theory of loans to ensure the security of flying drones communication. The idea of the method is that it would be unprofitable for the saboteur to perform a destructive impact on the group. In case the agent transmits incorrect information, its indebtedness increases. The results of the experiments showed that the intruder transmitting incorrect data was blocked in 90.2% cases.

To verify the reliability of the data, two approaches are proposed in the papers: objective and subjective. In the second case, the nodes rely on the opinion of other nodes to form a trust indicator. In [13], the authors addressed the data privacy problem when calculating the trust of the nodes and proposed a framework that allows finding a balance between trust and privacy in the system. Experiments conducted using the ONE network simulator showed that the use of the proposed linkability protocol can increase the privacy of transmitted data by using pseudonyms for nodes and offers more flexibility than the standard secure broadcast authentication protocol used in the ONE simulator.

2.2 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 [2].

One of the tasks of Game Theory implementation in the field of cybersecurity is to optimize the actions of the security administrators in network systems. In the context of Game Theory, this task can be formalized as follows: there are two coalitions: defenders (administrators) and attackers; the goal of administrators is to minimize damage to the system by optimally distributing tasks among themselves, and the goal of the attackers is to exploit the system. Considering the different behavior of attackers, it is possible to identify such strategies for the behavior of administrators (both for a coalition and for each administrators), in which, regardless of the attackers strategy, the damage to the system will be minimal. One of the approach was described in the [5]. The authors found a strategy in which Nash equilibrium is achieved, which guarantees an optimal solution to the defending side, regardless of the attackers decisions. The authors conducted a comparative analysis of approaches to ensuring a safety circuit based on Game Theory and common sense decision algorithms. To verify the developed model, real statistics were used from Hackmageddon, the Verizon 2013 Data Breach Investigation report, and the Ponemon report of 2011.

In [14] Roy et al. provide an overview of the game-theoretic models application for network security assurance. Authors review static games and divide them into complete imperfect information and incomplete imperfect information games. In the former type of game, the authors cite the example of an information war and a quantitative risk assessment for effective investment decisions in the field of cybersecurity. The latter gave examples of games in the framework to counter DDoS and intrusions in ad-hoc networks. The authors also analyze dynamic games and subdivide them into 4 types: complete perfect information, complete imperfect information, incomplete perfect information and incomplete imperfect information games. The first type of games 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

to determine the optimal strategy for several iterations, which allows to optimally distribute resources for long periods of time. For the second type, an IDS and several scenarios, based on the completeness of knowledge about the system by attackers were considered. This approach allows to determine the optimal strategies for the players, which can subsequently be applied as a deciding rule when implementing or modifying such a system. Third type described a game in which network participants reduce the propagation speed of a worm-attack, which allows to scan a system for important and valuable information. In the fourth type, games like admin-attacker were also considered. The described paper is interesting in the way that it considers Game Theory applications under various conditions of density and correctness of the available data from players.

In [19] Game Theory is used for security assurance in electronic commerce applications. The authors describe the security game model using the penalty parameter, calculate replicator dynamics, and analyze the evolutionary stable strategy of the game model. As a result, the authors conclude that reducing the cost of investment leads to the stimulation of investment in cybersecurity. With an increase in investment costs, the penalty parameter allows to save the incentive for investments.

The described papers on T&R and Game Theory approaches show the expediency of applying such approaches in the areas related to distributed networks and automated systems. We have already published works on the results of applying T&R in the group of AVs, and we believe that refining this approach using Game Theory fundamentals will help to achieve better results.

3 Problem Statement

There are various types of attacks on data transferred between agents in the system. Attacks can be both passive when the attacker does not directly influence the system, or active when an unauthorized modification of information assets, system properties, and its state occurs during the attack. As a means of counteracting these malicious attacks, various defenses can be used. However, there are some attacks when agents already authorized in the system, which were initially considered legitimate, begin to transmit inaccurate data due to the failure of the sensors or unauthorized interference with the hardware and software components. Using these improper data to optimize group actions can lead to a decrease in the efficiency of the system, and in the case of groups of AVs, it can lead to a traffic accident. Such attacks on context data integrity are called “soft” attacks in the literature [20].

To counter “soft” attacks on multi-agent systems, a T&R approach that has gained popularity in the field of e-commerce can be used [12, 9]. In this paper, we address the problem of contextual data integrity in the group of mobile robots and propose a model, based on T&R indicators using elements of the Game Theory. The next section describes our approach in more detail.

4 Our Approach, Based on Trust, Reputation and Game Theory

First of all, it is necessary to describe the limitations, assumptions, and operating conditions of the system to which the described calculus can be applied to calculate the T&R indicators of the agents. The group of AVs can be described as a set $E = \{e_1, e_2, \ldots, e_n\}$ of agents. The process of system functioning can be described as a discrete process, and accordingly consists of many states $T = \{t_0, \ldots, t_{end}\}$, where t_0 is the initial moment, and t_{end} is the endpoint in time. At each moment of time, the agents transmit to each other data on their location and state of the surroundings. Agents obtain these data using on-board sensors. These data are necessary for further planning and optimization of group actions, the description of which is beyond the scope of this paper. As an assumption, we consider the transfer of data between agents in ideal conditions, that is, without loss and interference.

The transmitted data can be either correct or bogus. 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 bogus due to breakdown, failure of the sensors or malicious interference with the software and hardware components of the agent e_i.

To identify agents that transmit bogus data, we propose the following procedure based on T&R assessment. Each of the group agents has an indicator of T&R. The assessment is based on the transmitted data verification at each time moment t by other agents. To describe our approach, we need to introduce three indicators: Truth, Trust, and Reputation.

4.1 Truth, Trust, and Reputation

$Truth$ - 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 (1).

$$Truth_t = f_{tr_t}(data), \tag{1}$$

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 time t.

Reputation (R) is an indicator based on a retrospective of the $Truth$ assessment of each agent. It can be described as (2).

$$R_t = f_{r_t}(Truth_t) = f_{r_t}(f_{tr_t}(data)), \tag{2}$$

where R_t is the reputation value at the time t, f_{r_t} is the evaluation function of R at the time t.

$Trust$ is an indicator characterizing a subjective assessment of agent behavior by other agents. It is calculated based on a combination of $Truth$ and R and can be represented as (3).

$$Trust_t = f_{trust_t}(R_{t-1}, Truth_t) = f_{trust_t}(f_{r_{t-1}}(f_{tr_{t-1}}(data)), f_{tr_t}(data)), \quad (3)$$

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

As a limitation, each of the above indicators is in the range of $[0, 1]$. However, in the process of functioning of the system, situations may arise 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 in the t_0 time moment (initialization of the system), when agents are distributed over the area and they do not have a retrospective assessment, or when a new agent joins the group. As an assessment mechanism in such situations, we propose using the approach based on the Game Theory described below.

4.2 Game Theory

In the context of Game Theory, a game will be understood as a confrontation between two agents: G - a trusted agent that receives data, and U - an agent that transfers data. Players have two strategies. For agent G: strategy 1 - trust to the agent U, and strategy 2 - do not trust to the agent U. For agent U: strategy 1 - transmit correct data, and strategy 2 - transmit bogus data. In order to consider the game in normal form and express it through the payment matrix, payments when the players win/lose can be designed.

Since agent G cannot confirm or refute the data at the time of its receipt, it is necessary to consider the risk of losing reliable data. For this, it is necessary to introduce the concept of the value of data. Let $data_i \in DATA$ be the kind of information existing inside the system. Then $\exists\ v(data_i) : v(data_i) \neq v(data_j), i \neq j$ is the maximum value of the data i. We consider the fact, that the value of data decreases with time, and it is necessary to introduce the concept of the value of data at time t. Let $\exists\ t_f : 0 < t_f \leq t$ be the time point for receiving data, then $\exists\ v(data_i, t_f, t) : v(data_i, t_f, t) \leq v(data_i)$ is the value of the data i at the time t. It can be calculated by the equation (4).

$$v(data_i, t_f, t) = v(data_i) \times k_{data_i}(t_f, t), \quad (4)$$

where $k_{data_i}(t_f, t)$ is the function of relevance of the data i at time t.

We consider $k(t_f, t) \neq 0$ as long as the agent cannot refute the data, therefore, we chose an exponential function of the form a^x, presented in (5) for calculating the actuality of the data.

$$k_{data_i}(t_f, t) = (a_{data_i})^{t-t_f}, \quad (5)$$

where $a_{data_i} \in (0; 1)$. Therefore, $k_{data_i}(t_f, t) \in (0; 1]$.

Based on the foregoing, agent's payoff function G can be described by the equation (6).

$$f_G(x,y) = \begin{cases} v(data_i) & \text{x = 1, y = 1} \\ 0 & \text{x = 1, y = 2} \\ v(data_i, t_f, t) & \text{x = 2, y = 1} \\ v(data_i, t_f, t) & \text{x = 2, y = 2} \end{cases}, \tag{6}$$

where x, y is the number of agents' G and U strategies.

For the agent U, the biggest gain will be the the value $Truth(data_i) = 1$ of the agent G, in the case when the agent U lied, and minimal - when the agent G has trust to U, and U provided him with correct data. To denote the wins of the agent U, we introduce the payoff function, presented in (7).

$$f_U(x,y) = \begin{cases} -1 & \text{x = 1, y = 1} \\ 1 & \text{x = 1, y = 2} \\ 0 & \text{x = 2, y = 1} \\ 0 & \text{x = 2, y = 2} \end{cases}, \tag{7}$$

where x, y is the number of agents' G and U strategies. In the Table 1 the payment matrix of the game is represented.

Table 1. Game payoff matrix.

		Player U	
		Strategy 1	Strategy 2
Player G	Strategy 1	$v(data_i); -1$	$0; 1$
	Strategy 2	$v(data_i, t_f, t); 0$	$v(data_i, t_f, t); 0$

We assume that the agent U is rational in its actions with respect to G. Let us consider the resulting winnings. It can be seen from the Table 1 that the game has Nash equilibrium, namely, the outcome when agent U chooses strategy 2, and agent G chooses strategy 2. In this case, the equilibrium exists because agents cannot increase their winnings when the opponent does not change strategies.

Consequently, the agent U, if he is an intruder, will prefer to lie, since his winnings will fluctuate from 0 to 1, but not from -1 to 0. In turn, the agent G needs to understand that he will not receive the maximum win, no matter what strategy U agent chooses, the winnings will be stable. Thus, the authors formed the third condition for the formation of $Truth$ indicator - in the case when it is not possible for the agent to verify the information personally or by asking other trusted agents, the agent must not be trusted and $Truth(data_i) = 0$.

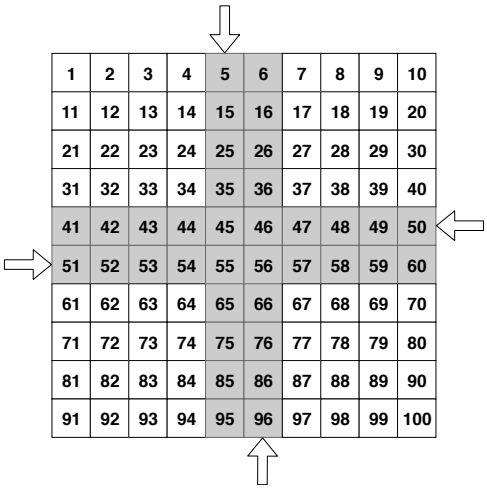

Fig. 1. Model of intersection and schematic representation of the vehicles' driving direction.

5 Software Simulation

To validate the effectiveness of our Game Theory approach implementation in a group of AVs, custom software simulator was developed. In the simulator, the movement of vehicles through an intersection was imitated. 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).

The experiment was conducted with a group consisted of 3 vehicles (agents): one of them was a saboteur and provided incorrect data to the other agents. The communication in the group was organized in the following way:

- depending on a situation, the saboteur can either transmit correct of bogus data;
- legitimate agents also can provide others with bogus data in case of technical problems; the probability of technical fail occurrence was set as 0.1;
- the initial value of agent reputation (R) was equal to 0.5;
- the agent that had the R value equal or less than 0.25 was considered as a saboteur and blocked from the group communication; such threshold was set because of the short communication period in the intersection;
- the information transmitted by one vehicle could be assessed only if this vehicle was visible to one of the trusted agents; the vehicle can detect others if they are located in one of the 8 adjacent sectors around it.

For the experiment, we decided to use a group of three AVs. Since one AV can detect objects in 8 sectors around itself, in order to ensure the correct operation of the T&R-based method, three members of the group are enough on this software testing ground. An increase in the number of group participants at the intersection will lead to the possibility of using agent's own observations, rather than relying on the proposed method.

Experiment setup:

- the experiment had 1000 independent tests;
- during each test, the movement of the vehicle group through the intersection was analyzed.

Results assessment:

- to assess the obtained results, 4 parameters were calculated:
  - True Positive (TP) - case when the AV was a saboteur and it was classified as a saboteur;
  - False Positive (FP) - case when the AV was not a saboteur but was classified as a saboteur;
  - True Negative (TN) - case when the AV was a legitimate agent and was classified as a correct agent;
  - False Negative (FN) - case when the AV was a saboteur and was classified as a legitimate agent.
- based on these values, a classification parameter *Accuracy* was calculated, as in (8).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{8}$$

The comparative analysis between 2 models was performed:

- model with standard T&R-based approach;
- model with T&R and integrated Game Theory approach.

The average results after 1000 independent tests are represented in Fig. 5. Our T&R and Game Theory approach contributed to the increase of saboteur detection accuracy: it is possible to note that the *Accuracy* parameter raised by 0.1. Moreover, implementation of Game Theory provided a significant increase in TP agent classification cases and helped to reduce FN rate values. However, the rise of FP errors and decrease of TN rate was noted. The reason of these deviations is that the Game Theory approach does not give an opportunity to set up a median $Truth$ level not only to saboteurs but also to legitimate agents.

6 Acknowledgments

This article was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation under the agreement No. 075-15-2019-1707 from 22.11.2019 (identifier RFMEFI60519X0189, internal number 05.605.21.0189).

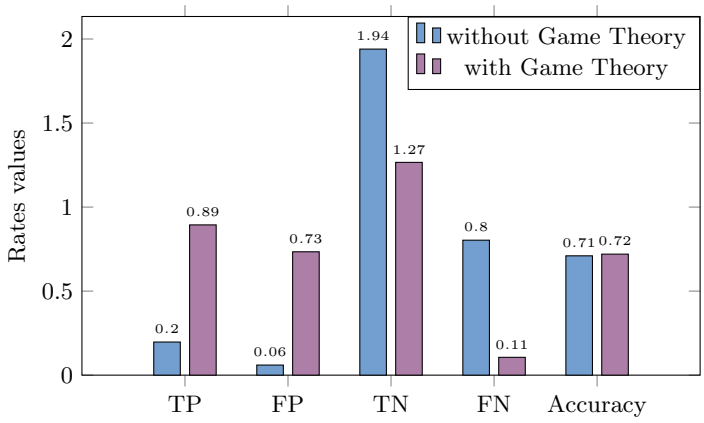

Fig. 2. Average True Positive, False Positive, True Negative, False Negative, and calculated Accuracy values on 1000 testing runs and its comparison with and without using Game Theory approach.

7 Conclusion

In this paper, we proposed an approach based on a combination of Trust, Reputation, and Game Theory fundamentals to secure communication in a group of unmanned vehicles. In addition to traditional attacks on data in distributed networks, there are also "soft" attacks when legitimate agents broadcast bogus data, which may be due to technical problems or unauthorized malicious access to the agent's hardware and software. The paper describes the characteristics and assumptions of a group of unmanned vehicles in which the implementation of the presented model is possible. To validate the effectiveness of the presented approach in a group of unmanned autonomous vehicles, we developed custom software simulator. Simulator allows to imitate traversal of the intersection by a group of AVs and communication between them. Despite the fact that the classification accuracy of saboteurs, transmitted bogus data, increased by 0.1, using of the T&R in a combination with Game Theory approach allowed to significantly increase the True Positive and reduce False Negative values.

References

1. Akhtar, N., Missen, M.M.S.: Contribution to the formal specification and verification of a multi-agent robotic system. arXiv preprint arXiv:1604.05577 (2015)
2. Başar, T., Zaccour, G.: Handbook of Dynamic Game Theory. Springer (2018)
3. Chmaj, G., Walkowiak, K.: A p2p computing system for overlay networks. Future Generation Computer Systems **29**(1), 242–249 (2013)
4. 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 **12**(23), 4527 (2019)

5. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.: Game theory meets information security management. In: IFIP International Information Security Conference. pp. 15–29. Springer (2014)
6. Gibb, J.R.: Trust: A new view of personal and organizational development. Guild of Tutors Pr (1978)
7. Kim, I., Viksnin, I.: Secure information interaction within a group of unmanned aerial vehicles based on economic approach. In: Intelligent Computing-Proceedings of the Computing Conference. pp. 59–72. Springer (2019)
8. Lee, E.A.: Cyber physical systems: Design challenges. In: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). pp. 363–369. IEEE (2008)
9. Melnikov, A., Lee, J., Rivera, V., Mazzara, M., Longo, L.: Towards dynamic interaction-based reputation models. In: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). pp. 422–428. IEEE (2018)
10. Mui, L., Mohtashemi, M., Halberstadt, A.: A computational model of trust and reputation. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences. pp. 2431–2439. IEEE (2002)
11. Nojoumian, M., Stinson, D.R.: Social secret sharing in cloud computing using a new trust function. In: 2012 Tenth Annual International Conference on Privacy, Security and Trust. pp. 161–167. IEEE (2012)
12. Pathan, A.S.K.: Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press (2016)
13. Pham, T.N.D., Yeo, C.K.: Adaptive trust and privacy management framework for vehicular networks. Vehicular Communications **13**, 1–12 (2018)
14. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A survey of game theory as applied to network security. In: 2010 43rd Hawaii International Conference on System Sciences. pp. 1–10. IEEE (2010)
15. Schollmeier, R.: A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proceedings First International Conference on Peer-to-Peer Computing. pp. 101–102. IEEE (2001)
16. SECTOR, S., ITU, O.: Series y: Global information infrastructure, internet protocol aspects and next-generation networks next generation networks–frameworks and functional architecture models. International Telecommunication Union, Geneva, Switzerland, Recommendation ITU-T Y **2060** (2012)
17. Singh, A., Kumar, M., Rishi, R., Madan, D.: A relative study of manet and vanet: Its applications, broadcasting approaches and challenging issues. In: International Conference on Computer Science and Information Technology. pp. 627–632. Springer (2011)
18. 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. In: 2017 12th System of Systems Engineering Conference (SoSE). pp. 1–6. IEEE (2017)
19. Sun, W., Kong, X., He, D., You, X.: Information security problem research based on game theory. In: 2008 International Symposium on Electronic Commerce and Security. pp. 554–557. IEEE (2008)
20. Zikratov, I.A., Lebedev, I.S., Gurtov, A.V.: Trust and reputation mechanisms for multi-agent robotic systems. In: International Conference on Next Generation Wired/Wireless Networking. pp. 106–120. Springer (2014)