Vulnerabilities, Points of Failure and Adaptive Protection Methods in the Context of Group Control of Unmanned Vehicles

A.Yu. Iskhakov$^1$ and M.V. Mamchenko$^1$

$^1$ V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Profsoyuznaya str. 65, 117342 Moscow, Russia

E-mail: iskhakovandrey@gmail.com, markmamcha@gmail.com

Abstract. Continuous improvements in the hardware, software and algorithms of unmanned vehicles (UVs) are nearing their mass deployment in all physical environments, including within unmanned groups, and with traditional means of transport controlled by the operators (drivers). Notwithstanding the measures taken to improve security and resilience, UVs as complicated cyberphysical systems have a number of vulnerabilities and failure points. This paper comprises the review of known vulnerabilities and failure points (including those in group control scenarios), and the development of the proposals to improve the resilience and security of UVs, and addresses the identified issues.

Introduction

At present, the idea of mass use of UVs, including the application in the «smart city» environment, is the most promising concept for the transport system of the future. The term «unmanned vehicles» applies equally to ground, aerial, and maritime autonomous unmanned vehicles and systems. It is obvious that the use of UVs on the routes by the enterprises will lead to the necessity of combining them into homogeneous and heterogeneous groups carrying out transportation tasks completely autonomously [1].

The most pressing issue is the safe operation of single UVs and their groups for the passengers, cargo transported, and other traffic participants, but both vulnerabilities that can be exploited by the attacker and failure points in various subsystems of the UVs threaten the very reliability of their autonomous exploitation. The proposed work focuses on the review and analysis of vulnerabilities and points of failure of the UVs and their subsystems, as well as on the proposals to increase their resistance and protection against unauthorized external influences and internal malfunctions. Thus, along with the description of the vulnerabilities and scenarios of typical attacks on the UVs, we will propose possible scenarios of failure of the autonomous vehicles, including the scenarios for UVs group engagement.

1. Unmanned Vehicles Group Control

UV group control involves the formation of homogeneous or heterogeneous groups. A homogeneous group consists of several identical autonomous unmanned vehicles and is intended to carry passengers or cargo. In turn, a heterogeneous group can be represented as a set of UVs with varied purposes, compositions, and capacity characteristics. To facilitate further analysis of vulnerabilities, attack
scenarios and failure points in the context of group control assume that UV groups consist of ground vehicles only.

It should be noted that a key aspect of the functioning of homogeneous and heterogeneous groups of UVs is a common objective for every unmanned vehicle in the group. But, beyond that, UVs activities within the group should be coordinated and time-synchronized. In addition, while UVs in a heterogeneous group may differ in design, functionality, and purpose, their generic architecture will be the same [2].

2. Unmanned Vehicle Generic Architecture

It is important to consider the common architecture of the UV in order to carry out a comprehensive analysis of their vulnerabilities and points of failure. Currently, operating UVs can be presented functionally as a set of four basic hardware-software systems.

2.1. Orientation and Navigation System

This system includes the navigation unit (inertial measurement unit (IMU) or inertial navigation system, INS) with Global Navigation Satellite System-based readings correction (GNSS; e.g. GPS/GLONASS), and the unit of orientation and tracking (including 2D, 2D+ and 3D lidars, radars, ultrasonic sensors, machine vision system – video cameras, stereo cameras, depth cameras, etc.) [3]. The navigation unit is responsible for determining the position of the UV in both global and local navigation systems, while the orientation unit is responsible for monitoring the current situation, including detecting and calculating the distance to the obstacles and other traffic participants, recognition of road signs and lanes, etc.

2.2. Communication System

This system is used for the exchange of data between the UVs in the group (Vehicle to Vehicle (V2V) communication), for the transmission of information to the elements of the “smart city” and data processing centers (Vehicle to Infrastructure, V2I), as well as for the interaction with the service systems or the operator (Vehicle to X (to any internet-enabled device), V2X) in order to transmit and receive diagnostics information, update firmware of devices, etc. Possible variants of communication systems include VHF digital communication systems; Wi-Fi (IEEE 802.11 standard), 4G/5G networks, satellite links, etc.

2.3. Data Processing, Self-Monitoring and Decision-Making System of the UV

This system is responsible for the collection of data from all systems of the UV, current situation awareness, as well as short-term prediction and decision making, including the transmission of control signals to the movement control system to adjust own position and speed, avoid obstacles and collisions.

Data flows comprise not only navigation readings, but also the UV’s current state information (including charge level, telemetry of diagnostic systems, engine status data from Engine Control Units (ECU), tire pressure from Tire-pressure Monitor Systems (TPMS), etc.) to be fused, processed and monitored by the Data Processing, Self-Monitoring and Decision-Making System [4].

2.4. Movement Control System

This system is responsible for the physical acceleration, maneuvering, constant speed movement, braking, etc.

2.5. Vulnerabilities and Failures as an Integral Part of Sophisticated Cyberphysical Systems

UV is a complicated cyberphysical system with a large number of heterogenous subsystems and interfaces. Despite the increased focus of the developers on safe operation of the UVs, these vehicles are potentially susceptible to both unauthorized attacks and unintentional failures. Taking into account the context of the group mission, as well as their purpose (transportation of passengers and cargo), the
inadequate operation within a group in complex conditions may result in the damage and/or destruction of one or more UVs, injury or death of the passengers, damaging/destroying the goods transported, as well as endangering other traffic participants and infrastructure. In this regard, there is a need to identify and analyze existing and potential UV vulnerabilities and points of failure, as well as propose ways to increase their resilience to unauthorized influence and unintentional failures.

3. UV Vulnerabilities and Relevant Attacks
Most commonly, UV vulnerabilities refer to deficiencies in its physical or hardware-software systems, that can be exploited by the attacker to achieve his aims (cause malfunctioning of the UV or hijack it). The negative effect will be greater if the entire group is hijacked or if all its elements are destroyed. Consider the main types of the UVs’ vulnerabilities and possible attacks.

3.1. Orientation and Navigation System Vulnerabilities and Cyberattacks

3.1.1. Spoofing and Jamming of GNSS Signals. It is known that the attacker can jam and spoof GNSS signals by transmitting false coordinates (e.g. GPS spoofing). The inability to adjust the INS readings on correct GNSS data would result in accumulation of errors in positioning and consequent traffic accidents [5].

3.1.2. Alteration of IMU (INS) Readings. The attacker may theoretically alter INS readings. It will be possible in case of physical access to the IMU or unauthorized access to data exchange interfaces within the navigation and orientation system [6].

3.1.3. Spoofing and Jamming of LiDAR Signals. The attacker may receive a laser pulse from the LiDAR and transmit it in other angles. This will force the decision-making system to identify a false obstacle that does not exist in reality. It is also possible that the LiDAR will be disabled (signal jamming) by directing a laser pulse to it at the same frequency [4, 5].

3.1.4. mmWave Radar Spoofing and Jamming. As with the LIDAR, the attacker sends signals with the same waveform and modulation type to the receiver of the Millimeter Wave (mmWave) radar. This will lead to creation of virtual (false) traffic objects and may even cause its malfunction [5].

3.1.5. Ultrasonic Sensors Spoofing and Jamming. The attacker records and analyses the reflected ultrasonic signal, then sends it to the receiver of ultrasonic sensors (the frequency of the signal may be changed), which leads to the malfunction of the parking and vehicles tracking systems, and creates false obstacles where they do not exist. This type of attack may result in possible accidents involving the UVs in motion [5].

3.1.6. Interference in the Functioning of Machine Vision Systems. Physical intervention is an attack in which the Complementary Metal-Oxide-Semiconductor sensors of machine vision systems are disabled by laser radiation [4]. The attacker can perform such an attack periodically, which results in constant «blinding» of the cameras [5].

In addition, the intruder may also interfere in the operation machine vision software, e.g. using the adversarial image attack. It implies the modification of the original image in such a way that the changes are almost invisible to the human eye, but are highly perceptible for the neural network working with such an image. The degree of such modification is usually measured as a maximum absolute change in a pixel. As a result, when such images are used as training data, the efficiency of pattern recognition may significantly reduce [7].

But even if the data training is correct, machine vision and pattern recognition systems are vulnerable to the perception of false images that the attacker can create. In particular, Tesla Model X (HW 2.5 and HW 3) and Mobileye 630 advanced driver-assistance systems (ADAS) cannot
distinguish an actual object (man, road sign, etc.) from their adversarial images placed on the road using the projector. In case of presence of a «phantom» person on the road the UV slows down and attempts to prevent the collision, even if all other sensors (LiDAR, radar, ultrasonic sensors) reasonably do not detect any obstacle ahead. This type of attack was called the «split-second phantom attack» [8].

3.2. Communication System Vulnerabilities and Cyberattacks

3.2.1. V2I/V2X Domain Name System Spoofing. Within the V2I or V2X communication channels the attacker can perform the Domain Name System spoofing, intercept firmware updates or even upload its modified version with unauthorized features (control override, illegal access to security cameras inside the vehicle, creation of botnets from the groups of the UVs, disabling several UVs or the whole group, etc.) [4, 5].

3.2.2. Disabling V2V Wireless Communications Within a Group of UVs or Gaining Unauthorized Access to V2V Wireless Data Traffic. In the context of weak protection of V2V communication links within the group, the attacker may intercept the service data traffic being transmitted. In particular, he can attack the group leader’s wireless access point (AP), based on the Wi-Fi 802.11 standard (Wi-Fi).

In the simplest case, the attacker can launch the deauthentication attack to disable all clients connected to the leader’s AP [9], or transmit a large number of client authentication frames (authentication flooding attack) which results in the AP’s denial of service (DoS) [10]. A more complicated variant is the capture of WPA2-PSK TKIP/AES «handshakes» between the AP and the connecting client in order to obtain the password using the dictionary brute force attack [11]. Finally, if no firmware patches detected, the attacker can use the KRACK attack and force the network clients to drop their encryption keys to zero values while reconnecting to the AP [12].

It is also possible to launch the «Evil Twin» attack to jam the target wireless network and simultaneously create a false one with the same Service Set Identifier, Media Access Control address and encryption type in an attempt to obtain a valid password [13].

Using other protocols and interfaces of data transmission instead of Wi-Fi (e.g., 5G networks or the dedicated Short Range Communication (DSRC) protocol) is not a viable solution, since any known data transfer technologies have their own vulnerabilities (examples for 5G networks are given in [14, 15]), and the increase of the signal/noise ratio and the power of the attacker’s transmitter in the required frequency range is enough to suppress the V2V communication links within the UVs group (e.g., DSRC is operating at 5.9 GHz with a 75 MHz bandwidth [6]).

3.2.3. V2X Attack on User Interface Devices. Vehicle Immobilizer Keyless Entry Systems are known to be vulnerable to spoofing, encryption key restoration, and packet injection attacks [5].

3.3. Movement Control System Violation via Attacking the Internal Interfaces

The attacker will be targeting the UV’s internal interfaces (buses; such as CAN, LIN, or Flexray) in order to disrupt the movement control system. He may manipulate (spoof) the data packets, inject malicious frames or cause DoS (CarShark’s CAN attack, OBD port attack, etc.) [4, 5].

Firmware updates interception and spoofing attacks (e.g., ECU firmware spoofing [6]), as well as attacks on specific subsystems (e.g., TPMS attack will lead to misleading the on-board computer/operator by sending false tire pressure data, which may force the UV (or the whole group) to stop or result in a traffic accident [4]) are more difficult to implement.

3.4. Other Types of Attacks

3.4.1. Physical Adversarial Attack Inside the UV. There is a possibility of the intentional and unauthorized influence of the adversarial passenger on the operation of the vehicle’s physical systems,
when the diagnostic system is inoperative or disabled: turning on/off the engine, gaining access to the steering, and braking systems, etc. In this case, the UV will not be able to function properly, but the decision-making system will not detect the unauthorized interference.

3.4.2. Side-Channel Attacks. Weak shielding of the wiring and the chips will allow the attacker to intercept useful data via the side channels (e.g. the TEMPEST attack allows you to restore the signal from the video output devices) [16].

4. UVs Points of Failure

Unlike attacks, which are the unauthorized influence on the UV or their groups through the exploitation of related vulnerabilities by the adversary, failure points are potential and unintended malfunctions of the UV subsystems, which may arise as a result of deficiencies at the stages of design and production, errors in the software or improper operation under unforeseen conditions.

The most common points of failure are:

- Code errors in the firmware may lead to incorrect variables, dependencies, reboot of the onboard computer, and other serious consequences. As an example, code vulnerabilities in the ECU firmware, identified in [4].

- Zero-day points of failure – unforeseen deficiencies originating from the design and production stages that are originally presented in a large number of UVs. Detection of such faults is always unexpected to the vendor and usually requires total recall of vulnerable vehicles. For example, studies revealed that Tesla Model S and Model X (released between 2012 and 2018) infotainment systems may suddenly fail due to worn-out eMMC NAND flash storage after a certain number of program/erase cycles. The vendor’s solution is to replace the MCUv1 Media Control Unit board [17].

- GNSS malfunctions. GNSS data are known to be used to correct INS readings. The absence of the satellite navigation system signal (as in the case of targeted jamming/spoofing) results in accumulation of UV positioning errors.

- Deficiencies in road environment information fusion systems. The UV’s local navigation sensors (monitoring current road situation) relay data to the on-board computer. However, in certain weather conditions, sensors may not function correctly (i.e., LIDARs are inefficient in snow and rain conditions, and direct sunlight can temporarily «blind» the machine vision cameras). Thus, external environment parameters should be taken into account while processing data. In this way, it is possible to identify a sensor of local navigation with the highest signal/noise ratio, and its readings should be defined as prioritized in the given (current) environment. The selection of the priority sensor must change dynamically according to the current external conditions. However, if sensor data in the decision-making system is fused and processed without priority sensor selection, this can lead to errors in the local navigation system and current situation assessment [3]. In addition, the long-term presence of equal signal/noise ratio values of several sensors or reaching and maintaining the threshold value (the condition of transferring the priority from one sensor to another) may lead to a looped switch of priority between different sensors and affect adversely the overall navigation of the UV [18].

- ADAS errors in real-time autonomous driving in the further training mode. It is obvious that machine learning cannot be fully and qualitatively implemented only through simulator training and driving in closed ranges. Therefore, some vendors (such as Tesla) issue updates for autopilot systems claiming almost 5th level of vehicle autonomy. When switching to autonomous driving mode, the ADAS with integrated artificial intelligence continues to train using data obtained from real driving. However, in this case ADAS may make incorrect decisions that could lead to accidents. It is appropriate to take as an example the described incorrect operation of local navigation sensors (machine vision cameras may be blinded by direct sunlight, and lidars may work improperly in rain and snow conditions), as well as errors
in the recognition of road signs, static and dynamic objects, obstacles, and other traffic participants (including the pedestrians) [7].

- Failure of the leader (in the case of centralized group control scheme). If the control system does not provide the transfer of the UV leader functions to another vehicle, this may lead to the disruption of the group and traffic accidents.

5. Addressing the Challenges and Enhancing the Security and Resilience of the UVs and their Groups

5.1. Adaptive Security Methods

The characteristic features of the UVs’ functioning have placed significant constraints on the most of known security methods in the sphere of group control, as they require increased costs, and in some cases such methods are not feasible because of technological and operational limitations. However, some of the main targets of the attackers are UVs operating in industrial and social facilities, and the level of skills of the attackers more often allows them to camouflage their presence in the guise of legitimate operations. In this regard, today many scientific researches in the sphere of theory on information security imply the development of new methods in risk-oriented security systems, Adaptive mechanisms for combining means of data protection when operating the UVs. However, the problem of adaptive adjustment of authentication criteria is not yet fully solved. Recent researches on cybersecurity also include studies on the development of proactive methods for searching and detecting threats that cannot be discovered by traditional means of data protection.

In particular, a new method for the adaptive protection of information systems with regular self-optimization of the system was proposed in paper [19]; its distinctive characteristics were the new mathematical statement of the problem of finding the optimal protection program, and the algorithm to solve it and enhance the protection against comprehensive destructive influences. This method is based on the author’s algorithm to evaluate the effectiveness of the systems protection using the performance and security indicators and models of the system functioning in the threat space, and an algorithm for evaluating the effectiveness of protection.

Developers throughout the world attempt to implement solutions based on multi-factor authentication algorithms in order to reduce the risk of compromising user accounts [20]. This concept implies that any authentication factor has a level of trust, and the choice of authentication factor depends on the risk level of the particular operation. User and entity behavioral analysis as a cybersecurity process to detect internal threats, attacks or fraud has gained high popularity among vendors and information security specialists [21]. The reasons for such decisions are quite obvious. The volume of information circulating in corporate networks and global information space is growing rapidly. The level of competence of the attackers is also increasing, and attacks that are carried out day by day to steal data or to modify it in the information systems become more covert. It becomes very difficult to distinguish these kinds of attacks from normal legitimate user behavior. The combination of the above-mentioned factors leads to the emergence of a new class of solutions, the UEBA modules of information security [22].

More recently, the class of indirect problem-solving methods has been particularly developed, and training is provided in many similar tasks [23]. Paper [24] considers the method of authentication using the Hausdorff distance based on the remote model for IP circuits in the service-centric environment of the Internet-of-Things. One can find the real positions of the identification data required for authentication by comparing the characteristics; and the authors propose a method for calculating the Hausdorff distance. The described method can convert the calculation of the distance into a minimum distance between two points. Thus, it allows improving the efficiency and stability of the method.

The main problem of using this approach when managing the UV groups is its inapplicability to the identification of UV subjects that often mask their actions as service procedures. Many researchers seek to identify a rational feature space that will allow reliable identification of visitors (users) based
on their indirect characteristics (working environment parameters) or through the processing of behavioral statistics (dynamic methods of biometric authentication). Anagi G et al. propose a solution that implies the identification of the attackers on the basis of behavioral characteristics, identity profiling, and the audit of digital footprints [25]. The paper describes an analytical model that takes into account risk elements from different risk domains. Processing each domain individually leads to insufficient evidence of malicious intent. By contrast, the assumption that different risk indicators should be analyzed together, and their intersection as a single block allows a significant improvement in the accuracy and timeliness of intruder detection.

Paper [26] focuses on the use of a framework to detect anomalies in a computer network based on linkages between multidimensional objects using graphs. The user–device interaction is described by a weighted undirected two-dimensional graph \( G = (V; E; W) \), where \( V \) is the vertex set (users), \( E \) is the set of edges, and \( W \) is the weight of edges. The vertex set consists of two types of objects – users and devices, while the edges represent the user’s interaction with the device. Anomaly detection is based on the Isolation Forest algorithm: features space is randomly partitioned, so that isolated points are on average separated from normal, clustered data. The result is averaged over several iterations of the algorithm.

Chen T et al. proposed a common formal framework for internal malicious threat analysis based on probabilistic modeling, as well as testing, and synthesis methods [27]. In the first stage, the framework uses Bayesian networks to identify the intention of the malicious insider to launch an attack; in the second stage, the framework calculates the attack success rate using probabilistic tests of models. This approach records the behavior of the subjects, and simulates both their intention (or risk of becoming attackers) and the risk of success of the malicious actions. Paper [28] presents a threat detection model used by organizations that repeat tasks at regular intervals. Such organizations may include military facilities and public authorities. This model is specifically optimized for the organization and evaluates each combination in terms of accuracy, Area Under the Curve, and True Positive Rate (AUC, and TPR respectively).

Therefore, while constructing the adaptive systems of UV protection, priority should be given to such indirect threats, as they become more common due to the increasing complexity of protected systems. In order to implement such processes, it is necessary to provide for collecting data on possible threats and indicators of compromise from different sources. Internet traffic in the form of dumps, statistics, structural, text or multimedia content can serve as input data for the system. Data providers may be local or global network nodes, as well as hardware and software systems.

5.2. Other Protection Measures and Methods
Other measures and techniques to take countermeasures against cyberattacks and increase the resilience and reliability of the UVs (including in heterogeneous and homogeneous groups) are as follows:

- Continuous diagnosis and monitoring of all major UV nodes, aggregates and systems (both physical and hardware-software).
- Implementation of algorithms of data integration (fusion) from heterogeneous sensors, e.g., with using an independent module for selecting the priority sensor depending on the external conditions [3].
- Ensuring secure operation of UV machine vision systems, e.g., through the approach described in paper [7]. Further safe training of UV neural networks using close to real and rare circumstances, as well as the design of special artificial intelligence systems to detect and respond to critical situations [29, 30].
- Shielding of cable assemblies and chips, as well as the use of optical fiber for data transmission can hamper the TEMPEST attacks.
- Implementation of navigation subsystem capable of short-term operation without satellite navigation data (e.g. using other sensors to correct INS (IMU) readings).
- Updating of UV firmware with integrity check function only when in service stations.
• The use of encryption and antinoise coding algorithms can increase the security of communication channels and their resistance to interference. In addition, secure data transfer algorithms for wireless communication channels should be used, when they are jammed by the adversary [31] (e.g., blockchain-based algorithms [32] and the ones using digital watermarks [33]).

• When integrating UVs into groups, it is recommended to use decentralized group control models or implement an algorithm of leader reassignment.

6. Conclusion
The rapidly growing UV industry implies the improvement of a set of technologies – artificial intelligence, communication systems, cyberphysical interfaces, and information security.

None of the proposed, designed or operated UVs in the world fully meets the requirements of the 5th level of autonomy for the unmanned vehicles. But it is already clear that the intelligent transportation infrastructure of the smart city and the operated UV should function in a reliable and stable manner in order to gain the trust and integrate into the emerging socio-cyberphysical environment. In this context, the solution of safety problems, while using novel and improved systems, algorithms, methods and principles of machine vision and navigation of autonomous unmanned vehicles is a relevant task. The analysis of vulnerabilities and failure points in both single engagement of unmanned vehicles, and scenarios of their integration and deployment in groups is a part of this ongoing process. And these circumstances dictate the relevance of such researches.

Acknowledgement
The reported study was partially funded by RFBR, project number 19-29-06044 (sections 1-4), and by Russian Federation President Grant for the young scientists MK-2421.2020.9 (section 5).

References
[1] Klimov A A, Pokusaev O N, Kupriyanovskiy V P and Namiot D E 2018 On architecture of autonomous (driverless) cars and infrastructure for their operation Modern Information Technologies and IT-Education 14(3) p 727–736
[2] Beloglazov D A, Gajduk A R, Kosenko E Yu, Medvedev M Yu, Pshihopov V H, Solovyev V V, Titov A E, Finaev V I and Shapovalov I O 2015 Group Control of Mobile Object in Uncertain Environments ed V H Pshihopov (Moscow: FIZMATLIT) chapter 1 pp 9–65
[3] Mamchenko M, Romanova M and Trefilov P 2020 Algorithm for Sensor Data Merging Using Analytical Module for Priority Sensor Selection 2020 Int. Conf. on Industrial Engineering, Applications and Manufacturing (ICIEAM) (Sochi) (IEEE) p 1–5
[4] Parkinson S, Ward P, Wilson K and Miller J 2017 Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges IEEE Transactions on Intelligent Transportation Systems vol 18(11) (IEEE) p 2898–2915
[5] Ren K, Wang Q, Wang C, Qin Z and Lin X 2020 The Security of Autonomous Driving: Threats, Defenses, and Future Directions Proc. of the IEEE vol 108(2) (IEEE) p 357–372
[6] Kumar A D, Chebrolu K N R, Vinayakumar R and Soman K P 2018 A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities Preprint abs/1810.04144
[7] Ishakov A and Jharko E 2020 Approach to Security Provision of Machine Vision for Unmanned Vehicles of “Smart City” 2020 Int. Conf. on Industrial Engineering, Applications and Manufacturing (ICIEAM) (Sochi) (IEEE) p 1–5
[8] Nassi B, Mirsky Yi, Nassi D, Ben-Netanel R, Drokin O and Elovici Yu 2020 Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks Proc. of the 2020 ACM SIGSAC Conf. on Computer and Communications Security (CCS ’20) (New York: Association for Computing Machinery) p 293–308
[9] Agarwal M, Biswas S and Nandi S 2015 Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach 2015 IEEE Int. Conf. on Systems, Man, and
[10] Elhigazi A, Razak S A, Hamdan M, Mohammed B, Abaker I and Elsafi A 2020 Authentication Flooding DOS Attack Detection and Prevention in 802.11 2020 IEEE Student Conf. on Research and Development (SCOREd) (Batu Pahat) (IEEE) p 325–329

[11] Juhász K, Póser V, Kozlovszky M and Bánáti A 2019 WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol 2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMII) (Herlany) (IEEE) p 333–338

[12] Fehér D J and Sandor B 2018 Effects of the WPA2 KRACK Attack in Real Environment 2018 IEEE 16th Int. Symposium on Intelligent Systems and Informatics (SISY) (Subotica) (IEEE) p 000239–000242

[13] Asaduzzaman M, Majib M S and Rahman M M 2020 Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack 2020 IEEE Region 10 Symposium (TENSYMP) (Dhaka) (IEEE) p 1704–1707

[14] Dutta A and Hammad E 2020 5G Security Challenges and Opportunities: A System Approach 2020 IEEE 3rd 5G World Forum (5GWF) (Bangalore) (IEEE) p 109–114

[15] Arjoune Y and Faruque S 2020 Smart Jamming Attacks in 5G New Radio: A Review 2020 10th Annual Computing and Communication Workshop and Conf. (CCWC) (Las Vegas) (IEEE) p 1010–1015

[16] Zhang C, Zhang H, Luo J and Du Y 2017 TEMPEST in USB 2017 IEEE 5th Int. Symposium on Electromagnetic Compatibility (EMC-Beijing) (Beijing) (IEEE) p 1–4

[17] Ruffo G H 2019 UPDATE: Tesla Cars Have A Memory Problem That May Cost You A Lot To Repair Available from https://insideevs.com/news/376037/tesla-mcu-emmc-memory-issue/

[18] Mamchenko M, Romanova M and Trefilov P 2020 An Algorithm for Evaluating the Measured Values of Dynamic Objects under the Influence of External Factors 2020 International Russian Automation Conference (RusAutoCon) (Sochi) (IEEE) p 1069–1073

[19] Levonevskiy D, Fedorchenko L, Afanasieva I and Novikov F 2018 Architecture of the software system for adaptive protection of network infrastructure Proc. of the 11th International Conference on Security of Information and Networks (SIN ’18) (New York: Association for Computing Machinery) p 1–4

[20] Dasgupta D, Roy A and Nag A 2017 Continuous authentication Advances in User Authentication. Infosys Science Foundation Series (Cham: Springer) p 235–279

[21] Iskhakov A Yu, Iskhakova A O, Meshcheryakov R V, Benderau R and Melekhova O 2018 Application of User Behavior Thermal Maps for Identification of Information Security Incident SPIIRAS Proc vol 6(61) (Saint Petersburg: St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences) p 147–171.

[22] Kotenko I V, Ushakov I A, Pelevin D V, Preobrazhenskij A I and Ovramenko A Yu 2019 Identification of insiders in the corporate network: UBA and UEBA based approach Information Security. Inside 5(89) p 26-35

[23] Kavousi F and Akbari B 2014 A Bayesian network-based approach for learning attack strategies from intrusion alerts Security and Communication Networks 7(5) p 833–853

[24] Liang W, Huang W, Chen W, Li K-C and Li K 2019 Hausdorff Distance Model-Based Identity Authentication for IP Circuits in Service-Centric Internet-of-Things Environment Sensors 19(3) 487 p 1–18

[25] Fagade T and Tryfonas T 2017 Malicious Insider Threat Detection: A Conceptual Model Security and Protection of Information p 31–44

[26] Anagi G, Li S and Serdar B 2017 A Graph Based Framework for Malicious Insider Threat Detection Proc. of the 50th Hawaii Int. Conf. on System Sciences (HICSS) (Waikoloa Village) p 2638–2647

[27] Chen T, Kammuller F, Nemli I and Probst C W 2015 A probabilistic analysis framework for malicious insider threats Int. Conf. on Human Aspects of Information Security, Privacy, and Trust (Berlin: Springer) p 178–189
[28] Oh J, Kim T H and Lee K H 2019. Advanced insider threat detection model to apply periodic work atmosphere KSII Transactions on Internet and Information Systems 13(3) p 1722–1737
[29] Pashchenko F F, Amosov O S, Amosova S G, Ivanov Y S and Zhiganov S V 2019 Deep Neural Network Method of Recognizing the Critical Situations for Transport Systems by Video Images Procedia Computer Science 151 p 675–682
[30] Amosov O S, Amosova S G, Ivanov Y S and Zhiganov S V 2019 The Use of Deep Neural Networks to Recognize Network Traffic Abnormalities in Enterprise Information and Telecommunication Systems 2019 Twelfth Int. Conf. "Management of large-scale system development" (MLSD) (Moscow) (IEEE) p 1–5
[31] Iskhakova A, Iskhakov A, Meshcheryakov R and Jharko E 2019 Method of Verification of Robotic Group Agents in the Conditions of Communication Facility Suppression IFAC-PapersOnLine vol 52(13) (Amsterdam: Elsevier) p 1397–1402
[32] Evsutin O and Meshcheryakov Y 2020 The Use of the Blockchain Technology and Digital Watermarking to Provide Data Authenticity on a Mining Enterprise Sensors 20(12) p 1–19
[33] Shumskaya O and Iskhakova A 2019 Application of digital watermarks in the problem of operating signal hidden transfer in multi-agent robotic system 2019 Int. Siberian Conf. on Control and Communications (SIBCON) (Tomsk) (IEEE) p 1–5