An Overlay Network Based on Cellular Technologies for the Secure Control of Intelligent Mobile Objects

Vitalii Tkachov[1], Andriy Kovalenko[1], Vyacheslav Kharchenko[2], Mykhailo Hunko[1] and Kateryna Hvozdetska[1]

[1] *Kharkiv National University of Radio Electronics, 14, Nauky Ave., Kharkiv, 61165, Ukraine*
[2] *National Aerospace University "KhAI", 17, Chkalova str., Kharkiv, 61070, Ukraine*

Abstract

The current state of the problem regarding secure control of smart mobile objects using existing tele-communication infrastructures is described in the paper. The scientific and technical task of developing the principles of using cellular communication systems for the organization of secure remote control of intelligent mobile objects has been solved. The solution lies in the use of overlay computer networks based on VPN tunneling. Proposals have been developed for constructing an overlay computer network based on VPN taking into account traffic aggregation as well as dividing network elements according to their purposes. The related problems of connection dependability at the access, distribution and core levels are considered. The possibility of using nested VPN tunneling in high-speed cellular communication systems to improve the security of transmitted data is analyzed. The result of a number of model and experimental studies is the proof of the proposed principles efficiency. Recommendations have been developed for using the proposed principles of constricting an overlay network based on cellular communication systems for the secure control of intelligent mobile objects in solutions related to the implementation of dependability and resilience of computer networks concept.

Keywords

Virtual private networks, Network security, Overlay networks, Intelligent Mobile Object.

1. Motivation

Modern data transmission between intelligent mobile objects (IMOs) and appropriate control node(s) always include some type of communication system. Intelligent mobile objects are characterized by the presence of a behavior trajectory with an aperture of possible deviations during performance a task. These deviations are required to maximize the survivability indicators of such a class of systems based on mobile objects, and their implementation is possible using methods of intelligent data analysis. Evolution of such communication systems and underlying methods for their creation is considered in [1, 2]. There is a method, which relies on a specific relay node inside the IMO grouping. It is responsible for data transmission between a stationary node and appropriate data transmission subsystem. Such "multi-layered" solutions have found application, for example, in support systems for natural disaster response operations. Specific data transmission approach for IMO and the control center implies that there is an inevitable trade-off between "green" aspects (or energy consumption) and performance. Depending on exact scenario, service zone of an autonomous IMO and a relay node may not coincide and it, in turn, makes impossible the continuous data exchange with the control center [3]. In another scenario, where all the network nodes are stationary, implementation of such network may be economically impractical [4, 5]. A separate issue is certification and licensing of

ICTERI-2021, Vol II: Workshops, September 28 – October 2, 2021, Kherson, Ukraine
EMAIL: tkachov@ieee.org (A. 1); andriy.kovalenko@nure.ua (A. 2); v.kharchenko@csn.khai.edu (A. 3); hunko@ieee.org (A. 4) ; kateryna.hvozdetska@nure.ua (A. 5)
ORCID: 0000-0002-6524-9937 (A. 1); 0000-0002-2817-9036 (A. 2); 0000-0001-5352-077X (A. 3); 0000-0002-8011-0693 (A. 4); 0000-0002-5233-5801 (A. 5)

© 2020 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

the frequency range that can be used by various commercial solution providers, which significantly increases the cost of this class solutions. The problem of using existing infrastructure solutions for data transmission in synergy with new systems based on the IMO group is considered in the paper. In addition, we assume application of existing cellular networks for data transmission between the IMO and the control center (or a higher-level IMO).Mostly, nowadays cellular networks are used for the Internet access supporting seamless principles: it is very important during mobile node movement through certain area. However, cellular networks are public networks with all inherent security problems: any data can be intercepted [5]. One of the ways to ensure security in mobile networks is to use virtual overlay networks, that is, networks that are built on top of the existing network infrastructures of telecommunication service providers. The basic method for implementing an overlay network is to use the virtual private networks technology. In this regard, there is urgent task of developing the principles of constructing an overlay computer network based on technology of VPN tunnels to ensure secure data exchange between the IMO and the control center through cellular communication systems. It is important to take into account such additional requirements as: a high level of reliability of data transmission channels; the ability of the IMO group to quickly respond to changes (reconfiguration) in the data transmission medium including autonomous operation during switching to other cellular network operators. It is assumed that these principles will be used when developing a complete system or a technology for constructing full-fledged technical solutions in a given class of problems.

2. Work related analysis and objectives

Novelty of the mentioned task is conditioned by the fact that high-speed cellular communication systems as a data transmission medium between sources of high-intensity traffic have been actively developing only in recent years.

In a number of publications [6-16], the authors proposed models, methods and technologies for constructing overlay networks based on a mobile platform, solutions for traffic management, etc. In particular, it is important to note the following, the most important of the publications.

In particular, in publication [12], the authors consider an LTE network as a data transmission medium between drones and a control point. As a method of protection, it is assumed to use various methods for data encryption, particularly, tunneling. Therefore, for example, the use of UDP and TCP protocols in the experimental studies in high-speed IMOs give very conflicting results: in theory, TCP has many advantages over UDP protocols, but TCP is a protocol that does not have a broadcast function. Alternatively, UDP can act as a broadcast protocol and is "easier" than TCP. However, the experiments have shown that UDP used more packets than TCP; and this is because the TCP connection in the MAVlink protocol, which is described in the work, used some UDP protocols to transmit telemetry data. On the other hand, under UDP connection, the MAVlink protocol used only UDP without TCP. Hence, UDP requests had more traffic than TCP. The disadvantage of the solutions proposed in the article is the presence of the repeated requests mechanism when data transfer processes are violated, tying them to one data transmission technology, which makes it impossible to use low-speed data transmission standards when switching communication standards.

Also known are works [13-16], in which the authors assume using of different media for data transmission. The paper describes the importance of considering the functioning parameters of all elements of the data transmission network, leading to a decrease in errors in the network, which significantly complicates the mathematical model. With a large model dimension, the error component, introduced by the inaccuracy of the analytical and numerical methods used, becomes very significant. In addition, the time required to solve a large-scale problem also becomes unacceptable when solving it in real time. Basically, the specifics of solving problems in real time lead to the fact that the lack of computational capabilities is to a certain extent equivalent to the lack of information about the conditions of the problem. This is due to the high dynamics of changes in the IMO's position in space. The situation is aggravated by the fact that the cellular networks described in the work almost never apply the introduction of specialized software for transferring control information between IMOs in the

control system, which allows to significantly reduce the errors of data and calculations for various layers of interaction as it is done in other technical IMO control systems.

Given the lack of described practical results on the application of the analyzed solutions, there raise doubts about the effectiveness of these approaches, since in conditions of high IMO mobility, the data transfer protocols used in stationary computer networks behave very differently, which requires deep experimental research.

Objective of the research is to investigate level of security of data transmission between IMOs by developing scenarios for building an overlay computer network based on VPN tunneling technology over existing public network infrastructures.

The paper is structured as a follows: Section 3 describes the main principles used in this research and Section 4 presents appropriate numerical studies.

3. Description of principles

Here, new principles are proposed which, in order to simplify the representation, are reduced to existing network architectures. The basement of each overlay computer network is appropriate hierarchical model. It, in turn, represents a virtual network as a multi-layer structure [11]. Such a principle of division a network into smaller pieces (subnets, etc.) contributes to the grouping of network component's functions and to fast localization of problems related to the IMO movement and reconstructing VPN tunnels. In addition, when creating a fault-tolerant segment of an overlay network, in which data that requires confidentiality circulates, it is required to protect data during its transmission to external networks, as well as to differentiate access when transferring it between overlay network segments within the IMO group.

Taking into account all above facts, now we can point out the elements of the overlay network and determine their appropriate functions: access layer (network segmentation, connection of various equipment to the network, switching, etc.); distribution layer (routing, traffic management, packet filtering, etc.); core layer (routing in tunnels, connecting in VPN, routing between tunnels, etc.)

Typically, access layer is represented by virtual switches. In turn, distribution layer is represented by virtual routers (mainly, performing firewall functions) and core layer is represented by virtual routers (mainly, performing the functions of creating VPN cryptographic protection).

When a number of IMOs in overlay network is pretty high, some of the nodes are transit nodes in a case of not fully connected topology. Thus, we need consider for such IMOs both availability of tunnels between nodes and their bandwidth. There could be situations in overlay network when it is required to use simultaneously several tunnels between the IMO and the control center and combine them (aggregation).

The aggregation condition will be as follows:

$$v_{inVPN} > v_{core-agg} \tag{1}$$

where v_{inVPN} is the bandwidth of the uplink tunnels from one IMO core towards the external network; $v_{core-agg}$ is the maximum bandwidth of one virtual tunnel between the core and aggregation layers. With a large number of internal control commands when operating in low-speed cellular communication systems ($v_{IMO \to IMO}$), it is advisable to aggregate virtual channels also between the IMO and virtual switches of the distribution layer. The aggregation condition will be:

$$v_{IMO \to IMO} + v_{core \to IMO} > v_{IMO \to agg} \tag{2}$$

where $v_{core \to IMO}$ is the data coming from the control server to other IMOs in the overlay network. $v_{IMO \to agg}$ is the maximum bandwidth of one tunnel between the IMO sublayer and the aggregation scheme. Thus, in a worst case, the bandwidth of one tunnel, and not all, between the two layers within

the segment of the IMO group in (1) and (2) is used. It is advisable to use other virtual channels connecting these segments not only for balancing, but also for reserving.

The considered principle requires a rather complex IMO configuration at all layers, more use of IP addresses. Simpler options are possible, in which IMOs at the distribution and aggregation layers are combined into a fault-tolerant virtual cluster. Thus, one virtual tunnel is functioning, while the other is in reserve at this time.

At the same time, this option requires implementing a larger number of ports on the IMO at all layers of the overlay network [17]. In case of a shortage of ports, such a scheme can have a fully-mesh cluster topology. However, this will reduce the object connectivity indicator to two.

4. Numerical studies

To numerically study the characteristics of the proposed principle for constructing an overlay network based on cellular communication systems for the secure control of Intelligent Mobile Objects using incomplete data, a simulation model was used, which was built using the aggregation approach mentioned earlier. The NS3 environment was used as a simulation environment [3].

At the first stage of simulation, various topologies of cellular networks were tested with different dynamics of the structure. They were created both programmatically (the number of nodes, the probability of denial, the degree of connectivity) and manually, using the capabilities of the visual topology designer of the modeling system. The sizes of cellular networks varied from 10 to 50 base stations within a conventional city.

As a result of this testing, a typical topology was chosen (Figure 1). The entire network, on which the overlay network is being constructed, consists of two sites saturated with nodes (right, left), which are connected by two routes passing through the virtual routers. These routers with their own communication channels create a bottleneck in the cellular network.

Let us consider an overlay network saturated with traffic (excluding service traffic) in such a way that adding a requirement will cause a denial of service. Then the dependence of the number of denials on the amount of service traffic should be linear. At the same time, it is assumed that there are no topological changes and changes in the state of the channels in the overlay network.

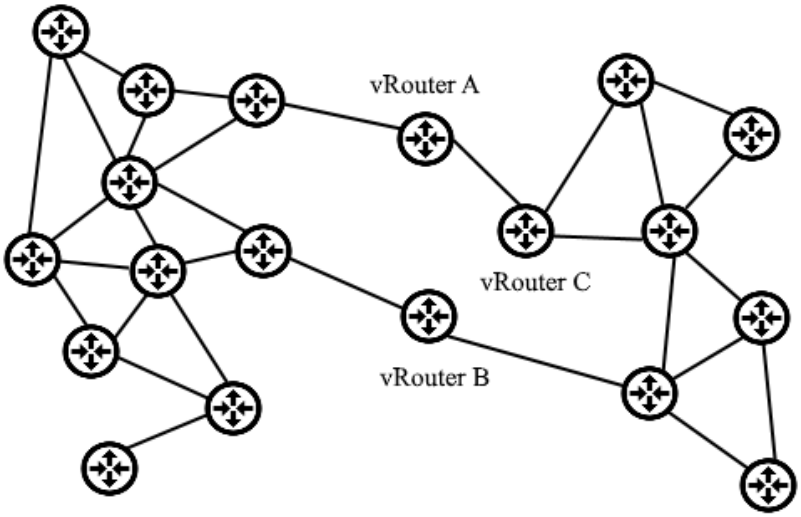

Figure 1: The considered topology of the overlay network

In the course of modeling, a general view of the dependence of the service traffic volume and the number of denials at the time of the change in the overlay network topology was obtained. The view of this dependence is shown in Figure 2.

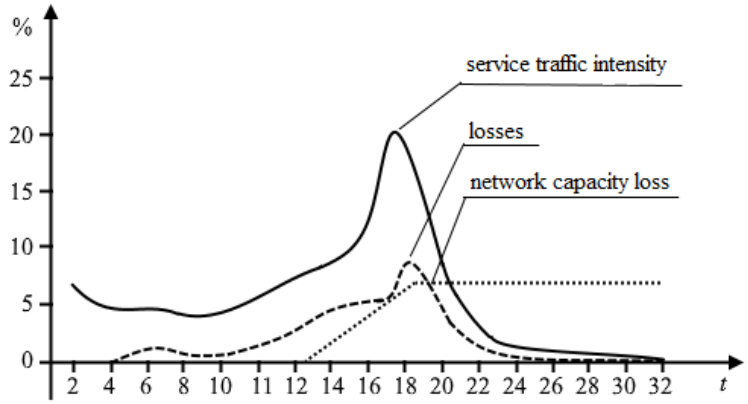

Figure 2: Service traffic at the moment of the overlay network nodes denial

The dash-dotted line denotes the percentage of capacity loss of the overlay network at the moment of the cellular network nodes denial. It is not so much necessary to determine the impact of the loss of network bandwidth, but to associate the event with the corresponding values of service traffic.

To check the operability of the overlay network, which is built according to the principle proposed in the work, and to estimate the costs of service traffic in a state of constant external conditions, the above topology was used (Figure 1). An overlay network is viewed as a network with constant characteristics. The bandwidth of virtual communication channels and the matrix of requirements were selected in such a way as to saturate network traffic. The function of increasing the transmission cost depending on the load was chosen constant, since the transmission cost, in this case, does not play a significant role. When simulating in such conditions, in the absence of changes in the cellular network, the expected dependence was obtained, which is shown in Figure 3.

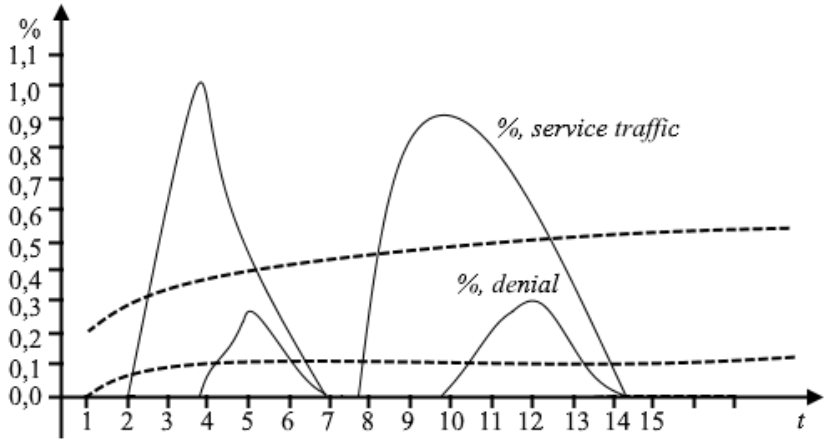

Figure 3: Denials in the saturated network

Solid graphs show the maximum possible peak values of the overlay network bandwidth share for service traffic and the resulting denial rate. Dashed lines represent the average values of the respective quantities. The following mechanism was used to generate the peak values of the service traffic volumes: when the simulation process was started, the update timers and a number of other parameters of the routing algorithm in the overlay network were selected in such a way as to ensure the simultaneous activation of the update procedure.

The given Figure shows a noticeable delay in the onset of denials from the moment the update procedure has been started. In addition, their amplitude is smaller. This is conditioned by the size of the message queue during the simulation. With its use, some messages are buffered, ensuring that some of the requirements are saved. This ensures the autonomy of IMO functioning in case of denial of an overlay or a cellular network.

Upon further investigation of the principles of constructing an overlay network based on cellular communication systems proposed in the work for the secure control of Intelligent Mobile Objects, an analysis can be carried out using incomplete data that allows to correctly select the queue size for the virtual router of the overlay network in order to minimize the number of denials.

The second step in research is to introduce sources of denial into the overlay network described above. They must meet the following requirements: on the one hand, they must be in the "network bottlenecks" so that their denials most strongly affect the redistribution of the load in the overlay network; and on the other hand, so as to exclude the probability of the cellular network integrity violation as a result of equipment denial due to oversaturation of communication matrices with service packets. We will select the nodes operating in the bridge node mode as untrusted nodes. When simulating over a long period, the dependence shown in Figure 4 was obtained.

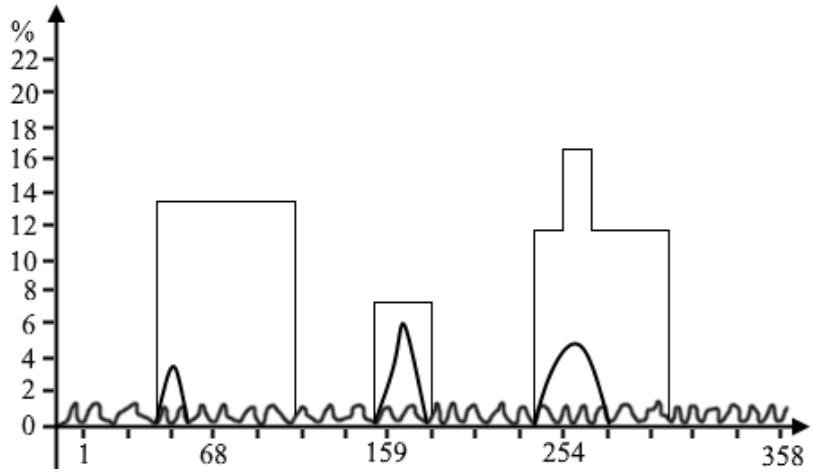

Figure 4: Service traffic and the number of denials

In Figure 5, we can see that the peak load immediately follows the change in the overlay network bandwidth, which corresponds to the change in the state of the denied virtual router located at the cellular network node.

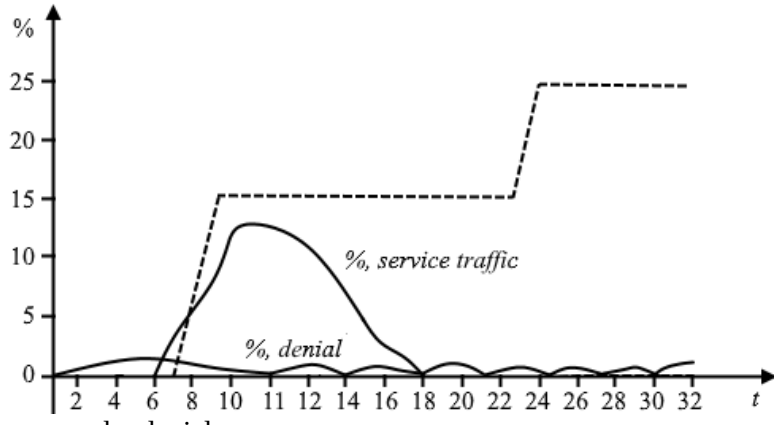

Figure 5: Recovery under denial

It is advisable to consider the moment of changing the overlay network bandwidth and the service traffic caused by this event in more detail. Figure 5 shows a fragment corresponding to two successive virtual node denials. The left front of the line of changing the network bandwidth corresponds to the denial of the first virtual router, which creates a critical state and causes not only a significant increase in the share of service traffic, but also a rather long time to restore the connectivity of routing data.

The second moment of changing the capacity of the overlay network, corresponding to the denial of the second bridge router, practically does not cause loss of requirements. This at first glance strange situation is explained by the fact that the first router, being important for its neighbors from the point of view of the overlay network connectivity, was used by them before the denial to form a route between the right and left groupings, and, therefore, a significant traffic from IMOs was passing through it. After its denial, the queues are quickly overflown and until connectivity errors in the routing data are eliminated, all requests are denied in order to avoid overloading the physical node on which the virtual router operates. In the second case, if the next virtual bridge router denies, the value of which, as a transmitting element, is small, the connectivity is broken for a small number of nodes, and is restored almost immediately.

Further, in the course of a numerical experiment, it is advisable to consider the dynamics of the share of service traffic for IMO controlling and the number of denied requests when the size of the effective routing areas in the overlay network increases. For this, the previous example is taken without changes, except that each virtual router entering the overlay network will have an effective routing area of size 6. The graphs of the corresponding dependencies are shown in Figs 6 and 7.

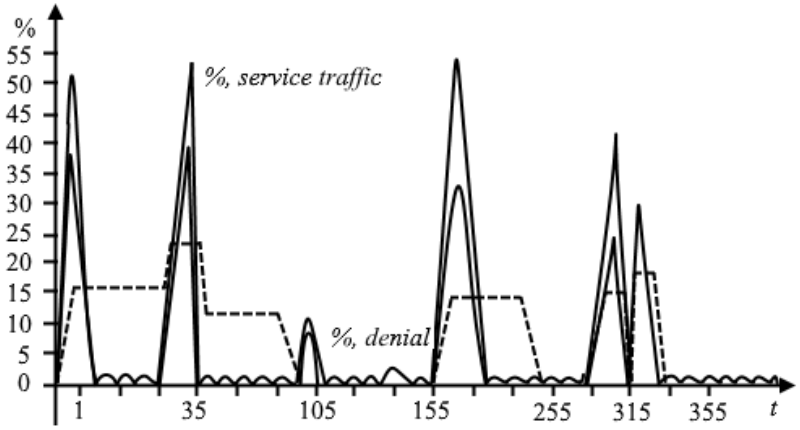

Figure 6: Service traffic and the number of denials

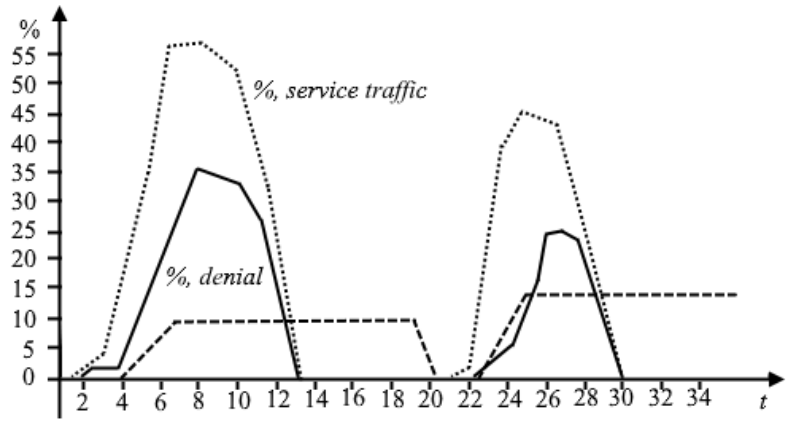

Figure 7: Recovery under denial

Analysis of the last figure reveals another aspect, which is as follows. A decrease in the capacity of the overlay network due to a denied virtual router can have a significantly less impact on the functioning of the overlay network than the wave of service traffic caused by it, aimed at restoring the optimal operating mode.

Analyzing the obtained numerical results of using the developed principles of constructing an overlay network based on cellular communication systems for the secure control of Intelligent Mobile Objects, two conclusions can be drawn. First, in the case of implementing an overlay network using

incomplete data, we have an adjustable level of service traffic and, accordingly, a controlled number of requirement losses caused by overloads of virtual bridge routers. Therefore, in Figs 6 and 7, it can be seen that when choosing different radii of areas of effective routing, losses vary in the range from 7% to 45%. Comparing this value with the average number of routing losses in the overlay network, it can be stated that the application of the principles proposed in the work can be useful for reducing losses by limiting the level of service traffic from the IMO. Second, the efficiency of systems using the proposed principles strongly depends on the correct choice of the size of the effective routing area in the overlay network constructed on the basis of cellular networks of telecommunications operators.

5. Conclusions

The development of principles for using existing infocommunication infrastructures as a data transmission medium between IMOs on the example of cellular networks of telecommunications operators is presented. It is shown that the aggregation scheme is the most applicable on the basis of these principles.

Using the principles of constructing an overlay network based on cellular communication systems for the secure control of Intelligent Mobile Objects, it is possible to create full-fledged segments in the "smart city" concept schemes, providing data transmission of varying confidentiality degrees with a sufficient degree of reliability when losses vary in the range from 7% to 45%.

The proposed principles were investigated by setting up numerical experiments, a number of model and field experiments, which undoubtedly requires a broader description, including modeling various network attacks to intercept and replace traffic in the chain "Intelligent Mobile Object – control node". The following attacks and impacts are considered: electromagnetic suppression and interception of the carrier frequency, artificial noise barriers at the data transmission frequency, substitution of data packets, the use of false nodes of the stationary infrastructure. The paper provides guidance on how to use these principles to securely control Intelligent Mobile Objects in smart city solutions related to realization of the "smart city" concept [18-19].

However, these principles have their advantages and disadvantages and can be applied according to a specific situation on the object and the capabilities of cellular communication systems. It is worth paying a particular attention to the logical structure of the overlay computer network, since the use of all the advantages of the supporting data transmission medium depends on its correct definition.

6. References

[1] 1. Dodonov, A.G., Gorbachyk, O.S., Kuznietsova, M.G.: Management organization of mobile technical objects group. Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Se-curity (ITS 2017), pp. 1-7. CEUR Workshop Proceedings (2017).

[2] Merlak, V., Smatkov, S., Kuchuk, N., Nechausov, A.: Resourses Distribution Method of University e-learning on the Hypercovergent platform. In 9th Int. Conference on Dependable Systems, Service and Technologies (DESSERT'2018), pp. 136-140. IEEE (2018).

[3] Dodonov, A.G., Gorbachyk, O.S., Kuznietsova, M.G.: Survivability of organizational management systems and the maintenance of critical infrastructure security. Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019), pp. 1-10. CEUR Workshop Proceedings (2019).

[4] Kuchuk, H., Kovalenko, A., Ibrahim, B.F., Ruban, I.: Adaptive compression method for video information. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.2), 66-69 (2019).

[5] Tiutiunyk, V., Kalugin, V., Pysklakova, O., Levterov, A., Zakharchenko, Ju.: Development of Civil Defense Systems and Ecological Safety. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 295-299. IEEE (2019).

[6] L. Orda, O. Gehrke and H. Bindner, "Testing Overlay Networks in a Smart Grid using Simulated and Physical Networks," 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2019, pp. 1-7, doi: 10.1109/SmartGridComm.2019.8909794.
[7] R. R. Hansen and C. W. Probst, "Modelling and Analysing Overlay Networks by Ambients with Wormholes," 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU), 2018, pp. 1-4, doi: 10.23919/ICMU.2018.8653596.
[8] Z. Cui, J. Liao, J. Wang, Q. Qi and J. Wang, "Cooperative traffic management for co-existing overlays," 2015 IEEE 40th Conference on Local Computer Networks (LCN), 2015, pp. 466-469, doi: 10.1109/LCN.2015.7366354.
[9] Z. Cui, J. Liao, J. Wang, Q. Qi and J. Wang, "An Approach to Improve the Cooperation between Heterogeneous SDN Overlays," 2016 IEEE 41st Conference on Local Computer Networks (LCN), 2016, pp. 236-239, doi: 10.1109/LCN.2016.51.
[10] A. F. Ibn Ibrahimy, F. Anwar, M. I. Ibrahimy and M. R. Islam, "Two Dimensional Array Based Overlay Network for Reducing Delay of Peer-to-Peer Live Video Streaming," 2014 International Conference on Computer and Communication Engineering, 2014, pp. 185-188, doi: 10.1109/ICCCE.2014.61.
[11] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani and J. Lim, "Security, Privacy and Trust for Smart Mobile- Internet of Things (M-IoT): A Survey," in IEEE Access, vol. 8, pp. 167123-167163, 2020, doi: 10.1109/ACCESS.2020.3022661.
[12] Aljehani, M., Inoue, M.: Communication and autonomous control of multi-UAV system in disaster response tasks. In KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, pp. 123-132. Springer, Cham (2017).
[13] Liu, D., Xu, Y., Wang, J., Xu, Y., Anpalagan, A., Wu, Q., Shen, L.: Self-organizing relay selection in UAV communication networks: A matching game perspective. IEEE Wireless Communications, 26(6), 102-110 (2019).
[14] Li, B., Fei, Z., Zhang, Y., Guizani, M.: Secure UAV Communication Networks over 5G. IEEE Wireless Communications, 26(5), 114-120 (2019).
[15] Kuchuk, G., Kovalenko, A., Kharchenko, V., Shamraev, A.: Resource-Oriented Approaches to Implementation of Traffic Control Technologies in Safety-Critical I&C Systems. Green IT Engineering: Components, Networks and Systems Implementation. Studies in Systems, Decision and Control series, 313-337 (2017).
[16] Kuchuk, G., Kharchenko, V., Kovalenko, A., Ruchkov, E.: Approaches to Selection of Combinatorial Algorithm for Optimization in Network Traffic Control of Safety-Critical Systems. In Proceeding of IEEE East-West Design & Test Symposium, Yerevan, Armenia, pp. 384-389 (2016).
[17] Tkachov, V., Hunko, M., Volotka, V.: Scenarios for Implementation of Nested Virtualization Technology in Task of Improving Cloud Firewall Fault Tolerance. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), pp. 759-763. IEEE (2019).
[18] Jo, J. H., Sharma, P. K., Sicato, J. C. S., & Park, J. H. (2019). Emerging technologies for sustainable smart city network security: Issues, challenges, and countermeasures. Journal of Information Processing Systems, 15(4), 765-784.
[19] Sajassi, A., Drake, J., Bitar, N., Shekhar, R., Uttaro, J., & Henderickx, W. (2018). A network virtualization overlay solution using ethernet VPN (eVPN). IETF RFC 8365.