Unmanned Aerial Vehicles Image Processing With the Use of a Neural Network

Alekseev Viktor Mikhailovich, Khusenov Dodokhon Naimboevich, Andreev Andrey Andreevich, Chichkov Sergey Nikolaevich

Russian University of Transport (MIIT), Moscow, Russia

Contribution on the State of the Art

https://doi.org/10.7251/JIT2202089M UDC: 623.746.2-519:629.7.014.9

Abstract: Transport infrastructure facilities are critically important. To ensure their functioning, it is necessary to apply tracking methods that provide a high degree of protection. The article deals with the issues of unauthorized intrusion of foreign objects controlling, in order to prevent a dangerous impact on the infrastructure of high-speed transport. In this regard, it is proposed to conduct round-the-clock surveillance using unmanned aerial vehicles.

Due to the fact that the range of UAV's action distance is limited, therefore, it is proposed to use a remote method of detecting the intrusion of objects on the infrastructure with the use of an optical cable OK. The joint use of UAVs and OK allows to create a reliable system that provides control over the intrusion on the infrastructure. Special video cameras (thermal imagers, Lidar) are installed on unmanned aerial vehicles, providing inspection of the invasion area during day and night time. Since video recording devices have different resolution, the task is to apply methods for integrating data with different resolution and processing them by a neural network. The implementation of infrastructure tracking systems requires increasing demands on the network structure. One of the tasks set in this article is the development of the structure of the intrusion detection network on the high–speed ground transport infrastructure.

Keywords: optical cable, local area computer network, structure of an unmanned vehicle network, video cameras, intrusion on infrastructure.

Relevance. High-speed traffic (HST) requires the expansion of the functionality of security systems aimed at the application of new methods, namely, theoretically and technically sound solutions in connection with possible acts of vandalism and terrorism. The HST requires a revision of technical solutions in the development of critical systems (protection of objects and information protection) and linkage with existing management systems (DC, MPC and others). At high speeds, minor changes in the parameters of the track, for example, due to changes in the structure of the superstructure of the track caused by undercutting, can lead to an accident. The collapse of rocks, the penetration of foreign objects into the infrastructure, are also potentially dangerous for the movement of a high-speed train.

In this regard, it is necessary to develop new solutions not only to control the infrastructure of the rolling stock path, but it is also extremely important to determine the moment of occurrence of an obstacle caused by the unauthorized appearance of foreign objects that pose a danger to movement and further transfer of information to control systems in order to adopt rational management. The existing control systems for high-speed trains of DC, MPC and auto-blocking provide safe control of objects, arrows, signals and other devices, but are not designed to control and generate information about the appearance of foreign objects on the infrastructure, landslides, landslides and other external dangerous impacts. This function is assigned to independent systems that, by aggregating information, determine the causes of a dangerous situation and transmit this information to control and traffic safety systems that correct the movement of trains in the face of a threat.

One of these approaches is that it is necessary to use a combined monitoring method using an optical cable (OC) and unmanned aerial vehicles equipped with video recording devices for the emerging threat at different times of the day and in any weather conditions.

Primary information about the occurrence of an incident is provided by an optical cable acting as a sensor, which is laid in several ways: underground or on barrier shields. The principle of operation of the OK - sensor is that the conditions for the passage of radiation (due to mechanical action) change in it, as a result of which the pattern (the so-called speckle) at the output end changes.

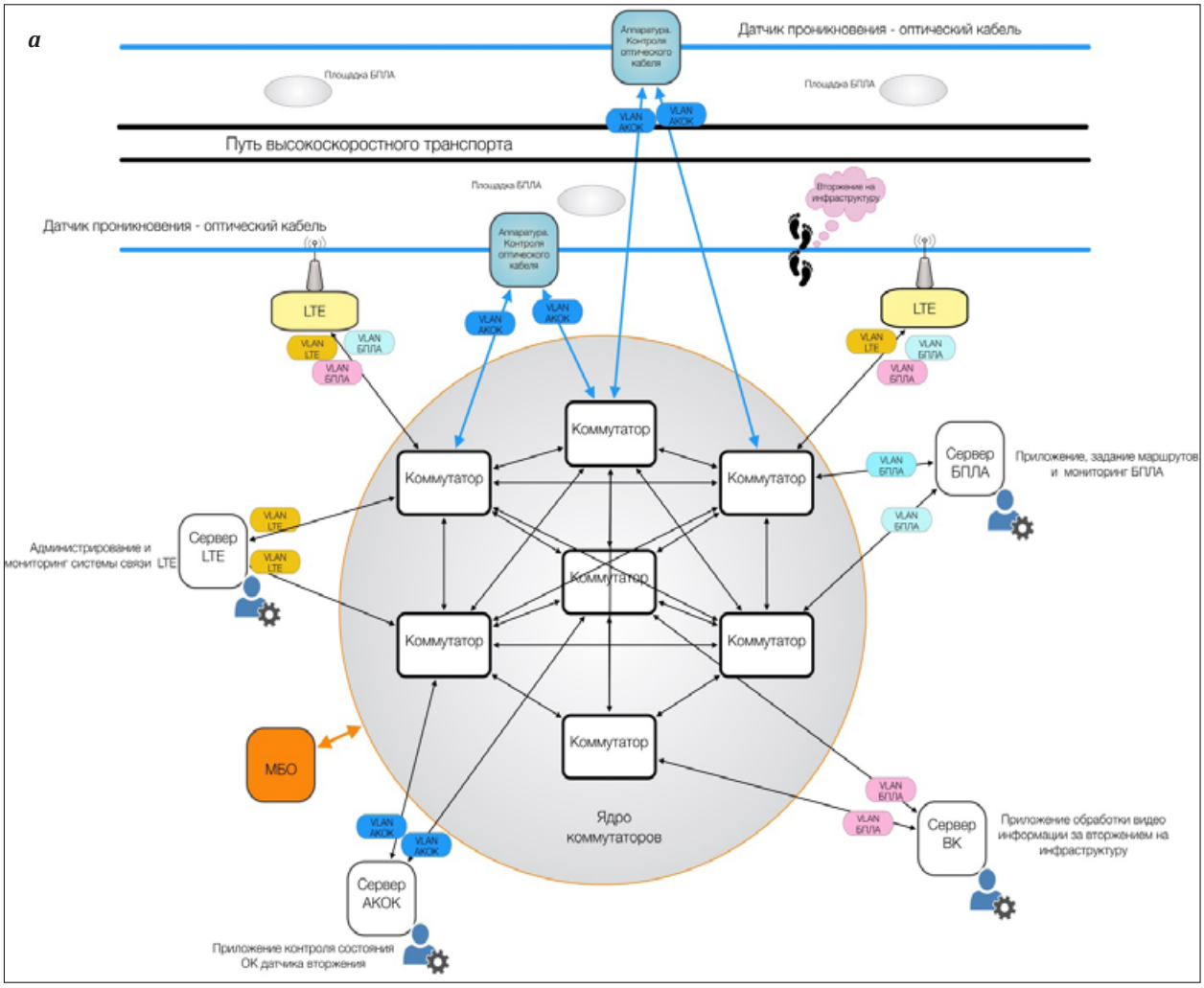
It is difficult to determine the nature of penetration using OK due to short-term exposure. In this regard, it is rational to use a UAV with a set of fixing cameras, which approaches the place of occurrence of the incident and captures the object of penetration at a short distance, transmits this information to the center, which determines the degree of danger. Video cameras, LiDAR and a thermal imager are installed on the UAV. This allows you to have an integrated picture of penetration at different times of the day and under all weather conditions.

The joint use of the UAV and the OK sensor allows you to create a reliable system for monitoring the intrusion on the infrastructure. The implementation of this approach imposes increased requirements on the network structure. How is this shown?

Firstly, for processing images from LIDAR cameras with thermal imagers mounted on UAVs, high-speed transmission of a large amount of information is required.

Secondly, for processing (on servers) it is necessary to use the technology of parallel processing of threads.

Thirdly, the organization of the structure should be based on the use of optical local networks and database equipment, which allows working at a data transfer rate of more than 20 GB/s.



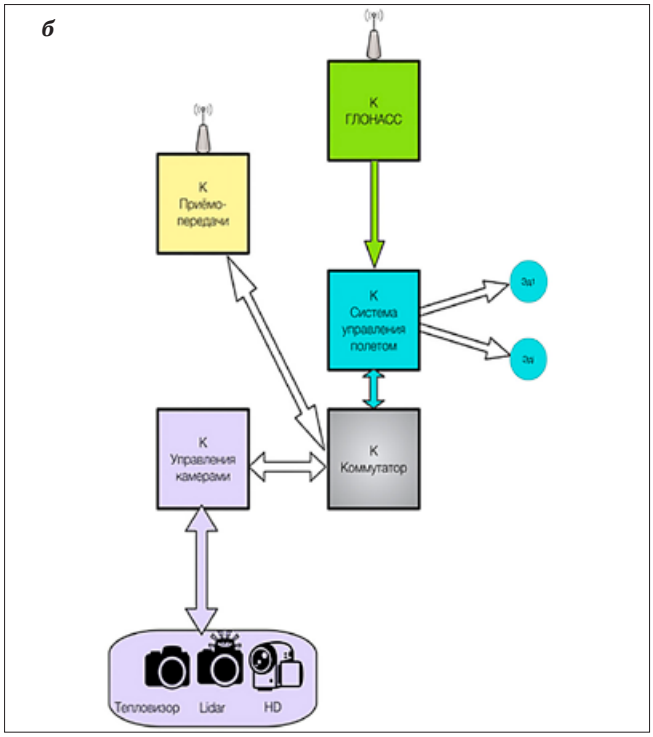


Figure 1 *- The structure of the drone network (a) and the processing center (b)*

The goal is to develop the structure of a local area network (LAN) for detecting an intrusion on the TSA transport infrastructure and image processing using a model based on a neural network.

Information delivery channels are built on the use of 4G (LTE) or 5G. This uses a ring structure that provides transmission in one of the two transmission directions. If a failure occurs in one of the sections of the LTE information transmission, the system transmits information on the second (not failed) ring. The local area network contains databases and servers for LTE, UAV video cameras and thermal imagers, as well as servers and databases for optical cable [2].

UAV quadrocopter video surveillance equipment consists of:

- HD camera;
- Lidar;
- Thermal imager.

The image is synchronized, according to the growth of the image. This means that a certain pixel with a HD camera is assigned a Lidar pixel and a thermal imager. It must be borne in mind that the resolution and ability of these devices is different. Therefore, when building a model, it is necessary to respect this feature. Let us consider the structure of the network equipment on the UAV. Figure 1a shows the structure of the UAV network equipment. The central device is switch K, which combines 4G (LTE) signal reception and transmission controllers, a flight control system controller connected to the GLONASS controller. On a separate port of the switch K, the controller for controlling cameras is turned on: HD, Lidar and thermal imager (Thermal imager). It is important to note that the operation of the cameras on board the UAV is synchronized. This means synchronous adjustment of the focal length and rotation angles. The flight control system controls the drone's ED engines, providing a given movement trajectory received from the UAV's central server (Figure 1б).

Consider the interaction of specialists and applications located in the LAN with the UAV. AKOK equipment is aimed at the task of detecting an intrusion on the infrastructure. In the absence of violations of the "speckle" images I(t) is sent to the data processing server:

$It = I_{t+\Delta t}$ - no violations. (1)

In the event of an invasion, there is a change in the "speckle"

$It \neq I_{t+\Delta t}$ - a violation has occurred. (2)

The reliability of the process is at the level of 0.96, which provides a ten-bit ADC of the parallel type.

When a signal is received, the unmanned vehicle is given a route of movement: approximately end points and characteristic points of the route (x*, y*, z*), which ensure avoidance of obstacles on the path of movement. Communication is carried out via a channel (LTE). This information is sent to the flight control system, where the engine control signal is generated. The flight control system compares the current coordinates coming from the GLONASS controller (x^t,y^t,z^t) with the given ones (x*,y*,z*). Based on the difference between the current and given coordinates, the drone movement is corrected [3, 4].

The LAN structure of the intrusion detection system consists of MK (4G) controllers providing 4G (LTE) communication between the center (Figure 1b) and the UAV (Figure 1a). The purpose of MK (4G) is the transmission and reception of information. The flight control system controller controls the movement of the UAV to the intrusion site.

The camera control MC configures the cameras to transmit the aggregated video control image us-

ing HD cameras, cameras with LIDAR and a thermal imager camera to the center. The control of pointing cameras at the place of penetration is carried out by a specialist. Upon reaching the approximate location of the intrusion, the HD and Lidar cameras are turned on during the daytime, and at night, an additional camera with a thermal imager is activated to detect the presence of a person or animals, the presence of a person or animals, as well as the possible location of cars or other equipment. Based on the received image, an analysis of the causes and possible consequences of the intrusion is carried out. This is done by a specialist, carefully examining the site of the invasion. Lidar is used to determine the distance to objects located in the area of invasion [5].

The platform for the UAV is guarded. Motion sensors are used as security sensors. Power is provided - during the day from solar collectors, at night from the network. In the event of an attack on the UAV site, the UAV site immediately leaves in order to prevent damage to them and to identify the circumstances of the attack situation.

The task of recognition should provide identification of the penetration of various objects into the infrastructure. This should be done on the basis of recognition methods. Currently, one of the most common approaches is the use of neural networks [6, 7, 8]. An optical cable, as mentioned above, allows you to fix the place and moment of penetration into a distributed infrastructure. In this regard, the training of the recognition model should take place continuously, since the parameters of the optical cable, as a rule, are not restored after the physical impact of the intruder. This imposes the condition of fast retraining of the violation fixation model. In order to determine the penetration point, special notches are created in the optical cable, reflecting part of the light flux. Under the mechanical action of the intruder, an additional reflection signal appears, which does not coincide with the reflected signal of the notches. The difference between these signals determines the distance to the point of penetration. The task of recognition, which is solved using unmanned aerial vehicles, differs from the task of recognition of OK. In this case, the problem of belonging of the intruder-object to one of the preset reference images is solved. The most common approach to solving these problems is the use of neural networks [9].

Let us consider the implementation of a recognition model based on a neural network. To train neural networks, the back propagation algorithm is used [10]. Training by the error backpropagation algorithm involves two passes through all layers of the network: forward and backward. The backpropagation algorithm involves the use of gradient descent and is one of the effective learning algorithms. Assume that there are $R_j; j = 1, m$ source images of intrusion objects:

$$X_k^{R_j} => Y_j, \tag{3}$$

where $X_k^{R_j}$ – is the input feature vector of the original images R_j, $R_j => Y_j$, $j = 1, m$, $k = 1, m$, Y_j,
Y_j - hidden layer vector of network outputs corresponding to the input vector: $X_k^{R_j}$.

The output of hidden neurons Y_j represented as the scalar product of features $X_k^{R_j}$ and the weight vector $w_{k_j}^i$ given initially randomly:

$$Y_j = \Sigma_{k=1}^m w_{k_j}^i \times X_k^{R_j}; i = 1, \bar{l}; \tag{4}$$

$$Y_j^* = F_a(Y_j), \tag{5}$$

where Y_j^* - neural network softmax output function [10],
F_a - activation function, non-linear function.

The activation function can be: sigmoid, hyperbolic tangent, logarithmic function and other nonlinear functions. The introduction of a non-linear function is necessary so that the separating functions are non-linear and allow one to build a nonlinear separation of the points of the original images.

The learning task is to calculate the value $w_{k_j}^i$ of the weights, which are determined using the back propagation algorithm.

Let's introduce the notation $L^{R_j}(w_{kj}^i)$ - the loss function of non-linear regression. We start training with the choice of initial weights $w_{k_j}^i$, then we make updates on all weights w_{kj}^{i+1}, we get:

$$w_{kj}^{i+1} = w_{k_j}^i - \eta \times \frac{L^{R_j}(w_{k_j}^i)}{\partial w_{k_j}^i}, \tag{6}$$

where η - learning rate coefficient 0<η <1.

The functional $L^{R_j}(w_{kj}^i)$ is subject to minimization and is determined by the following formula:

$$L^{R_j}(w_{kj}^i) = -\sum_{j=1}^m \left(Y_j^* \times ln\left(\overline{f}(Y_j^*)\right) + (1 - Y_j^*) \times \left(1 - ln\left(1 - \overline{f}(Y_j^*)\right)\right)\right) -> min_w\left(L^{Rj}(w_{kj}^i)\right),$$

where $\bar{f}(Y_j) = F_a\left(\left(w_{kj}^{T_i} \times x_k^{Rj}\right)\right)$. (7)

The gradient optimization method consists in iterative refinement of w_{kj}^{i+1} according to formula (5). The initial value of the parameter η is chosen small enough to ensure convergence.

Thus, we can draw the following conclusion: the rate of convergence of the learning process is determined by the gradient method of finding the minimum $L^{R_j}(w_{kj}^i)$ (6). However, it is essential that the introduction of nonlinearity and the use of differentiable functions at all stages of the implementation of the neural network allows you to implement feedback (error backpropagation algorithm), thereby automatically searching for a solution, for a given activation function and the number of layers of the neural network [11, 12].

Findings. The paper proposes the structure of a network of unmanned aerial vehicles, which implements modern approaches to building an information system for a model for analyzing penetration into a distributed structure of transport.

The penetration analysis model for a distributed transport infrastructure must be built using two technical solutions: determining the location of penetration using optical cable technology, and identifying penetration objects based on the analysis of images from HD cameras, LiDAR thermal imagers installed on unmanned aerial vehicles.

It is proposed to use recognition methods based on neural networks to process images and determine the degree of danger of penetration.

Acknowledgements

The study was financially supported by the Russian Foundation for Basic Research, NTU Sirius, JSC Russian Railways and the Talent and Success Educational Foundation within the framework of the scientific project No. 20-37-51001 (Application 2020): transport systems (GRTS) based on big data technology.

Information about authors

Alekseev Viktor Mikhailovich - Professor of the Department of Information Management and Security, Russian University of Transport (MIIT)
academic degree: doctor of technical sciences
academic title: professor
e-mail: alekseevvm@rambler.ru

Khusenov Dodokhon Naimboevich – post-graduate student of the department "Information Management and Protection" of the Russian University of Transport (MIIT)

Andreev Andrey Andreevich - post-graduate student of the department "Management and information protection" of the Russian University of Transport (MIIT)

Chichkov Sergey Nikolaevich - post-graduate student of the department "Management and information protection" of the Russian University of Transport (MIIT)

Обработка изображений беспилотных летательных аппаратов с использованием нейронной сети

Алексеев Виктор Михайлович, Хусенов Додохон Наимбоевич, Андреев Андрей Андреевич, Чичков Сергей Николаевич

Российский университет транспорта (МИИТ), alekseevvm@rambler.ru

Оригинальная научная статья

Аннотация: Объекты транспортной инфраструктуры являются критически важными. Для обеспечения их функционирования необходимо применять методы слежения обеспечивающие высокую степень защиты. В статье рассматриваются вопросы контроля несанкционированного вторжения посторонних объектов, с целью предотвращения опасного воздействия на инфраструктуру высокоскоростного транспорта. В этой связи, предлагается вести круглосуточное наблюдение с использованием беспилотных летательных аппаратов.

В связи с тем, что диапазон расстояния действий БПЛА ограничен, поэтому предлагается применение дистанционного метода обнаружения вторжения объектов на инфраструктуру с использованием оптического кабеля ОК. Совместное использование БПЛА и ОК позволяют создать надежную систему, обеспечивающую контроль за вторжением на инфраструктуру. На беспилотных летательных аппаратах устанавливается специальные видеокамеры (тепловизоров, Lidar), обеспечивающие осмотр места вторжения как в дневное, так и в ночное время. Поскольку устройства видеофиксации имеют различную разрешающую способность в работе ставится задача применения методов интеграции данных с различной разрешающей способностью и обработку их нейронной сетью. Реализация систем слежения за инфраструктурой предъявляет повышенные требования к структуре сети. Одной из задач, которая ставится в данной статье является – разработка структуры сети обнаружения вторжения на транспортную инфраструктуру высокоскоростного наземного транспорта.

Ключевые слова: оптический кабель, локальная вычислительная сеть, структура сети беспилотного аппарата, видеокамеры, вторжение на инфраструктуру.

Актуальность. Высокоскоростное движение (ВСД) требует расширения функциональных возможностей систем безопасности направленное на применение новых методов, а именно теоретически и технически обоснованных решений в связи с возможными актами вандализма и терроризма. ВСД требует пересмотра технических решений в разработке критических систем (охраны объектов и защиты информации) и увязки с существующими системами управления (ДЦ, МПЦ и другие). При больших скоростях незначительные изменения параметров пути, например, из-за изменения структуры верхнего строения пути, вызванного подмывом, может привести к аварии. Обрушение скальных пород, проникновение на инфраструктуру посторонних объектов, также являются потенциально опасными для движения высокоскоростного состава.

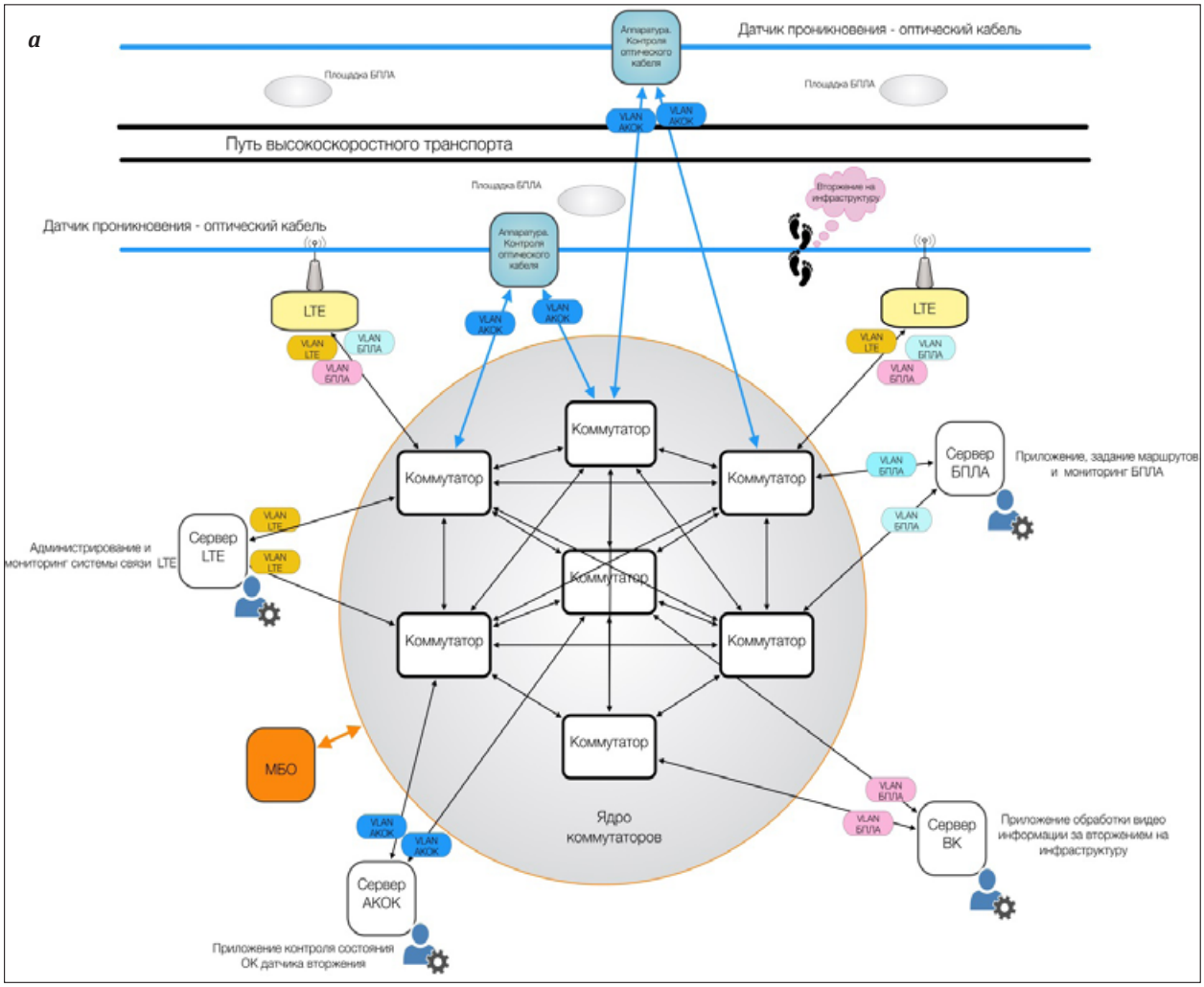
В этой связи, требуется разработка новых решений не только к контролю инфраструктуры пути движения подвижного состава, но и крайне важно, к определению момента возникновения препятствия, вызванного несанкционированным появлениям посторонних объектов, несущих опасность движению и дальнейшей передачи информации в системы управления с целью принятия рационального управления. Существующие системы управления высокоскоростными составами ДЦ, МПЦ и автоблокировки обеспечивают безопасное управление объектами стрелками, сигналами другими устройствами, но не предназначены для контроля и формирования информа-

ции о появлении на инфраструктуре посторонних объектов, оползней, обвалов и других внешних опасных воздействий. Эта функция возлагается на независимые системы, которые агрегируя информацию определяют причины возникновения опасной ситуации и передают эту информацию в системы управления и обеспечения безопасности движения, которые корректируют движение поездов в условиях возникшей угрозы.

Один из таких подходов заключается в том, что необходимо применение комбинированного метода контроля, использующего оптический кабель (ОК) и беспилотные летательные аппараты, оборудованные устройствами видеорегистрации возникшей угрозы в различное время суток и в любых погодных условиях.

Первичную информацию о возникновении инцидента даёт оптический кабель, выступающий датчиком, который прокладывается несколькими способами: под землей или на заградительных щитах. Принцип действия ОК - датчика заключается в том, что в нем изменяются условия прохождения излучений (из-за механического воздействия), в результате чего изменяется картина (так называемый спекл) на выходном конце. Определение характера проникновения с помощью ОК ввиду кратковременного воздействия затруднительно. В этой связи, рационально использовать БПЛА с набором фиксирующих камер, который приближается к месту возникновения инцидента и на небольшом расстоянии фиксирует объект проникновения, передаёт эту информацию в центр, который определяет степень возникшей опасности. На БПЛА устанавливают видеокамеры, LiDAR и тепловизор. Это позволяет иметь интегрированную картину проникновения в различное время суток и при любых погодных условиях.

Совместное использование БПЛА и ОК-датчика позволяют создать надежную систему контроля за вторжением на инфраструктуру. Реализация данного подхода предъявляет повышенные требования к структуре сети. В чем это проявляется?



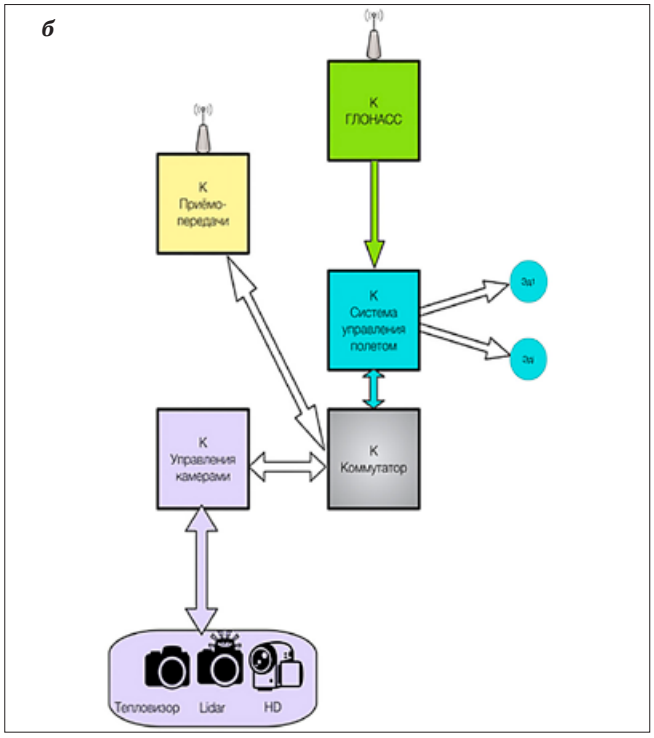


Рисунок 1 *- Структура сети беспилотника (а) и центра обработки (б)*

Во-первых, для обработки изображений с камер с LIDAR с тепловизорами, установленными на БПЛА необходима высокоскоростная передача большого объема информации.

Во-вторых, для обработки (на серверах) необходимо применять технологию параллельной обработки потоков.

В-третьих, организация структуры должна базироваться на применении оптических локальных сетей и оборудовании баз данных, позволяющая работать на скорости передачи данных свыше 20 ГБ/с.

Целью является – разработка структуры локальной вычислительной сети (ЛВС) обнаружения вторжение на транспортную инфраструктуру ВСТ и обработка изображения с помощью модели на основе нейронной сети.

Каналы доставки информации строятся на использовании 4G (LTE) или 5G. При этом используется кольцевая структура, обеспечивающая передачу в одном из двух направлений передачи. При возникновении отказа на одном из участков передачи информации LTE система передаёт информацию по второму (не отказавшему) кольцу. Локальная вычислительная сеть содержит базы данных и сервера для LTE, видеокамер и тепловизоров БПЛА, а также сервера и базы данных для оптического кабеля [2].

Оборудование видеонаблюдения квадрокоптера БПЛА состоит из:

- камера HD;
- Lidar;
- тепловизор.

Изображение синхронизировано, по растру изображения. Это означает, что определенному пикселю с камеры HD соответствует пиксель Lidar и тепловизора. Надо иметь ввиду, что разрешающая способность этих устройств различна. В этой связи, при построении моделей необходимо учитывать эту особенность. Рассмотрим структуру сетевого оборудования на БПЛА.

На рисунке 1а показана структура сетевого оборудования БПЛА. Центральным устройством является коммутатор К, который объединяет контроллеры приема-передачи сигналов 4G (LTE), контроллер системы управления полетом, связанный с контроллером ГЛОНАСС. На отдельном порту коммутатора К включается контроллер управления камерами: HD, Lidar и тепловизора (Тепловизор). Важно отметить, что работа камер на борту БПЛА синхронизирована. Это означает синхронную регулировку фокусного расстояния и углы поворота. Система управления полетом управляет двигателями ЭД беспилотника, обеспечивая заданную траекторию движения, полученную из центрального сервера БПЛА (рисунок 1б).

Рассмотрим взаимодействие специалистов и приложений, находящихся в ЛВС с БПЛА. Оборудование АКОК нацелено на задачу фиксации вторжения на инфраструктуру Приложение АКОК работает по модели осуществляющий непрерывный контроль состояний ОК. При отсутствии нарушений «спекл» изображений I(t) поступает на сервер обработки данных:

$It = I_{t+\Delta t}$ - нарушений нет. (1)

В случае вторжения происходит изменение «спекла»

$It \neq I_{t+\Delta t}$ - произошло нарушение . (2)

Достоверность процесса на уровне 0,96, что обеспечивает десятиразрядный АЦП параллельного типа.

При поступлении сигнала беспилотному аппарату задается маршрут движения: приблизительно конечные точки и характерные точки

маршрута (x*,y*,z*), обеспечивающие огибание препятствий на пути движения. Связь осуществляется через канал (LTE). Эта информация поступает на систему управления полетом, где формируется сигнал управления двигателями. В системе управления полетом происходит сравнение текущих координат, поступающих с контроллера ГЛОНАСС (xt,yt,zt), с заданными (x*,y*,z*). На основании разности между текущими и заданными координатами осуществляется корректировка движения беспилотника [3, 4].

Структура ЛВС системы обнаружения вторжения состоит из контроллеров МК (4G) обеспечивающих связь по технологии 4G (LTE) между центром (рисунок 1б) и БПЛА (рисунок 1а). Назначение МК(4G) – передача и прием информации. Контроллер системы управления полетом осуществляется управление движением БПЛА к месту вторжения.

МК управления камерами осуществляет настройку камер для передачи агрегированного изображения видеоконтроля с помощью камер HD, камер с LIDAR и камеры тепловизора в центр. Управление наведением камер на месте проникновения осуществляет специалист. Достигнув приблизительного места вторжения, включается камера HD и Lidar в дневное время, а в ночное время дополнительно камера тепловизором с целью выявления присутствия человека или животных присутствие человека или животных, а также возможного нахождения машин или иной техники. На основании полученного изображения проводится анализ причин и возможных последствий произошедшего вторжения. Этим занимается специалист, тщательно обследуя участок вторжения. Lidar служит для определения расстояния до объектов находящихся на участке вторжения [5].

Площадка для БПЛА охраняемая. В качестве датчиков охраны используются датчики движения. Питание осуществляется - днем от солнечных коллекторов, ночью от сети. В случае нападения на площадку БПЛА, происходит незамедлительное покидание площадки беспилотников с целью предотвращения их повреждения и выявлений обстоятельств ситуации с нападением.

Задача распознавания должна обеспечить идентификацию проникновения на инфраструктуру различных объектов. Это должно осуществляться на основе методов распознавания. В настоящее время, одним из наиболее распространенных подходов является применение нейронных сетей [6, 7, 8]. Оптический кабель, как было указано выше, позволяет фиксировать место и момент проникновения на распределённую инфраструктуру. В этой связи, обучения модели распознавания должно проходить непрерывно, так как параметры оптического кабеля, как правило, не восстанавливаются после физического воздействия нарушителя. Это накладывает условие быстрого переобучения модели фиксации нарушения. С целью определения места проникновения в оптическом кабеле создаются специальные насечки, отражающие часть светового потока. При механическом воздействии нарушителя появляется дополнительный сигнал отражения, который не совпадает с отраженным сигналом насечек. По разности этих сигналов определяется расстояние до места проникновения. Задача распознавания, которая решается с использованием беспилотных летательных средств отличается от задачи распознавания ОК. В этом случае, решается задача принадлежности нарушителя-объекта к одному из заранее заданных эталонных изображений. Наиболее распространённым подходом в решении этих задач является использование нейронных сетей [9].

Рассмотрим реализацию модели распознавания на основе нейронной сети. Для обучения нейронных сетей применяется алгоритм обратного распространения ошибки (back propagation) [10]. Обучение алгоритмом обратного распространения ошибки предполагает два прохода по всем слоям сети: прямого и обратного. Алгоритм обратного распространения ошибки предполагает применение градиентного спуска и является одним из эффективных обучающих алгоритмов. Предположим, что имеется $R_j; j = 1$ исходных изображений объектов вторжения:

$$X_k^{R_j} => Y_j, \quad (3)$$

где $X_k^{R_j}$ – входной вектор признаков исходных изображений R_j, $R_j => Y_j$, $j = 1, m$, $k = 1, m$, Y_j, Y_j - вектор скрытого слоя выходов сети, соответствующий входному вектору: $X_k^{R_j}$.

Выход скрытых нейронов Y_j представляется как скалярное произведение признаков $X_K^{R_j}$ на вектор весов $w_{k_j}^i$ заданный начально случайно:

$$Y_j = \Sigma_{k=1}^m w_{k_j}^i \times X_k^{R_j}; i = 1, \bar{l}; \quad (4)$$

$$Y_j^* = F_a(Y_j), \quad (5)$$

где Y_j^* - выходная функция softmax нейронной сети [10],

F_a - функция активации, нелинейная функция.

В качестве функции активации могут выступать: сигмоида, гиперболический тангенс, логарифмическая функция и другие нелинейные функции. Введение нелинейной функции необходимо для того, чтобы разделяющие функции были нелинейными и позволяли строить нелинейное разделение точек исходных изображений.

Задача обучения состоит в расчёте значения $w_{k_j}^i$ весов, которые определяются с помощью алгоритма обратного распространения ошибки back propagation.

Введём обозначения $L^{R_j}(w_{kj}^i)$ - функция потерь нелинейной регрессии. Обучение начинаем с выбора начальных весов $w_{k_j}^i$, далее делаем обновления по всем весам w_{kj}^{i+1}, получаем:

$$w_{kj}^{i+1} = w_{k_j}^i - \eta \times \frac{L^{R_j}(w_{k_j}^i)}{\partial w_{k_j}^i}, \quad (6)$$

где η - коэффициент скорости обучения 0<η <1.

Функционал $L^{R_j}(w_{kj}^i)$ подлежит минимизации и определяется следующей формулой:

$$L^{R_j}(w_{kj}^i) = -\sum_{j=1}^{m}\left(Y_j^* \times ln\left(\bar{f}(Y_j^*)\right) + (1 - Y_j^*) \times \left(1 - ln\left(1 - \bar{f}(Y_j^*)\right)\right)\right) -> min_w\left(L^{Rj}(w_{kj}^i)\right), \quad (7)$$

где $f(Y_j) = F_a\left(\left(w_{kj}^{T_i} \times x_k^{Rj}\right)\right)$.

Градиентный метод оптимизации состоит в итерационном уточнении w_{kj}^{i+1} согласно формуле (5). Начальное значение параметра η выбирается достаточно малым для обеспечения сходимости.

Таким образом, можно сделать следующий вывод: скорость сходимости процесса обучения определяется градиентным методом поиска минимума $L^{R_j}(w_{kj}^i)$ (6). Однако, существенно то, что введение нелинейности и использование дифференцируемых функций на всех этапах реализации нейронной сети, позволяет реализовать обратную связь (алгоритм обратного распространения ошибки), тем самым осуществить автоматический поиск решения, при заданной функции активации и количестве слоев нейронной сети [11, 12].

Выводы. В работе предложена структура сети беспилотных летательных средств, в которой реализованы современные подходы к построению информационной системы для модели анализа проникновения на распределённую структуру транспорта.

Модель анализа проникновения на распределённую инфраструктуру транспорта необходимо строить с использованием двух технических решений: определение местоположения проникновения с применением технологии оптического кабеля, а идентификацию объектов проникновения на основе анализа изображений с камер HD, LiDAR тепловизора, установленных на беспилотных летательных средствах.

Предложено для обработки изображений и определения степени опасности проникновения применять методы распознавания на основе нейронных сетей.

Благодарности.

Исследование выполнено при финансовой поддержке РФФИ, НТУ «Сириус», ОАО «РЖД» и Образовательного фонда «Талант и успех» в рамках научного проекта № 20-37-51001 (Заявка 2020 года): «Разработка моделей и методов оптимизации производственных ресурсов городских рельсовых транспортных систем (ГРТС) на основе технологии больших данных (bigdata)».

References / Список использованных источников

[1] Алексеев В.М., Хусенов ДН. // ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ материалы Международной научно-практической конференции. Москва, 2022г., С. 379-384.

[2] Доклады и статьи ежегодной научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами», г. Коломна, 2016. С. 274 .

[3] Ким Н.В., Кузнецов А.Г., Крылов И.Г. Применение систем технического зрения на беспилотных летательных аппаратах в задачах ориентации на местности // Вестник МАИ. - 2010. - Т. 17, № 3. - С. 46-49. EDN:

MTYMWP
[4] Чиванов А.Н. Методы повышения технических характеристик тепловизоров // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2004. № 15. С.132-136.
[5] Поляков А.В., Сахончик Д.Г. Оптоволоконная подземная система охраны периметра // В сборнике: Квантовая электроника. Материалы XI Международной научно-технической конференции. 2017. С. 141-143.
[6] Сайт Евразийский научный журнал: https://journalpro.ru/articles/algoritm-obucheniya-mnogosloynoy-neyronnoy-seti-metodom-obratnogo-rasprostraneniya-oshibki/ Дата 19.03.2022.
[7] Сайт IBM: https://www.ibm.com/ru-ru/cloud/learn/neural-networks Дата 19.03.2022
[8] Сайт Евразийский научный журнал: https://journalpro.ru/articles/algoritm-obucheniya-mnogosloynoy-neyronnoy-seti-metodom-obratnogo-rasprostraneniya-oshibki/ Дата 19.03.2022.
[9] Доклады и статьи ежегодной научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами», г. Коломна, 2016. – 274 с.
[10] Сайт Prog.Tversu: http://prog.tversu.ru/da/02-learning.pdf Дата 19.03.2022.
[11] Йеллепедди А. Увеличение дальности обнаружения объектов лидаром с применением метода слежения // Электроника: Наука, технология, бизнес. 2021. № 3 (204). С. 88-91.
[12] Алексеев В.М., Кулагин МА. //ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ, материалы Международной научно-практической конференции. Москва, 2022г., С. 40-44.

Received: May 17, 2022 / Получено: 17 мая 2022 г.
Accepted: October 10, 2022 / Принято: 10 октября 2022 г.

Сведения об авторах

Алексеев Виктор Михайлович – профессор кафедры «Управление и защита информации» Российского университета транспорта (МИИТ)
ученая степень: доктор технических наук
ученое звание: профессор
e-mail: alekseevvm@rambler.ru

Хусенов Додохон Наимбоевич – аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ)

Андреев Андрей Андреевич - аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ)

Чичков Сергей Николаевич - аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ)

For citation
Alekseev Viktor Mikhailovich, Khusenov Dodokhon Naimboevich, Andreev Andrey Andreevich, Chichkov Sergey Nikolaevich, Unmanned Aerial Vehicles Image Processing With the Use of a Neural Network, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 12(2022) 2:89-99, (UDC: 623.746.2-519:629.7.014.9), (DOI: 10.7251/JIT2202089M), Volume 12, Number 2, Banja Luka, December (65-172), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004