Intelligent SDN Architecture With Fuzzy Neural Network and Blockchain for Monitoring Critical Events

Alexey Finogeev\textsuperscript{a}\textsuperscript{,} Michael Deev\textsuperscript{a}, Danila Parygin\textsuperscript{b}, and Anton Finogeev\textsuperscript{a}

\textsuperscript{a}CAD Department, Penza State University, Penza, Russia; \textsuperscript{b}CAD Department, Volgograd State Technical University, Volgograd, Russia

ABSTRACT

The article deals with the creation of an intelligent architecture of the Internet of Things transport environment based on software-defined network (SDN) and blockchain for detecting threats and attacks. The transport environment is created for the monitoring system of critical events in the road transport infrastructure. Blockchain technology is used to authenticate network nodes, store sensor data in a distributed ledger. The network packet clustering method based on a fuzzy neural network is used to detect packets with possible malicious content. The intelligent SDN architecture is a hierarchy of four layers with six levels and includes: a) edge computing layer (sensor nodes and routers level, SDN switches data level), b) fog computing layer (zone server level, control level in SDN controllers), c) a cloud computing layer with data center servers, d) a layer for presenting monitoring results on user devices and applications. Detection of threats and attacks is implemented by validating network nodes and analyzing header fields of IP packets and TCP segments. The intrusion detection system includes a parser and analyzer of data packets, a module for filtering traffic by type, port numbers and other characteristics of packets, a module for synthesizing digital signatures of trusted nodes and their validation, a module for analyzing and clustering packets based on fuzzy logic and a neural network, modules for logging procedures. The probability function of packets belonging to clusters is tuned through deep learning of a five-layer neural network. The conclusion about belonging and degree of similarity with malicious packages is formed using the fuzzy logic apparatus. To train the neural network, the previously synthesized rules of the flow tables and the identified signs of atypical data packets are used. The functionality and effectiveness of the SDN architecture with an intrusion detection system is validated by simulating procedures in the NS3 Simulator system, evaluating authenticity, latency, throughput, response time, and accuracy in detecting atypical data packets.

Introduction

The introduction of Internet of Things (IoT) technologies into various spheres of human life has led to the widespread use of machine-to-machine interaction...
between cyber-physical systems. Cyber-physical systems exchange data in the IoT transport environment, including sensor networks, which are connected through gateways to the Internet. Such systems include networks of sensors, actuators, drives, information-measuring and control devices, program-controlled machine tools, programmable logic controllers, image processing devices and robotic complexes, unmanned systems integrated into the IoT network with the ability to access them from the Internet. An increase in the number of machine-to-machine interactions for communication between nodes of sensor networks, gateways and computing devices, control of production and technological processes, remote access via the Internet causes an increase in information security threats. The problem is that the IoT combines security threats specific to sensor networks with threats that traditionally exist on the Internet (Alexey Finogeev et al, 2017). An increase in the risk of information attacks is also associated with a steady increase in the number of cyber-physical IoT devices and mobile communication tools for accessing sensor data, with the distributed nature of networks of sensor data transmission channels, remoteness and autonomy of the functioning of network nodes (Zaman et al., 2021). Information risks increase when using wireless data exchange technologies. The greatest threat in IoT sensor networks is flooding attacks in the form of generating a large number of third-party requests to network nodes, which leads to a reaction in the form of a “denial of service” (DoS attack) (Mauro Contia et al, 2018). In addition to ensuring the stable operation of distributed sensor nodes and secure traffic transmission, it is necessary to solve the problem of reliable distributed storage of the results of collection and primary processing of sensor data.

To solve the tasks of improving the stability and security of IoT networks, it is proposed to use a software-defined network (SDN) architecture with distributed registry technology and an intelligent intrusion detection system to ensure the secure collection, transmission, processing and storage of sensor data. Abnormal situations and security problems of sensor networks and distributed autonomous cyber-physical objects can be prevented by monitoring network traffic parameters, authenticating network nodes, and analyzing data packets. The results are supposed to be used for predictive analysis and predictive assessment of possible risks of abnormal events at distributed objects.

In modern information flow management systems, there are basically no real-time traffic mining mechanisms to prevent the occurrence and implementation of information risks and threats. In addition, traditional methods for protecting sensor networks and network nodes require appropriate computing and energy resources, which is not always possible due to the limited capabilities of sensor devices. As you know, the procedures for collecting and processing sensory data from distributed cyber-physical systems are implemented using the technologies of “edge,” “fog” and “cloud” computing. The
tasks of source authentication, intellectual analysis and recognition of malicious data packets can be solved at three levels: the level of sensor nodes of the edge layer (sensors and measuring devices, coordinators, gateways, routers, switches), the level of nodes of the foggy layer of data processing (controllers, zone servers), the level of the cloud data processing layer (computers and servers of data processing centers). However, due to the limited computing and energy resources of sensor nodes, the use of blockchain technologies, intellectual analysis and neural networks to process network traffic and authenticate network nodes through edge computing is very problematic. Therefore, the article describes an intelligent intrusion detection system that is implemented on zone servers and in SDN fog level controllers.

Recently, researchers have proposed ways to use the architecture of software-defined networks (SDN) to ensure the information security of network systems (Latif et al., 2022; Islam & Rahman et al., 2021). The main idea of SDN is to separate the level of logical control of the network from the level of switching and relaying of data packets in network switches. Data flows in the network are managed by SDN controllers, which are mainly used in specialized systems (Internet of things, industrial networks, sensor networks, etc.) (Zhu et al., 2021). Network switches play the role of packet relays according to the flow distribution rules. However, the SDN architecture has a number of limitations compared to conventional networks. For example, one should note the problem of SDN scalability associated with the centralization of flow control in the SDN controller (Yeganeh et al., 2013). Another SDN problem is related to distributed DoS attacks, when the controller does not have time to process incoming requests and generate new flow table rules for switches (Valdovinos et al., 2021). Therefore, to protect network traffic, methods and tools are needed to detect and prevent information attacks. To implement intrusion detection systems in SDN, it is advisable to use the methods and technologies of machine learning, intellectual and statistical analysis, neural networks, virtualization of network functions and blockchain (Shakila Zaman et al, 2021; Iqbal Alam et al, 2021).

The article presents a model and methods for ensuring the information security of the IoT transport environment in the process of collecting and processing sensor data on spatially distributed sensor nodes using the SDN architecture, distributed registry technologies (blockchain), intellectual analysis and neural networks for node authentication, analysis of sensor packets, data, synthesis of flow table rules, safe and secure storage of sensory data and transactions.

**Theoretical Background**

The current state of industrial development within the fourth revolution (Industry 4.0) is characterized by the transition to the mass adoption of digital and intelligent technologies. Digitalization and intellectualization involve the introduction and application of cyber-physical systems that exchange data
flows in real time through sensor networks, IoT and the Internet according to industrial information integration technologies (Chen, 2020). Sensor networks and IoT technologies are used in many areas of human life, including the creation of intelligent production and technological lines, in smart home and smart city projects, in energy and environmental monitoring systems, in intelligent transport systems and road monitoring systems, in intelligent dispatching systems, etc. (L.D. Xu et al, 2014).

The results of the design studies presented in this article are related to the creation of a safe and reliable transport IoT environment for collecting, processing, transmitting and storing big sensor data in monitoring systems for abnormal events and accidents at spatially distributed critical infrastructure facilities in urban or industrial systems. The transport environment is built using wireless sensor networks and is part of the IoT network with support for remote access from mobile and stationary Internet nodes. In the process of collecting and consolidating sensory data from heterogeneous cyber-physical devices in the IoT network, procedures for analyzing and verifying data blocks and network nodes are implemented in order to detect and prevent the risks of occurrence and development of information attacks (Xu, 2020). A safe transport environment is being developed to support the functioning of an intelligent monitoring system for road transport infrastructure (Alexey Finogeev & Anton Finogeev, 2017). The system works with large sensory data on traffic accidents and violations of traffic rules for predictive analysis of traffic situations under the influence of external factors (Finogeev et al., 2017). Data is collected from a variety of photo radar complexes for photo and video recording of violations, as well as from CCTV cameras distributed over a large area of city highways, which are placed and used as part of the “Safe City” and “Safe Roads” concepts (Anton Finogeev et al, 2020).

To solve the problems associated with ensuring the security of the IoT transport environment for collecting, transmitting and storing large amounts of sensory data at many dispersed photo and video recording nodes, it is proposed to use SDN technologies for reliable and stable data flow management, a distributed registry (blockchain) for network authentication nodes and storage of sensory data, intelligent analysis of data packets, neural networks, fuzzy logic and deep learning to detect likely information threats and attacks.

At present, the topic of using a distributed registry (blockchain) is especially relevant in the light of advances in the organization of distributed decentralized secure data stores using hashing technologies for unique identification of data blocks and transactions. For example, in 2021 alone, the IEEE Xplore archive contains more than 2,500 publications on this topic. Blockchain technology is being actively implemented in IoT today (Khan et al., 2019). Most cyber-physical systems in the IoT transmit data streams through public channels of cellular communication providers, which causes
problems with ensuring the confidentiality and integrity of information. Blockchain solves this problem. The article (Sharma et al, 2018) analyzes the latest advances in distributed ledger technology, existing research gaps and potential solutions for IoT networks on the cloud and fog layer of data processing in smart city systems, intelligent transport, e-health and other industries.

A number of major companies, such as IBM and Samsung, are developing and promoting the IOTA (blockchain-based) blockchain platform to organize and support industrial IoT networks (Ashraf Uddin et al, 2021). The relevance of implementing such platforms in IoT is confirmed by the presence of inconsistent communication models and protocols from various manufacturers of sensor devices, which makes it difficult to create monitoring and control systems based on a single data exchange scheme. To organize industrial IoT networks, the article (Paddy Baker, 2019) proposes a decentralized peer-to-peer telemetry system (ADEPT – Autonomous Decentralized Peer-To-Peer Telemetry), designed to collect sensory data from any end devices. The system works with three protocols: BitTopent for file exchange, Ethereum for smart contracts and TeleHash for messaging. In (Panikkar et al, 2015), blockchain technology makes it possible to implement a transaction processing structure for secure storage and machine-to-machine exchange of sensory data in IoT, and is also used to control and coordinate interacting sensory devices. Sensor devices are registered in a distributed ledger, and data exchange operations are presented in the form of corresponding transactions. Examples of transactions in the blockchain can be such operations as:

(a) registration of equipment in the network,
(b) user registration and authentication,
(c) collecting data from sensors, measuring devices and video surveillance cameras,
(d) monitoring the parameters of technologi

An example of using blockchain technology to ensure security when transferring data between IoT nodes is presented in the article (Ozyilmaz & A. Yurdakul, 2019). A smart contract implemented in the blockchain allows you to check the IP address of the node from which the request was received and determine whether it belongs to the white or black list. Keys for accessing sensor nodes in IoT are generated only after registering the correct IP addresses from the white list. The problem is that only IP addresses from the white list are used to check trusted devices, so it is impossible to recognize an attack in the form of packet flooding from bots, as well as attacks in the form of substitution or distortion of data packets.

The introduction of software-defined networks to create a transport environment in the IoT network and the need to protect against DDoS attacks and
flooding require new approaches to detect and prevent such information security threats. SDN technology is a centralized way to manage and configure network switches. In an SDN architecture, blockchain technology can be used as a mechanism for updating, modifying, and validating flow rule tables for switches and other relay devices in sensor networks (Rodrigues et al., 2017). The combined use of blockchain and SDN technologies allows minimizing the risks and consequences of DDoS attacks (Mohammad Mousavi, 2014; Yan & Yu, 2015).

Distributed denial of service (DDoS) attacks are the most commonly used hacking technique. Despite the growth in protection methods and mitigation solutions, DDoS attacks continue to grow in frequency, volume, and severity. This requires the introduction of new protection mechanisms. In (Bawany et al., 2017), the authors made a comprehensive review of existing solutions for detecting and preventing DDoS attacks using the SDN architecture, and also proposed a platform for proactive DDoS attack detection and mitigation for corporate smart city networks. The article (Babiker Mohamed et al., 2022) proposes the joint use of SDN, blockchain, and network function virtualization technologies to protect IoT networks from information threats. The authors provide an overview of similar security solutions with a statement of the existing problems, including the lack of standardization, low efficiency in detecting malicious traffic and high delays with a large number of attacks.

The SDN architecture presented in (Nupur Giri et al, 2021) makes it possible to detect DDoS attacks in real time with minimal performance requirements for network nodes, which is especially important for low power sensor networks. The following article (Lee & Kim, 2018) describes the procedure for detecting a flood attack in the SDN controller’s data cache. Attacks are detected in the process of data exchange between generating devices and electricity meters at consumers, where the blockchain is used to store user data, and a smart contract to confirm consumer authentication. The work (Velmurugadass et al, 2021) proposes an SDN architecture for a heterogeneous network consisting of mobile communication devices, switches, and SDN controllers with blockchain. Blockchain is used to encrypt data packets using an elliptic curve algorithm and then transfer it to a cloud server. The SDN controller supports the blockchain for data authentication and user signatures.

Materials and Methods

Let us consider a combined approach to ensuring information security in a heterogeneous transport environment when implementing the operations of collecting, processing and storing sensory data. The main idea is to use distributed ledger technology to protect data processing transactions, organize decentralized data storage, SDN architecture with intelligent packet analysis
tools, attack detection and data flow control. The integration of the blockchain with SDN ensures the security and reliability of the transport environment through the mechanism for updating, modifying and validating the tables of flow rules, which allows detecting and preventing information attacks. Distributed registry technology is a way to ensure the reliability, uniqueness and integrity of digital files, as well as increase the resilience of industrial networks to cyberattacks (Mendel et al, 2013; Balistri et al, 2020). The distributed ledger uses a unique data block identifier as a hash function calculation result, which is added to its header and to transactions written to the block. Thus, the ledger is formed from a set of transaction blocks connected to each other by including the hash of the previous block in the current one. The distributed ledger database contains records of the same type. Transactions in our case represent the operations of collecting, processing and exchanging data from sensor devices in the wireless transport environment of the road infrastructure monitoring system (Finogeev A. et al, 2017). Sensor data packages include: a) data on photo and video recording devices (identifier and coordinates of the device, operating time and fixing incidents, device parameters, etc.), b) recorded data on vehicles (number, speed, registration numbers, type etc.); road infrastructure, hitting a pedestrian, etc.); - speeding, crossing a solid line, crossing a stop line, passing a prohibitory signal, not allowing a pedestrian, etc. (Finogeev A. et al., 2021).

To ensure the integrity of sensory data, a double hashing method is proposed. Let’s assume that after a data processing operation, an error is found in the registry: for two consecutive entries in the blockchain, the hash of the first entry does not match the value stored in the second entry. This means that the record is corrupted, which is detected after the hashes are calculated and compared. There remains the problem of determining the modified record. For the solution, the method of double hashing of records is used. Links to successive registry entries are provided by two hashes that are computed for the body of the entry and for its metadata. In this case, each of the parts of the record is used to calculate the hash of the other part. Then the resulting hash is inserted into the header of another entry, similar to the watermark of an electronic document. If the hash is not found in the entry or does not match after calculation, then this means that this entry has been modified.

**SDN Architecture for IoT**

The SDN architecture of the transport environment of the road traffic monitoring system includes four layers of network devices with six levels of data processing and control:
(1) Edge computing layer, including the level of end sensor nodes, relay routers, coordinators of sensor network segments and the data layer in SDN switches. This layer implements the functions of collecting, primary processing, storing equipment telemetry and sensor data, as well as relaying/filtering sensor data packets by SDN switches.

(2) The layer of foggy computing, including the level of zone servers and the level of management in SDN controllers. The layer implements the functions of processing flow tables, organizing and supporting the work of a distributed registry, synthesizing and validating the digital signature of network nodes, smart contracts for analyzing and filtering traffic, an intrusion detection system based on intelligent analysis and clustering of packets, a deep learning module for a fuzzy neural network for clustering packages, logging module. At the zone server level, the functions of processing, aggregating and storing sensor data aggregates are also performed.

(3) Cloud computing layer with data center servers, which implements the main functions of the monitoring system for processing and predictive analysis of aggregated data, centralized storage of data and monitoring results.

(4) Layer of visualization and presentation of monitoring results on mobile and stationary user devices and applications (Figure. 1).

Processing, consolidation and aggregation of data blocks from sensory devices are implemented on fog layer zone servers. Multiple zone servers support distributed storage of sensory data based on distributed hash table (DHT) technology. This technology was chosen for the road transport infrastructure monitoring system, since most of the information blocks are photographs or videos from the scene of an incident or violation. The technology solves the problem of storage scalability, since the performance remains unchanged with an increase in the number of requests to it for receiving data by users and downloading data from an ever-growing number of photoradar systems and video cameras in DHT storage systems.

**Analysis and Filtering of Network Traffic in SDN**

SDN switches filter out invalid traffic by checking port numbers on transport layer segments that are associated with application protocols such as HTTP (ports 80 and 443), FTP (ports 20 and 21), SMTP (ports 25 and 465), etc. Therefore, in the first stage, the controllers form rules for filtering traffic according to the numbers of allowed ports. Valid traffic packets are sent by the controllers for further analysis. Controllers also form rules for filtering network traffic packets according to other criteria: by Time To Life (TTL), by size (Total Size), by IP addresses from unauthorized nodes, by traffic limit
from one node, etc. Rules are synthesized to redistribute network traffic between zone switches, which is necessary to increase the scalability and fault tolerance of the transport environment in the face of possible DDoS attacks to reduce the risks of denial of service on switches. An example of processing input traffic from sensor nodes is provided by the script. In the road monitoring system, nodes such as photoradar systems, CCTV cameras, lidars and weather stations transmit four types of traffic: $T_{video}$ real-time video stream traffic, $T_{image}$ photo FTP traffic, $T_{http}$ data and telemetry data files
HTTP traffic, SNMP command traffic diagnostics and management for touch devices $T_{snmp}$. Rules are formed for each type of traffic according to port numbers before analyzing data packets and validating host addresses.

**Script 1**

```plaintext
Let traffic be Tvideo, Timage, Thttp, Tsnmp
begin // start the process
initialize
i1,i2,i3,.... in // total sensor nodes
i1,i2,i3,.... in→ packet forwarding
if (i1→ Tvideo or Timage or Thttp or Tsnmp) // identifying traffic
    {
        Sh check Pn valid // verify port numbers from the flow table
        forward packet
    else
        discard packet
    }
end if // end of traffic validation
repeat step 4 upto in
Sh monitor fe
if (fe>emax)
    {
        migrate packets // packets are shifted to nearby switch
    else
        continue processing
    }
end if
end // finish the process
```

The traffic type and port numbers are checked by the ingress switch according to the packet filtering rules in the flow table. Traffic with an invalid port number is filtered, and the remaining packets are redistributed among the zone switches for balancing.

**Digital Signature Synthesis and Network Node Authentication**

At the next step, the tasks of synthesizing digital signatures of network nodes and their validation in SDN controllers are solved to synthesize rules for filtering packets from invalid devices. Invalid nodes include unauthorized, fake, or compromised sensor nodes or user devices. They are added to the black list and rules are generated to filter traffic based on the IP addresses of these nodes. The procedure is performed before parsing data packets from valid devices.

To authorize network nodes in the control plane of SDN controllers, a module operates that performs the algorithm for synthesizing a linear homomorphic signature (LHS) of a node (Lin et al., 2020; Chen et al, 2016).
The identity of the authorized sensor node (its unique signature) is synthesized by combining two hash functions:

(a) $H_1(Id,(X,Y))$, where the input is the $Id$ of a sensor or mobile device, its latitude and longitude coordinates $(X,Y)$,

(b) $H_2(T)$, where $T$ is a point on an elliptic curve in a finite field with coordinates $(x,y)$:

$$\{(x,y) \in (\mathbb{R}p)^2\mid y^2 = x^3 + ax + b(mod\ p), 4a3 + 27b2 \neq 0(mod\ p)\} \cup \{0\},$$  

(1)

where $\mathbb{R}p$ - final field of integers $a, b$ modulo $p$, 0 - point at infinity.

The elliptic curve point is included to increase the security of the node, to complicate the signature decryption procedure, which is based on the discrete logarithm problem in a group of curve points.

The generated signature can be represented as a combined hash $S$:

$$S = (H_1(Id, (X,Y)), H_2(T(x,y)))$$  

(2)

To calculate the first part of the digital signature $H_1(Id,(X,Y))$, the SHA-256 (Secure Hash Algorithm) algorithm is used, which is used in the blockchain as a bitcoin hashing algorithm. To synthesize the second part of the signature $H(T(x,y))$, the algorithm with a public key ECDSA (Elliptic Curve Digital Signature Algorithm) defined in a group of points on an elliptic curve.

Signature hash generation is performed iteratively as follows:

1. Choose a random integer $m \in \{1, \ldots, n-1\}$, where $n$ is the order of the group,
2. Determine a point on the curve $T = mP$, where $P$ — subgroup base point,
3. Calculate the parameter $y = xP \mod n$, where $xP$ - $x$ coordinate point $P$,
4. If $y = 0$, then choose another number $m$ and go to step 2,
5. Calculate $S = m^{-1} (H_2+x \ H_1) \mod n$,

If $S = 0$, then choose another number $m$ and go to step 2.

The $S$ signature is verified by the blockchain and allows certified nodes to make transactions to collect and store sensor data from trusted sources, and authorized users to access monitoring results.

The network node validation algorithm is implemented as a smart contract with executable code and private states in the Ethereum blockchain (Pedro Franco, 2014). The choice of the Ethereum blockchain is due to its higher performance compared to other systems, which is important for the speed of packet routing. Authentication of data sources and remote access devices is
necessary to detect possible attack sources and prevent traffic from them to zone servers. Packets from unauthorized nodes are considered malicious and are filtered, and their characteristics are transferred to the clustering subsystem for initial training of the neural network to recognize similar packets. Identified addresses of invalid hosts are added to the blacklist, and information about their discovery is recorded in the security event log. Logging is a security measure and a procedure for preparing data for auditing the operation of SDN controllers. In the general case, the controller fills in and stores lists of white and black IP addresses, sets of characteristics of malicious data packets, and a security event log.

**Analysis and Clustering of Data Packets Based on a Fuzzy Neural Network**

The next step is to analyze network packets from authorized nodes related to valid traffic in order to identify atypical packets with possible malicious content. The architecture of the subsystem for analysis and detection of atypical data packets includes a parser, an analyzer, a clustering module with a fuzzy neural network, and a logging module (Figure 2).

Packet parsing, analyses and clustering modules are needed to detect sensor data packets whose characteristics differ from those normally transmitted from those authorized by the node. The fact is that a decentralized sensor network is subject not only to attacks from unauthorized nodes, but also to attacks by means of substitution or modification of data packets. Such packages may contain malicious content. Therefore, it is necessary to analyze
the characteristics of all data packets from trusted network nodes. The procedure is implemented in the SDN controller and allows you to detect atypical behavior of trusted sensor nodes. Packets are extracted by the parser and passed to the parser. The parsing module extracts the essential characteristics of the packet from the PDU headers. Such characteristics can be source and destination IP addresses, port numbers, header length, packet and header size, lifetime, type of service, etc. Characteristics are used to cluster packets in the feature space in order to determine the degree of similarity with previously detected atypical data blocks. Subsequently, the SDN controller generates an appropriate filtering rule for the set of characteristics of the identified atypical packet. Clustering helps detect atypical packets from real and false sensor nodes. A false node can send packets with the IP address of a real node, but the set of all analyzed characteristics in the complex is too complicated for their simultaneous modification. Therefore, the clustering of a packet in the space of its characteristics (features) makes it possible to identify the probable compromise of the packet and the node with the IP address. Thus, the SDN controller receives evidence of the attack by changing data packets. The revealed facts of the attack are stored in the security log. Packet feature sets define points in feature space that are grouped by degree of proximity or similarity. Characteristic sets of atypical packets also form clusters with centroids, relative to which the degree of proximity of probable compromised data blocks is determined. For such sets of characteristics and for the IP addresses of the nodes from which they come, a flow table rule for SDN switches is synthesized. Entries in the security logs about the detected facts of the attack are stored in the controllers and are available to network administrators.

Packet clustering is implemented by a combined method based on fuzzy logic and a neural network. A similar approach is used in ANFIS (Adaptive Network-based Fuzzy Inference System) (Jang, 1993). This combination combines the advantages of fuzzy logic and neural networks. To train the neural network at the initial stage, sets of characteristics from unauthorized nodes are used, and later on, previously identified sets for correct and atypical packets. The parameters of the membership function of packets to clusters are adjusted using the algorithm for training neural networks, and the conclusion about membership and degree of similarity with the centroids of clusters is formed using the fuzzy logic apparatus.

The clustering process takes into account nine characteristics of data blocks: source IP address (IP_src), destination IP address (IP_Dst), header length (Head_Lng), total packet length (Total_Lng), fragment identifier (Frag_Id), packet time to live (TTL), service type (Srv_type), which are extracted from the IP header of the network layer packet, as well as the sender protocol port number (Port_Srv) and the destination protocol port number (Port_Dst), which are extracted from the TCP or UDP transport layer segment.
The fuzzy clustering method is based on the fuzzy c-means algorithm (Khang et al., 2020; Bezdek et al., 1984) and includes the following steps:

1. The number of clusters of packages $M$ is set, which is further corrected in the learning process, the degree of fuzziness of the objective function is selected $m > 1$.
2. The input feature sets of the package represent feature vectors $X_j$ ($j = 1, \ldots, N$). The vector defines a point in space that can refer to clusters with centroids $C(k)$ ($k = 1, \ldots, M$) with a probability membership function $\mu_{X_j}^{(k)}$, where $0 < \mu_{X_j}^{(k)} < 1$, $\sum_{k=1}^{M} \mu_{X_j}^{(k)} = 1$, which acts as the degree of proximity to the centroid and is determined by the distance $D_{X_j}^{(k)}$.
3. Points are randomly distributed over clusters, the distribution of points is determined by the matrix of degrees of proximity to centroids in the feature space with 9 coordinates, which are the characteristics of the packets $(x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6}, x_{i7}, x_{i8}, x_{i9})$.
4. The coordinates of the centroids of the clusters $C^k$ ($k = 1, \ldots, M$) are calculated by calculating the average proximity of the cluster points:

$$C_k = \frac{\sum_{k=1}^{M} \left( \mu_{X_j}^{(k)} X_j \right)}{\sum_{k=1}^{M} \left( \mu_{X_j}^{(k)} \right)}.$$  (3)

5. Distances between points and centroids of clusters are determined:

$$D_{X_j}^{(k)} = \sqrt{\left\| X_j - C(k) \right\|^2}.$$  (4)

6. The degrees of belonging of points to clusters are recalculated and the distribution matrix of points is updated:

$$\mu_{X_j}^{(k)} = \frac{1}{\sum_{k=1}^{M} \left( \frac{D_{X_j}^{(k)}}{D_{X_j}^{(k)}} \right)^{2/m - 1}}.$$  (5)

where $m > 1$ – clustering fuzziness coefficient.
7. To stop the iterative process, set the parameter $\varepsilon > 0$. If condition: $\left| \left\{ \mu_{X_j}^{(k)} - \mu_{X_j}^{(k-1)} \right\} \right| < \varepsilon$ is not executed, then go to item 5.

The clustering algorithm makes it possible to determine the probabilistic belonging of a data packet to clusters of correct and atypical packets. The probability degree of belonging to clusters of atypical packages is distributed over 3 intervals: a) 0–33%), b) 34–66%), c) 67–100%). The decision on the
synthesis of filtering rules is made when the packet enters the 3rd interval. Such a packet is considered atypical, the source is identified as a compromised host, and its address is added to the exception rule of the flow table. If, according to the degree of membership, the packet falls into 1 interval, then it is considered normal. A rule is created to relay packets with similar sets of characteristics, and the source address is added to the white list. If a packet falls into the second interval, it means that its degree of proximity to clusters of normal and atypical packets is questionable. The package and its source cannot be considered normal and atypical, so this package is considered to belong to the new cluster. The point corresponding to the feature vector of the package becomes the centroid of this cluster. The number of clusters is increased by one and the clustering problem is solved again with the redistribution of feature vectors.

The procedure for training the clustering algorithm and detecting atypical packets is also implemented using a fuzzy neural network. The network represents a five-layer structure without feedbacks with weight coefficients and activation functions. The Takagi-Sugeno-Kanga (TSK) adaptive type model (Olej 2005; Chang and Liu 2008) was chosen as the basis. The output signal is determined by the aggregation function for M rules and N variables (in our case, there are N = 9 packet characteristics at the network input):

\[
y(x) = \frac{\sum_{k=1}^{M} (w_k \ast y_k(x))}{\sum_{k=1}^{M} (w_k)} \tag{6}
\]

where \( y_k(x) = z_{k0} \sum_{j=1}^{N} (z_{kj} x_j) \) is the \( i \)-th polynomial component of the approximation, the weights \( w_i \) represent the degree of fulfillment of the conditions of the rule \( w_k = \mu_A^{(i)}(x_j) \).

The membership or fuzzification function \( \mu_A^{(i)} \) for the variable \( x_j \) is represented by the Gaussian function:

\[
w_k = \mu_A^{(k)}(x_j) = \prod_{j=1}^{N} \left[ \frac{1}{1 + \left( \frac{(x_j-c_j^{(k)})}{\sigma_j^{(k)}} \right)^{2b_j^{(k)}}} \right], \tag{7}
\]

where \( k \) is the number of membership functions \( (k = 1 \ldots M) \), \( j \) is the number of variables \( (N = 9) \), \( c_j^{(k)}, \sigma_j^{(k)}, b_j^{(k)} \) are function parameters Gauss, defining its center, width and shape of the \( k \)-th membership function of the \( j \)-th variable.

Rules for inferring output variables \( Y = (y_1, y_2, \ldots, y_M) \) for the set of variables \( X = (x_1, x_2, \ldots, x_9) \), taking on the set of values \( A_j^{(k)} \) represents a matrix of values of membership functions of size 9×M:
R1: if $x_1^{(1)} \in A_1^{(1)}$ and $x_2^{(1)} \in A_2^{(1)}$ and, $\ldots$, and $x_9^{(1)} \in A_9^{(1)}$, then $y_1(x) = z_{10} \sum_{j=1}^{9} (z_{1j} x_j)$,

\begin{equation}
R_M: \text{if } x_1^{(M)} \in A_1^{(M)} \text{ and } x_2^{(M)} \in A_2^{(M)} \text{ and, } \ldots, \text{ and } x_9^{(M)} \in A_9^{(M)}, \text{ then } y_M(x) = z_{M0} \sum_{j=1}^{9} (z_{Mj} x_j).
\end{equation}

To reduce the computational complexity within the framework of the work, we assume that the number of rules coincides with the number of membership functions, although they may differ. The fuzzy neural network has 5 layers (Figure 3).

In the first layer, fuzzification is carried out according to formula 3 for each variable $x_j$. In this case, for each rule $R_j$ the values of the membership function are determined $\mu_A^{(k)}(x_i)$:

\begin{equation}
\mu_A^{(k)}(x_i) = \frac{1}{1 + \left(\frac{x_i - c_i^{(k)}}{\sigma_i^{(k)}}\right)^2},
\end{equation}

In the second layer, the coefficients $w_k = \mu_A^{(l)}(x)$ are determined by aggregating the values of the variables $x_i$. The $w_i$ parameters are passed to the third layer,
where they are multiplied by the $y_i(x)$ values, and also to the fourth layer to calculate the sum of the weights.

In the third layer, the values $y_i(x) = z_{k0} \sum_{j=1}^{N} (z_{kj} * x_j)$, are calculated and multiplied by the weight coefficients $w_k$. The linear parameters $z_{kj}$ are functions of the consequences of the rules, and $z_{k0}$ is considered as the center of the membership function.

The fourth layer is represented by two neurons: $f_1$ and $f_2$ that aggregate the results:

$$f_1 = \sum_{k=1}^{M} w_k y_k(x) = \sum_{k=1}^{M} \left[ \left( \prod_{j=1}^{N} \mu_{A}^{(k)}(x_j) \right) c_k \right],$$

$$f_2 = \sum_{k=1}^{M} w_k = \sum_{k=1}^{M} \left[ \prod_{j=1}^{N} \mu_{A}^{(k)}(x_j) \right]$$

The fifth normalizing layer is represented by one neuron, where the weights are normalized and the output function is calculated:

$$y(x) = \frac{f_1}{f_2} = \frac{\sum_{k=1}^{M} w_k \times y_k(x)}{\sum_{k=1}^{M} w_k} = \frac{\sum_{k=1}^{M} \left[ \left( \prod_{j=1}^{N} \mu_{A}^{(k)}(x_j) \right) \times c_k \right]}{\sum_{k=1}^{M} \left[ \prod_{j=1}^{N} \mu_{A}^{(k)}(x_j) \right]}.$$  \hspace{1cm} (12)

The TSK neural network contains the first and third parametric layers, in which the parameter values are selected at the training stage. The parameters of the first layer $c_j^{(k)}$, $\sigma_j^{(k)}$, $b_j^{(k)}$ are considered to be nonlinear, and the parameters of the third layer $z_{kj}$ are considered to be linear. The training is done in two steps. At the first step, the parameters of the membership functions of the third layer are selected by fixing the individual values of the parameters and solving the system of linear equations:

$$y(x) = \sum_{k=1}^{M} w_k (z_{k0} + \sum_{j=1}^{N} (z_{kj}x_j)).$$ \hspace{1cm} (13)

The output variables are replaced by reference values $d_P$ ($P$ is the number of training samples). The system of equations can be written in matrix form: $D_p = W*Z$. The solution of the system of equations is found by means of the pseudo-inverse matrix $W^+$: $Z=W^+D_p$. Further, after fixing the values of the linear parameters $z_{kj}$, the vector $Y$ of the actual output variables is calculated and the error vector $E = Y - D_p$ is determined.

In the second step, the errors are sent back to the first layer, where the parameters of the gradient vector of the objective membership function are calculated with respect to the parameters $c_j^{(k)}$, $\sigma_j^{(k)}$, $b_j^{(k)}$. Then, the membership function parameters are adjusted by the fast descent method using the gradient method:
\[ c_j^{(k)}(n + 1) = c_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial c_j^{(k)}}, \]  
(14)

\[ \sigma_j^{(k)}(n + 1) = \sigma_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial c_j^{(k)}}, \]  
(15)

\[ b_j^{(k)}(n + 1) = b_j^{(k)}(n) - \eta \frac{\partial E(n)}{\partial b_j^{(k)}}, \]  
(16)

where \( n \) is the iteration number, \( \eta \) is the learning rate parameter.

After the refinement of the nonlinear parameters, the process of adaptation of the linear and nonlinear parameters is started again. The iterative process is repeated until all process parameters are stabilized.

The advantage of using a fuzzy neural network for training and clustering is the high processing speed and taking into account nine characteristics of packets to detect information attacks by replacing them. The approach allows detecting atypical packets in the SDN controller after authentication of sensor and mobile nodes.

The result of clustering is the synthesis of new packet processing rules and the inclusion of their source addresses in white or black lists. SDN switches further process packets according to the rules of the flow table, filtering atypical packets and relaying normal packets from sensor and mobile nodes to zone servers.

An example of a fragment of a smart contract demonstrating the work of the parser and analyzer.

Smart Contract Process Followed in Controllers

begin // start the process
i1,i2,i3,........,in→ Controller //Packets from sensor node’s is submitted into controller
if (PacketParser → Flow_Mod, Packet_In, Status_Reply, Features_Reply) // message fields between SDN switch and controller
{  
PacketParser = 1
Regular packet
else
Irregular packet // Begin controller processing
}
end if // end of Packet ParserPacket features extract // Packet feature extraction
if (Signature = True) // Node signature authentication
{  
Authorized sensor node // Node permitted into the system with signature validation
Goto packet classification step
}
else
    Unauthorized Node // Invalid signature and node is not permitted
end if

packet classification
features extraction (IP_src, IP_Dst, Head_Lng, Total_Lng, Frag_Id, TTL, Srv_type, Port_Srv, Port_Dst)
FL → IP_src, IP_Dst, Head_Lng, Total_Lng, Frag_Id, TTL, Srv_type, Port_Srv, Port_Dst
→ FO // Features processed in fuzzy logic
if (FO > 0.66 & FO < 1) // Decision making in fuzzy logic
    { 
        Legitimate Packet Packets
        Goto blockchain step
    }
else if (FO < 0.34)
    { 
        Malicious packets
        Goto filtration step
    }
else if (FO > 0.33 & FO < 0.67)
    { 
        Probably malicious packets
        Goto new cluster centroid step
    }
end if
end if
end if // end of decision making

evidence stored in controller
{
    records r1,r2,r3,......
    for each r_i
        { 
            node = node id // node identification
            IP_src, = xxx.xxx.xxx.xxx
            IP_Dst = yyy.yyy.yyy.yyytime = hh:mm:ss // event fix
            timelocation = X,Y position // node latitude and longitude
            action = node action
        }
    end for
    r1,r2,r3,......→blockchain // records stored in the blockchain
    blockchain →Tr1,Tr2,Tr3....... // Transactions in blockchain
} // finish the process

The characteristic sets of normal and atypical packets, as well as the addresses of compromised nodes, are stored in the SDN controller. Entries in the security event log include host ID, IP address, attack detection time, event fix time, host coordinates, transaction type, and other characteristics.
**Results of Testing SDN Architecture**

Modeling of the SDN network was performed in the Network Simulator version 3 (NS3) [(ns-3.35, 2021); (Lavacca et al., 2020)]. To assess the efficiency of the clustering subsystem, five unauthorized nodes were created that generated atypical packets in the general stream once per second on average. In the OpenFlow network model, the switches worked with 40 flows. Two controllers worked with the switches, which analyzed the characteristics of the packets. The result of the simulation is an estimate of the performance of the architecture, such as transmission delay, response time, throughput and accuracy of recognition of atypical packets.

As you know, transmission delay is an indicator that affects the quality of service in the network. In the study, the growth of the transmission delay was estimated depending on the increase in the number of sensor nodes and the number of processed packets (Figure 4).

The graphs show that the amount of latency gradually increases as the number of devices increases, with changes of only a few milliseconds after a packet is transmitted from the end node. However, with an increase in the number of nodes, the changes will already be quite significant, since a linear dependence is observed. A weaker dependence of the delay is observed with an increase in the number of packets arriving at the input of the switches from each node.

Response time is the time it takes for network nodes to receive a response to a request. The metric is determined on the basis of requests received from end nodes to the gateway, which are then transmitted to SDN switches, where they are relayed or filtered according to the rules of the flow tables after validating the authenticity of nodes and analyzing packets in SDN controllers. The response time includes the running time of the node address validation algorithm and the time for packet clustering. Comparison of the response time in the proposed SDN architecture with the response time in the traditional architecture without the analysis and clustering subsystem showed a slight increase in latency by an average of 10.5% (Figure 5).

![Figure 4. Diagrams of the dependence of the delay on the number of sensor nodes and the number of packets.](image_url)
Throughput is shown as the number of bytes of data packets relayed (without filtered packets) from end sensor nodes through gateways and SDN switches to fog layer servers in a given time. On Figure 6 shows diagrams of throughput change depending on the number of requests to sensor nodes when transmitting packets in a network with a traditional SDN architecture and in a network with a subsystem for clustering, detecting and filtering atypical packets. The decrease in throughput (up to 16% on average) is due to the work of the modules for the synthesis of filtering rules for invalid traffic, node address authentication, neural network training, packet analysis and clustering. The decrease in performance is compensated by the increase in information security in the proposed architecture.

Figure 5. Comparison of the response time of a traditional SDN network and an SDN network with an HNS and an LHS algorithm.

Figure 6. Comparison of throughput in SDN network with traditional architecture and in SDN network with HNS and LHS algorithm.
Table 1. Atypical packet detection accuracy.

| Packets arriving for processing (packet/sec) | Total number of packages | Number of packages resulting from clustering |
|---------------------------------------------|--------------------------|---------------------------------------------|
|                                             | Normal packages | Atypical packages | Normal packages | Atypical packages | Recognition accuracy (%) |
| 20                                          | 400           | 75              | 399             | 76              | 98,68%                     |
| 40                                          | 800           | 150             | 797             | 153             | 98,03%                     |
| 60                                          | 1200          | 225             | 1195            | 230             | 97,82%                     |
| 80                                          | 1600          | 300             | 1590            | 310             | 96,77%                     |
| 100                                         | 2000          | 375             | 1980            | 395             | 94,94%                     |

Increasing information security is achieved through the synthesis of new rules for filtering invalid traffic, packets from unauthorized nodes and atypical packets in SDN switches. Filtering improves the quality of service for network devices, provides a higher network payload, and dramatically reduces the likelihood of DDoS attacks, flood attacks, and attacks from unauthorized hosts. To assess the degree of information security, a metric is proposed for the accuracy of recognition of atypical packets in relation to the total number of packets arriving at the input of the switches. To assess the accuracy of detection, 5 nodes without a genuine signature were added to the network, which generated conditional atypical packets with random characteristics that differ from those of normal packets. Table 1 shows the accuracy of detecting atypical packets depending on the speed of their arrival at the input of the switches. It can be seen that the accuracy of packet detection is quite high, but decreases as the rate of packet arrival increases. In our opinion, this is due to the insufficient speed of synthesis of new rules for packets of the second group, which at the first stage of recognition cannot be accurately attributed to existing clusters and they require time to form a new cluster, recalculate membership functions, and synthesize a new rule. With a large number of incoming packets, the smart contract does not have time to implement the second phase of their processing, and the probability of their retransmission increases.

Discussion

The development and implementation of IoT, distributed registry (blockchain) and software-defined networks has led to a number of studies in the direction of integrating these technologies (Sohaib et al., 2022; Islam et al., 2021; Alam et al., 2021; Khan et al., 2019; Sharma et al., 2018; Ashraf Uddin et al., 2021; Ozyilmaz & Yurdakul, 2019; Babiker Mohamed et al., 2022; Giri et al., 2021; Lee & Kim, 2028; Velmurugadass et al., 2021; Rathore et al., 2019; Mkrtchian et al., 2021, Yazdinejad et al., 2019; Qiu et al., 2018; Aliyu et al., 2021). The presented research results do not pretend to be a novel problem statement. The article presents an SDN architecture for intelligent network traffic management in a wireless IoT transport environment with built-in
cyber threat protection. The architecture is being developed for a system of road transport monitoring and monitoring of technological processes of energy distribution with network nodes that are dispersed over a large area.

A similar SDN architecture is discussed in the article (Sharma et al, 2018), where, unlike our project, the authors propose a three-layer architecture of the transport environment, including the SDN switch layer, the fog layer with SDN controllers, and the cloud layer for blockchain implementation and secure access to the computing infrastructure. This is a different approach, since in our research, DHT-based distributed storage technology and blockchain are implemented on fog layer zone servers. The tasks of source authentication, intelligent analysis and recognition of malicious packets can be solved at three levels: the level of sensor nodes of the edge layer (sensors and measuring devices, switches), the level of nodes of the foggy layer of data processing (controllers), the level of the cloud layer of data processing (servers of centers data processing). However, due to the limited computing resources of sensor nodes, the use of blockchain technologies, intellectual analysis and neural networks to process traffic and authenticate nodes through edge computing is very problematic. Therefore, in the project, an intelligent intrusion detection system is implemented on zone servers and in SDN fog level controllers. This approach allows you to support the blockchain and distributed storage of data blocks and transactions on specialized zone servers that act as miners and SDN controllers to minimize the risks of attacks on data center servers.

The integration of zone servers and SDN controllers on the fog layer allows you to redistribute the computing load between them to solve scaling problems, as well as separate security processes and big data processing processes on the cloud layer. In the second case, the technology allows eliminating the computational load on cloud servers, which is associated with solving complex problems of calculating hashes, finding their collisions and discrete logarithm in the blockchain. Thus, the servers of the cloud layer solve only the tasks of processing large sensory data received from a huge number of IoT devices (photoradar systems, video surveillance cameras, weather stations, other measuring, diagnostic and control equipment), which requires large computing resources. The servers perform the procedures of statistical, intellectual and predictive analysis of the characteristics of incidents, participants and factors of influence, forecasting the risks of incidents depending on the influence of factors on distributed objects of the road transport infrastructure.

An example of the synthesis of the transport environment for road infrastructure facilities is the research in (Aliyu et al, 2021). Here, the issues of synthesis of a secure communication system for automotive controllers and control units that control the operation of internal components are considered. The authors propose to use SDN network technology with blockchain to solve the problem of using confidential data of manufacturers and owners of
vehicles, as well as to detect unauthorized access to the car control system. The authors of the article (Sohaib et al., 2022) explore the benefits of blockchain and SDN integration. For peer-to-peer IoT networks, they offer a new routing protocol based on node clustering to reduce the power consumption of sensor nodes and ensure security. To synthesize a secure transport environment in a sensor network, we also use our own routing protocols [(Kamaev et al., 2017); (Alexey et al., 2015)].

An interesting related work (Islam et al., 2021), in which the authors propose a distributed and decentralized blockchain-based software-defined network architecture for the IoT network in smart cities. The network, in their opinion, solves the problems of scalability, flexibility, complexity and is designed to monitor, collect data, manage, and protect against cyber threats. In contrast to this study, we are developing an SDN architecture for a scalable environment for a specific application. The system is designed to solve the problems of monitoring critical events in the road transport infrastructure and in energy transportation and distribution systems.

Security issues associated with the creation of integrated IoT and SDN networks are also of interest to researchers. Despite numerous advantages, the heterogeneous IoT transport environment is a target for information attacks (Javeed et al., 2021). The authors of the article show how intelligent technologies in software-defined networks are becoming an effective tool for ensuring security and combating cyber threats. SDN architecture allows the use of hybrid threat detection algorithms in IoT networks. The SDN architecture, as well as in our project, is a computing platform for implementing complex mechanisms for detecting attacks and threats that cannot be implemented on end IoT devices with limited resources. The authors propose to use a two-layer Cuda-Deep Neural Network Long short-term memory with the addition of a Cuda-Deep Neural Network Gated Recurrent Unit layer to detect threats. In our project, we also use deep learning methods to solve image recognition problems (Osipov et al., 2022) and data packet clustering problems, but for a five-layer fuzzy neural network during clustering and recognition of atypical packets. The elements of fuzzy logic in our project allow us to determine the probabilistic belonging of network packets to the found clusters, and in case of obtaining ambiguous recognition results, retrain the network with the addition of new clusters and redistribution of points in the feature space. In contrast to the approach proposed by the authors of the article, our technology allows, in addition to detecting threats, to solve issues of minimizing uncertainty in recognition.

The article (Hu et al., 2021) deals with the vulnerability of trust relationships between SDN control and data planes when integrating with IoT nodes. To solve the problem, Gelenbe et al., (2018) propose an integrated system that combines edge computing and SDN for security. Blockchain is seen as a third-party edge-computing service to validate data flows for rewards. In our
opinion, this approach cannot be applied to ensure the safety of urban life support systems. Firstly, it increases the cost of services provided, for example, the cost of energy for the population, secondly, it delegates responsibility for security problems to third parties, and thirdly, it complicates and slows down the process of detecting cyber threats. Work (Ren et al, 2021) is related to the problems of access control and permissions from IoT applications to the interfaces of many heterogeneous SDN controllers. To solve the problem of performance and scalability to ensure secure access, the authors propose to use blockchain and attribute encryption as a trusted and decentralized authorization mechanism. IoP applications are authorized using encrypted access tokens, which are treated as blockchain currency. This approach differs from that proposed in our article, since we use blockchain technology to synthesize and validate digital signatures of IoT nodes and mobile user devices.

To reduce the computational load on controllers during the analytical processing of data packets, a three-stage traffic analysis technology is implemented. The first stage performs fast filtering of invalid traffic by port numbers. At the second stage, the authenticity of data sources and access devices is confirmed and traffic from invalid nodes from the “black” list is filtered. At the third stage, where complex neural network training and intellectual analysis procedures are performed for clustering and recognizing atypical packets, a limited number of packets that have passed two stages are allowed. This approach is necessary to improve performance and partially solve the problems of scalability of the proposed architecture.

However, there are other scalability issues that arise in the process of integrating IoT networks with blockchain technologies and SDN networks. First of all, they are related to the bandwidth limitations of the transport IoT environment (Novo, 2018). Insufficient scalability of IoT networks is determined by the limited computing and energy resources of sensor nodes (Xu and Helal, 2016; Sarkar et al., 2015; Anisha Gupta et al, 2017). These restrictions do not allow solving the tasks of organizing a distributed registry and ensuring security by intelligent methods directly on sensor nodes. Most sensor networks operating on ZigBee (802.15.4) protocols have low-speed communication channels (up to 256 Kbps). Therefore, the integration of SDN technologies with IoT networks of devices operating within this standard has limitations on the speed of collecting data packets for analysis and relaying them by switches.

To solve this problem in the process of collecting and transmitting data from nodes with low-speed communication channels, on the edge layer of our architecture, coordinators are used in the segments of sensor networks that are connected to WiFi router gateways. Gateways, together with coordinators, act as collectors of sensor data packets from many nearby nodes and transmit them over high-speed mobile communication channels. Basically, this technology is involved in the collection of data from sensors and measuring
equipment. In our project to create a transport IoT environment for a road infrastructure monitoring system, the main sensor nodes are photoradar systems and video surveillance cameras operating on fast protocols within the standards of WiFi, WiGi (802.11) wireless networks and 4G mobile networks with communication channels of a fairly high bandwidth. Therefore, there are practically no special restrictions in this environment associated with the low bandwidth of data transmission channels in such an IoT architecture. To solve problems with the bandwidth of communication channels between switches, SDN controllers and zone servers, they are located in the same room close to each other and connected by a local Ethernet network. Modem pools and WiFi routers are also located here to collect data from remote nodes and transfer it to the control plane to the main SDN controller.

Another issue is the scalability of the Software Defined Network itself. The problem arises when traffic management processes are centralized in the SDN controller, as well as with the addition of new functions for validating network nodes, analyzing network traffic, and clustering data packets. In particular, the problems of scalability of software-defined networking and methods for solving them are considered in (Yeganeh et al, 2013). The authors of the article show that one controller can potentially become the bottleneck in the network operation. As the size of a network grows, more requests are sent to the controller, and at some point, the controller cannot handle all the incoming requests. The way to solve the problem is to use several controllers with the main controller, which acts as a hypervisor to balance traffic and redistribute network packets that arrive for analysis in the intrusion detection system. To create a scalable SDN architecture in our project, we use this method. Also, when developing such an architecture, we expect that SDN controllers and switches in the near future will have sufficient bandwidth and computing power to solve the tasks of intelligent traffic analysis.

**Conclusion**

In the course of the research, a secure architecture of the transport IoT environment for a traffic monitoring system based on SDN, DHT technology, blockchain, data mining using a fuzzy neural network was synthesized.

Based on the analysis of research results in this area, it can be stated that in the course of working on our projects, a number of new results were obtained, which include: a) SDN architecture of the IoT environment with four layers of devices and six levels of data processing and control, b) methods for detecting cyber attacks using a fuzzy neural network and a clustering algorithm for the probabilistic evaluation of malicious packets by nine characteristics and compromised nodes, c) a set of characteristics of data packets for recognizing and detecting attacks and criteria for probabilistic evaluation of the malicious content of the packet, d) a distributed registry system for storing data about...
network nodes with generation and validation of the digital signature of nodes using the double hashing method to improve the efficiency and stability of identification, e) a set of smart contracts within the Ethereum blockchain, used for two-stage detection of incorrect data streams from compromised sensor nodes.

Modeling and evaluating the effectiveness of the proposed approach showed a sufficiently high speed of network traffic processing to detect information attacks. To reduce the computational load during analytical processing of packets, controllers and switches implement a three-stage traffic analysis technology. At the first stage, invalid traffic is filtered by port numbers. At the second stage, the authenticity of data sources and access devices is confirmed and traffic from invalid nodes from the “black” list is filtered. At the third stage, where the machine learning and intellectual analysis procedures are performed, only filtered packets are transferred directly to the controller. Three-stage processing improves the performance and scalability of the architecture.

The article is an integrative continuation of previously completed research published in (Alexey Finogeev & Anton Finogeev, 2017; Alexey Finogeev et al, 2019; Finogeev A. et al, 2017; Anton Finogeev et al., 2020; Finogeev et al., 2021; Mkrttchian et al, 2021, Kamaev et al, 2017; Finogeev Alexey et al, 2015; Osipov et al, 2022) as part of a new project to create a secure and reliable wireless IoT network for collecting, consolidating and processing sensor data in the process of monitoring critical events on distributed energy consumption systems in the urban environment and in road transport infrastructure. In particular, the environment is created for the processing and storage of large sensory data on photoradar complexes for photo and video recording of traffic accidents, video surveillance cameras and other sensor devices, as well as for new generation dispatching SCADA systems that control the processes of transportation and distribution of energy carriers. It is also planned to introduce the proposed architecture in the network environment of the production line monitoring system.

Acknowledgment

The study was supported by the grant from the Russian Science Foundation, RSF 20-71-10087. The research results presented in sections 3.2 and 3.3 were obtained within the grant of the Russian Science Foundation (RSF) and the Volgograd Region (project № 22-11-20024). The research results presented in Section 4 were obtained within the grant of the Russian Science Foundation (RSF) and the Penza Region (project № 22-21-20100).

Disclosure statement

No potential conflict of interest was reported by the author(s).
Funding

The work was supported by the Russian Science Foundation [20-71-10087]; Russian Science Foundation [22-11-20024]; Russian Science Foundation [22-21-20100].

ORCID

Alexey Finogeev http://orcid.org/0000-0002-4777-3364
Michael Deev http://orcid.org/0000-0002-0371-5517
Danila Parygin http://orcid.org/0000-0001-8834-5748
Anton Finogeev http://orcid.org/0000-0001-8280-1474

References

Alam, I., K. Sharif, F. Li, Z. Latif, M. M. Karim, S. Biswas, B. Nour, and Y. Wang. 2021. A survey of network virtualization techniques for internet of things using SDN and NFV. ACM Computing Surveys 53:1.

Alexey, F., F. Ludmila, F. Anton, N. Irina, F. Egor, T. Q. Vinh, and K. Valery. 2015. Methods and tools for secure sensor data transmission and data mining in energy SCADA system. Creativity in Intelligent Technologies and Data Science Series «communications in Computer and Information Science» 535:474–87. Part XI. doi:10.1007/978-3-319-23766-4_38.

Aliyu, I., M. C. Feliciano, S. Van Engelenburg, D. O. Kim, and C. G. Lim. 2021. A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system. IEEE Access 9:102593–608, 10.1109/ACCESS.2021.3094365.

Ashraf Uddin, M., A. Stranieri, I. Gondal, and V. Balasubramanian. 2021. A survey on the adoption of blockchain in IoT: Challenges and solutions. Blockchain: Research and Applications 2:100006.

Babiker Mohamed, M., O. Matthew Alofe, M. Ajmal Azad, H. Singh Lallie, K. Fatema, and T. Sharif. 2022. A comprehensive survey on secure software-defined network for the internet of things. Transactions on Emerging Telecommunications Technologies 33 (1):e4391. doi:10.1002/ett.4391.

Baker, P. 2019. Investors pounce on IOTA as Jaguar Land Rover announces crypto integration. Accessed on Sep 20, 2019. https://cryptobriefing.com/iotajaguar-land-rover-crypto/

Balistri, E., F. Casellato, C. Giannelli, and C. Stefanelli. 2020. Blockchain for increased cyber-resiliency of industrial edge environments. IEEE International Conference on Smart Computing (SMARTCOMP) 2020. 1–8. doi:10.1109/SMARTECOMP50058.2020.00021.

Bawany, N. Z., J. A. Shamsi, and K. Salah. 2017. DDoS attack detection and mitigation using SDN: Methods, practices, and solutions. Arabian Journal for Science and Engineering 42:425–41. doi:10.1007/s13369-017-2414-5.

Bezdek, J., R. Ehrlich, and W. Full. 1984. Fcm—the fuzzy C-means clustering-algorithm. Computers & Geosciences 10:191–203. doi:10.1016/0098-3004(84)90020-7.

Chang, P. C., and C. H. Liu. 2008. A TSK type fuzzy rule based system for stock price prediction. Expert Systems with Applications 34 (1):135–44.

Chen, Y. 2020. A survey on industrial information integration 2016–2019. Journal of Industrial Integration and Management 5(01):33–163.

Chen, W., H. Lei, and K. Qi. 2016. Lattice-based linearly homomorphic signatures in the standard model. Theoretical Computer Science 634. doi:10.1016/j.tcs.2016.04.009.

Finogeev, A., M. Deev, A. Finogeev, and I. Kolesnikoff. 2020. Proactive big data analysis for traffic accident prediction. Proceeding of the 5th International Conference on Innovative
Technologies in Intelligent Systems and Industrial Applications (CITISIA). doi:10.1109/CITISIA50690.2020.9371796.

Finogeev, A., and A. Finogeev. 2017. Information attacks and security in wireless sensor networks of industrial SCADA systems. Journal of Industrial Information Integration 5:6–16. doi:10.1016/j.jiii.2017.02.002.

Finogeev, A., A. Finogeev, L. Fionova, A. Lyapin, and K. Lychagin. 2019. Intelligent monitoring system for smart road environment. Journal of Industrial Information Integration, 15:15–20. 10.1016/j.jiii.2019.05.003

Finogeev, A., A. Finogeev, and S. Shevchenko. 2017. Monitoring of road transport infrastructure for the intelligent environment «smart road». Communications in Computer and Information Science 754:655–68. doi:10.1007/978-3-319-65551-2_47.

Finogeev, A., D. Parygin, S. Shevchenko, A. Finogeev, and D. Ather. 2021. Collection and consolidation of big data for proactive monitoring of critical events at infrastructure facilities in an Urban environment. InCreativity in Intelligent Technologies and Data Science. Communications in Computer and Information Science, A. G. Kravets, M. Shcherbakov, D. Parygin, P. P. Groumpos, eds, vol. 1448; Springer:Cham. doi:10.1007/978-3-030-87034-8_25.

Franco, P. 2014. Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series). Hoboken, New Jersey, U.S: John Wiley & Sons, 288. ISBN 978-1-119-01916-9.

Gelenbe, E., J. Domanska, T. Czăchorski, A. Drosou, and D. Tzovaras. 2018. Security for internet of things: The seriot project, proc. IEEE International Symposium on Networks, Computers and Communications (ISNCC) 1–5.

Giri, N., R. Jaisinghani, R. Kripiani, T. Ramakhyani, and V. Bhatia. 2021. Distributed denial of service (DDoS) mitigation in software defined network using blockchain. 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019 Dec 12–14, SCAD Institute of Technology SCAD Knowledge City Palladam - Pollachi Highway Palladam - 641 664 Tirupur District, Tamil Nadu, INDIA, pp. 673–678. https://www.sci-hub.ru/10.1109/I-SMAC47947.2019.9032690

Gupta, A., R. Christie, and R. M. Prof. 2017. Scalability in internet of things: features, techniques and research challenges. International Journal of Computational Intelligence Research 13 (7):1617–27.

Hu, J., M. J. Reed, N. Thomos, M. F. Al-Naday, and K. Yang. 2021. Securing SDN-controlled IoT networks through edge blockchain. IEEE Internet Things Journal 8 (4):2102–15. doi:10.1109/JIOT.2020.3017354.

Islam, M., A. Rahman, S. Kabir, M. Razaful, U. Acharjee, M. Nasir, S. Band, Shahab, M. Sookhak, and W. Shaoen. 2021. Blockchain-SDN based energy-aware and distributed secure architecture for iots in smart cities. IEEE Internet of Things Journal 9 (5):3850–64. doi:10.1109/JIOT.2021.3100797.

Jang, J.-S.R. 1993. ANFIS: Adaptive-network-based fuzzy inference system (англ./j.-S.R. Jang//IEEE Transactions on Systems, Man and Cybernetics: Journal 23 (3):665–85.

Javeed, D., T. Gao, and M. T. Khan. 2021. SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. Electronics 10 (8):918. doi:10.3390/electronics10080918.

Kamaev, V. A., A. G. Finogeev, A. A. Finogeev, and D. S. Parygin. 2017. Key management schemes using routing information frames in secure wireless sensor networks. Journal of Physics: Conference Series: Proceedings of the International Conference on Information Technologies in Business and Industry 803:1–7.

Khan, M., F. Algarni, and M. Quasim. 2019. Decentralised Internet of Things. 10.13140/RG.2.2.12659.68649
Khang, T.D., N.D. Vuong, M.-K. Tran, and M. Fowler. 2020. Fuzzy C-means clustering algorithm with multiple fuzzification coefficients. *Algorithms* 13 (7):158. doi:10.3390/a13070158.

Latif, S. A., F. B. Xian Wen, C. Iwendi, L.L.F Wang, S. Muhammad Mohsin, Z. Han, and S. S. Band. 2022. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systemsm. *Computer Communications* 181:274–83.

Lavacca, F.G., P. Salvo, L. Ferranti, A. Sperranza, and L. Costantini. 2020. Performance evaluation of 5G access technologies and SDN transport network on an NS3 simulator. *Computers* 9 (2):43. doi:10.3390/computers9020043.

Lee, C. H., and K.-H. Kim. 2018. Implementation of IoT system using block chain with authentication and data protection. *International Conference on Information Networking (ICOIN)* 1: 936–940. doi:10.1109/ICOIN.2018.8343261.

Lin, C.-J., R. Xue, S.-J. Yang, X. Huang, and L. Shimin. 2020. Linearly homomorphic signatures from lattices. *The Computer Journal* 63:1871–85. doi:10.1093/comjnl/bxaa034.

Mauro Contia, A. D., K. Frankec, and S. Watson. January. 2018. Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78 (2):544–46.

Mendel, F., T. Nad, and M. Schläffer. 2013. Improving local collisions: New attacks on reduced SHA-256//advances in Cryptology – Eurocrypt 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30. Springer Berlin Heidelberg. pp. 262–78. doi:10.1007/978-3-642-38348-916.

Mkrtchian, V., S. Vasin, L. Gamidullaeva, and A. Finogeev. 2021. The impact of blockchain technology on the smart city industry. ACM International Conference Proceeding Series. In IV International Scientific and Practical Conference (DEFIN-2021). Association for Computing Machinery, New York, NY, USA, Article 85, 1–5, 3490940. 10.1145/3487757.3490940

Mohammad Mousavi, S. 2014. “Early detection of DDoS attacks in software defined networks controller”. Ontario: Carleton University Ottawa.

Novo, O. Apr. 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things Journal* 5(2):1184–95.

ns-3.35. 2021. Accessed October 14, 2021. https://www.nsnam.org/releases/ns-3-35/

Olej, V. 2005. Design of the models of neural networks and the Takagi–Sugeno fuzzy inference system for prediction of the gross domestic product development. *WSEAS Transactions on Systems* 4 (4):314–19.

Osipov, A., E. Pleshakova, S. Gataullin, S. Korchagin, M. Ivanov, A. Finogeev, and V. Yadav. 2022. Deep learning method for recognition and classification of images from video recorders in difficult weather conditions. *Sustainability* 14 (4):10.3390/su14042420.

Ozyilmaz, K. R., and A. Yurdakul. 2019. Designing a blockchain-based iot with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks. *IEEE Consumer Electronics Magazine* 8 (2):28–34. doi:10.1109/MCE.2018.2880806.

Panikkar, B., S. Nair, P. Brody, and V. Pureswaran. 2015. ADEPT: An IoT practitioner perspective. Draft Copy for Advance Review, IBM. Accessed November 17, 2022. http://static1.squarespace.com/static/55f73743e4b051fc0b02cf/55f73e5ee4b09b2bfb5b2eca/55f73e72e4b09b2bfb5b3267/1442266738638/IBM-ADEPT-Practitioner-Perspective-Pre-Publication-Draft-7-Jan-2015.pdf

Qiu, C., F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao. 2018. Blockchain-based software-defined industrial internet of things: A dueling deep Q-learning approach. *IEEE Internet Things Journal* 6 (3):4627–39.
Rathore, S., B. W. Kwon, and J. H. Park. 2019. BlockSeciotnet: Blockchain based decentralized security architecture for IoT network. *Journal of Network and Computer Applications* 143:167–77.

Ren, W., Y. Sun, H. Luo, and M. Guizani. 2021. Siledger: A blockchain and ABE-based access control for applications in SDN-Iot networks. *IEEE Transactions on Network and Service Management* 18 (4):4406–19. doi:10.1109/TNSM.2021.3093002.

Rodrigues, B., T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller. 2017. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. *11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2017*, 2017 July 10–13, Zürich, Switzerland: Springer. vol. 1, pp. 16–29. doi:10.1007/978-3-319-60774-0_2.

Sarkar, C., A. U. N. SN, R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini. 2015. DIAT: A scalable distributed architecture for IoT. *IEEE Internet of Things Journal* 2 (3):230–39.

Sharma, P. K., M.-Y. Chen, and J. H. Park. 2018. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* 6:115–24. doi:10.1109/ACCESS.2017.2757955.

Valdovinos, I. A., J. Arturo Pérez-Diaz, K.-K. Raymond Choo, and J. Felipe Botero. 2021. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy challenges and future directions. *Journal of Network and Computer Applications* 187:103093.

Velmurugadass, P., S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan. 2021. Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu 626 126, India*, vol. 37, pp. 2653–2659. doi:10.1016/j.matpr.2020.08.519.

Xu, L. 2020. Industrial information integration - an emerging subject in industrialization and informatization process. *Journal of Industrial Information Integration* 17:100128. doi:10.1016/j.jii.2020.100128.

Xu, Y., and A. Helal. 2016. Scalable cloud–sensor architecture for the internet of things. *IEEE Internet of Things Journal* 3 (3):285–98. doi:10.1109/JIOT.2015.2455555.

Xu, L. D., W. He, and S. Li. 2014. Internet of things in industries: A survey. *IEEE Transactions on Industrial Electronics* 10 (4):2233–43.

Yan, Q., and F. R. Yu. 2015. Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine* 53 (4):52–59. doi:10.1109/MCOM.2015.7081075.

Yazdinejad, A., R. M. Parizi, A. Dehghantahna, and K.K.R Choo, Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks, IEEE Trans. Netw. Sci. Eng. 2019, doi:10.1109/TNSE.2019.2937481.

Yeganeh, S. H., A. Tootoonchian, and Y. Ganjali. 2013. On scalability of software-defined networking. *IEEE Communications Magazine* 51 (2):136–41.

Zaman, S., K. Alhazmi, M. A. Aseeri, M. Raisuddin Ahmed, M. S. K. Risala Tasin Khan, and M. Mahmud. 2021. Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. *Access IEEE* 9:94668–90.

Zhu, L., M. M. Karim, K. Sharif, C. Xu, F. Li, X. Du, and M. Guizani. 2021. SDN controllers. *ACM Computing Surveys* 53:1.