Detection of Attacks in Wireless Networks of IoT

Olexander Belej[a], Nataliia Bokla[a], and Liubov Halkiv[a]

[a] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79013, Ukraine*

Abstract

The article considers the problems of ensuring the fault tolerance and reliability of the system, which are the main characteristics of the wireless Internet of Things. Wireless data networks continue to grow rapidly. However, security in these networks often does not meet the required level. Intrusion detection systems are used to protect against wireless network attacks. Thanks to modern computing capabilities, the task of analyzing the parameters of network traffic for signs of an attack can be solved using data mining. The analysis of network attacks relevant to local wireless networks is carried out. The results of the experiments allow us to conclude about the practical significance of the proposed approach to detecting attacks in local wireless Internet of Things.

Keywords

Internet of things, network traffic, wireless, attack, detection systems.

1. Introduction

Wireless networks have gained immense popularity. Their wide distribution is due to the undeniable advantages over traditional cable networks: ease of deployment, mobility of users in the network coverage area, easy connection of new users. On the other hand, the security of such networks often limits their use. If an attacker needs to have a physical connection to the network during an attack on a wired network, in the case of wireless networks, he can be anywhere in the network coverage area. Also, these networks are subject to attacks that are related to the imperfection of the data transmission protocol in wireless IoT networks. Due to the low level of security, such networks are of limited use in IoT.

Due to the instability and poor protection of wireless networks, various researchers are looking for ways to improve current protocols. In [1], the author proposes to encrypt the entire MAC data block (MPDU), including MAC headers, except for the sequence of checking the FCS frame, which will lead to significant delays in data transmission and low bandwidth of the channel. Another approach is to enter a hash in the control frame of a certain string known only to a particular sender, by transmitting which in the future it can be uniquely identified and processed [2]. However, this method prevents only one type of attack.

In practice, to protect against network attacks, ordinary users and small organizations are usually limited to the use of anti-virus software or special additional security modules [3]. Large businesses are forced to buy expensive wireless intrusion detection systems (WIDS). However, there are currently no generally accepted standards in this area. Often the problem of assigning a fragment of network traffic to some type of attack or normal network activity can be solved by using methods of data mining (DM) [4].

In [5, 6] to solve this problem, the use of neural networks and the method of reference vectors Support Vector Machine (SVM) is proposed. In [7] the approach to the organization of the attack detection system of the neural network based on the two-layer perceptron and the Kohonen network was considered. It should be noted that the above studies concerned the detection of intrusions into traditional wired networks [8].

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: oleksandr.i.belei@lpnu.ua (A.1); lubov.i.halkiv@lpnu.ua (A.2); nataliia.i.bokla@lpnu.ua (A.3)
ORCID: 0000-0003-4150-7425 (A.1); 0000-0001-5166-8674 (A.2); 0000-0002-8919-6622 (A.3)

Despite the significant amount of work on the targeted use of data mining methods to detect attacks specific to local wireless networks, this area of research requires further study and experimentation with different algorithms for detecting attacks in wireless IoT networks. For this reason, this study examines the main types of attacks inherent in wireless networks, some recommended methods of protection against them, and proposes the architecture of an attack detection system based on data mining methods. At the end of the study, the evaluation of the effectiveness of the used algorithms for detecting attacks in wireless IoT networks.

2. Attacks Implemented in the Wireless Networks of IoT

Wireless network attacks are based on the interception of network traffic from an access point or traffic between two connected stations, as well as the introduction of additional data into a wireless session. To better understand the types of wireless attacks that an attacker can carry out against a wireless network, it is important to classify them. Thus, attacks can be directed at different levels of the OSI model: application, transport, network, channel, and physical.

Depending on the purpose of the attack, specific to the family of 802.11 protocols, can be divided into several categories [9]: obtaining unauthorized access to the network; violation of integrity; breach of confidentiality; violation of access; theft of personal data.

Depending on the purpose of the attack on local wireless networks, OSI models can be divided into several categories [10]:

- Obtaining unauthorized access to the network: false access point; MAC spoofing; hacking the network client; hacking of access points.
- Integrity violation: 802.11 frame input; play 802.11 data, delete 802.11 data; play 802.1X EAP; play 802.1X RADIUS.
- Breach of confidentiality: eavesdropping; evil twin; AP phishing; the man in the middle.
- Accessibility violations: radio frequency noise; Queensland DoS; Probe with a request for attacks;
- Associate/authenticate/disconnect/de-authenticate an attack; 802.1X EAP Start, EAP Failure Flood.
- Authentication bypass: pre-shared key; Theft of personal data 802.1X; 802.1X EAP Decrease; 802.1X password hacking; hacking of domain accounts; hacking WPS pin.

These attacks are based on the use of vulnerable wireless networks presented in the WVE database [11]:

- Sending probe requests with a zero-length SSID tag field (WVE-2006-0064).
- EAP denial attacks (WVE-2005-0050).
- RTS / CTS attacks (WVE-2005-0051).
- The capture of WLAN packets of dissociation (WVE-2005-0046).
- The capture of a wireless local area network by network packets (WVE-2005-0045).
- Sending an invalid authentication reason code.
- Sending too long SSID (WVE-2006-0071, WVE-2007-0001).
- Sending the Airjack beacon frame (WVE-2005-0018).
- Sending invalid channel numbers in beacon frames (WVE-2006-0050).

Wireless access testing for WPA2-Enterprise. In this case, the connection means a sequence of packets that begin and end at certain points in time, between which data streams are transmitted from the source IP address to the IP address of the recipient using a specific protocol [12]. Each connection is referred to as normal or as some type of attack from four categories of attacks: denial of service (DoS), unauthorized acquisition of user rights Remote to Local (R2L), an unauthorized increase of user rights to superuser User to Root (U2R) and sounding. The ratio of the number of attacks of different types is shown in Tables 1 and 2.

Table 1.
The ratio of the number of attack signatures for the training base in the wireless network of IoT

Normal		67343	
DoS		R2L	
Class	Quantity	Class	Quantity
neptune	41214	guess_passwd	162
smurf	2646	ftp_write	8
Pod	201	imap	11
teardrop	892	phf	4
land	18	multihop	7
back	956	warezmaster	40
U2R		Probe	
Class	Quantity	Class	Quantity
buffer_overflow	30	portsweep	2931
load-module	9	upsweep	3599
Perl	3	satan	3633
rootkit	10	nmap	1493

Table 2.
The ratio of the number of attack signatures for the test base in the wireless network of IoT

Normal		9711	
DoS		R2L	
Class	Quantity	Class	Quantity
neptune	4657	guess_passwd	1231
smurf	665	ftp_write	3
Pod	41	imap	1
teardrop	12	phf	2
land	7	multihop	18
back	359	warezmaster	944
U2R		Probe	
Class	Quantity	Class	Quantity
buffer_overflow	20	portsweep	157
load-module	2	upsweep	141
Perl	2	satan	735
rootkit	13	nmap	73

Some of these types of attacks are losses due to the use of radiofrequency data technology, and also depend on the human factor and must be addressed through organizational measures. Wireless intrusion detection (WIDS) systems are significantly different from network security systems, except firewalls.

3. Attacks Implemented in the Wireless Networks of IoT

The decision on the security of any network activity in commercial security systems is implemented using closed algorithms, the principle of which is a trade secret. Moreover, the stated number and types of detected attacks differ for different products, although in reality, they belong to the same type of attack, which is explained by the lack of standards in the classification.

The problem of detecting and classifying attacks can be solved using data analysis methods (DM), which allow identifying significant relationships, patterns, and trends in large amounts of data on attacks. The developed system uses algorithms for constructing a classification model based on the reference vector method, the method of k-nearest neighbors, neural networks, and decision trees.

The proposed architecture of the intelligent attack detection system has a modular scheme for the organization of interaction between components with a dedicated subsystem of the sensor and centralized control through the administrator console. The architecture of the attack detection system is presented in Fig. 1.

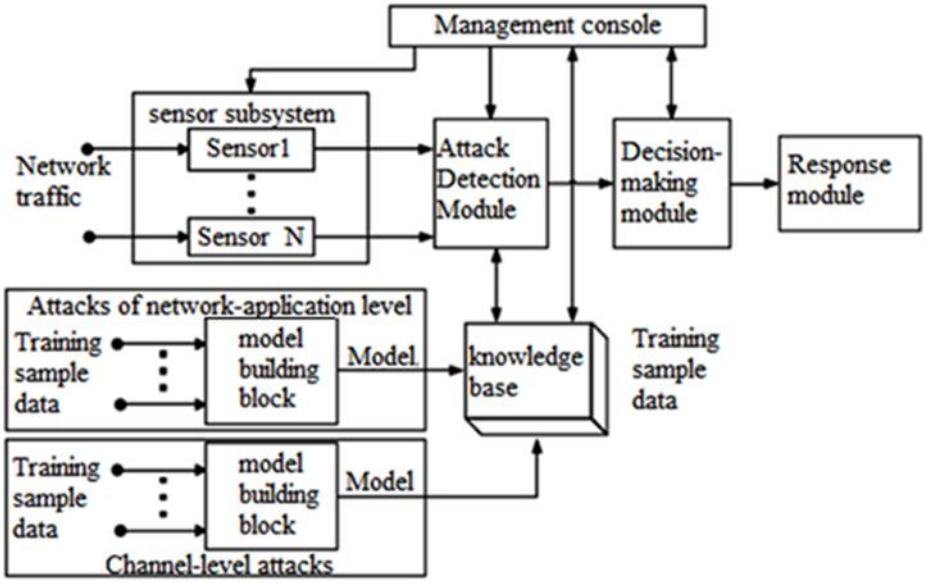

Figure 1: Structure of the attack detection system in the wireless network of IoT

The basis for detecting attacks is the knowledge base, the construction of which at the stage of the initial configuration of the system involves a block of construction of the classification model. The classification model is based on the signatures of the training sample and then used to classify the actual activities of the network.

The attack detection module of the designed attack detection system can be functionally divided into a submodule for detecting network attacks at the transport and application level and a submodule for detecting attacks at the communication level.

The system works in two models:

- Configuration model, when a set of signatures is loaded into the block to build a classification model as an input, each of which is a pair {vector of traffic parameters | attack type}.
- Normal operation model, when the values of the motion parameters are given as input data to the sensor subsystem.

The main tasks of detecting and classifying attacks can be solved using DM methods to detect significant correlations, patterns, and trends in large arrays of network attacks. To analyze large arrays of attacks, we will use DM methods, which form the basis of the algorithm for constructing a classification model of the proposed system.

4. Methods for Analysis of Attacks in Sensor Wireless Networks of IoT

The reference vectors (SVM) method was used to analyze attacks and IoT wireless networks. In this case, each state of the system is represented as a point in multidimensional space, the coordinates of which are the characteristics of the system. Two sets of points belonging to two different classes are separated by a hyperplane in this space. In this case, the hyperplane is constructed in such a way that the distances from it to the nearest instances of both classes are maximum, which provides the greatest accuracy of classification.

Fig. 2 shows the classification of network attacks in two-dimensional space using SVM.

The figure shows a training data set, which is a set of points of the form $\{x_i, y_i\}, i = 1, \dots, l$, where $x_i \in R^n$, $y_i \in \{1, -1\}$ is an indicator of the class to which the point belongs x_i. The classes of points are linearly separable, that is, there is such a hyperplane, on one side of which there are points of the class $y_i = 1$, and on the other of the class $y_i = -1$. Points located directly on the hyperplane satisfy

the equation:

$$\omega \cdot x - b = 0, \quad (1)$$

where the vector ω is the perpendicular to the dividing hyperplane, the quantity $|b|/\|\omega\|$ (the absolute value of b divided by the modulus of the vector ω) determines the distance from the origin to the hyperplane, the operator "·" denotes the scalar product in the Euclidean space in which the data lies.

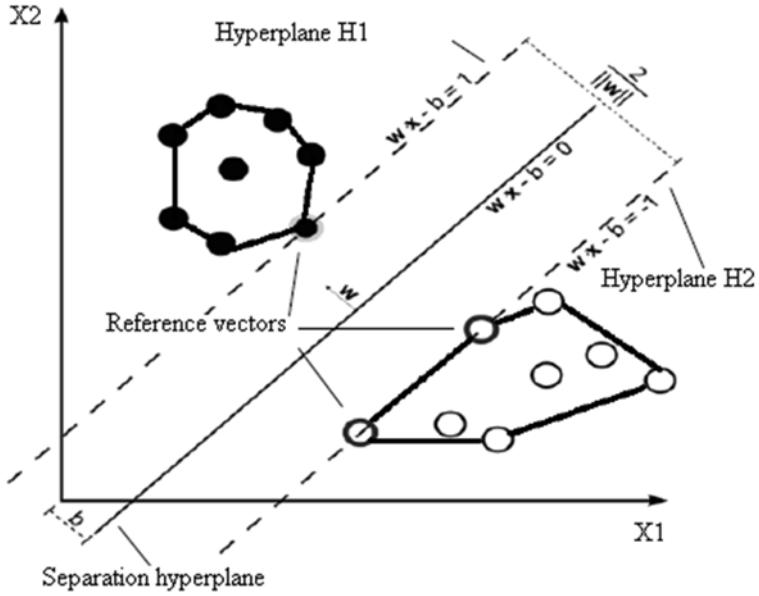

Figure 2: Classification of support vectors in the wireless network of IoT

All points for which the condition $\omega \cdot x_i - b = 1$ is lie in the hyperplane H_1 parallel to the separating hyperplane and at a distance $|1 - b|/\|\omega\|$ from the origin. Similarly, those points for which the condition $\omega \cdot x_i - b = -1$ are lie in the hyperplane H_2 parallel to the plane H_1 and the separating hyperplane, at a distance $|-1 - b|/\|\omega\|$ from the origin. Thus, the distance between the plane and the positive reference vector is $1/\|\omega\|$, and therefore, the width of the strip is $2/\|\omega\|$.

The method of detecting attacks based on the reference vector method was used to build a classification model based on the training sample. The model was tested for attacks such as buffer overflow, rootkit, and SYN flood, and demonstrated the appropriateness of using the support vector method as the basis for an attack detection system. The advantages of this method are high accuracy, generalization, and low computational complexity of decision making. The disadvantage is the relatively high computational complexity of building a classification model.

The k-nearest neighbor (*k-NN*) method is used to assign network attacks to the class that is most common among neighbors for certain attacks. Neighbors are formed from many objects whose classes are already known and based on the given value of *k (k≥1)*, it is determined which of the classes is the most numerous among them. If *k=1*, then the object simply belongs to the class of the only nearest neighbor. The *k-NN* method is one of the simplest DM methods. The disadvantage of the *k-NN* method is its sensitivity to the local data structure.

Neural networks can solve practical problems related to the recognition and classification of network attacks. The neural network consists of interconnected neurons that form the input, intermediate, and output layers. Learning occurs by adjusting the weight of neurons to minimize classification errors. The advantages of neural networks reveal their ability to automatically acquire knowledge in the learning process, as well as the ability to generalize. The main disadvantage is the sensitivity to noise in the input data.

Decision trees are used to record in detail the attributes on which the target function depends, the values of the target function are written in "leaves", and the attributes that distinguish network attacks are written to other nodes. To classify a new object, you need to go down the tree from root to leaf and get the appropriate class, the path from the root to leaf acts as a classification rule based on the

values of the attributes of the attacks. The advantages of decision trees are a simple principle of their construction, good interpretation of the results; the disadvantage is the low accuracy of classification.

To determine the most effective method of constructing a classification model using a wireless attack detection system, a comparison of the considered DM methods will be performed.

5. Analysis of Cyberattacks in Sensor Wireless Systems of IoT

The accuracy of recognition of the considered types of attacks using SWS was evaluated by comparing the results of classification using different DM methods.

Based on the above classification of attacks by OSI model levels, attacks on local wireless networks can be divided into two groups: physical attacks and communication layer attacks, which are specific to wireless networks; application-level network attacks inherent in any LAN organization technology, including Ethernet.

The corresponding sub-module of detection of attacks of the offered system during experiments uses signatures of base NSL KDD-2009 as an example of network attacks and level of application programs. To form a training sample of wireless attacks at the channel and network level, a test local wireless network with WPA2-PSK access protection technology was organized. The collected packages were analyzed and reduced to the form used in the NSL-KDD-2009 database.

Initially, 41 attributes were used to describe the attacks in the NSL-KDD-2009 database, which reflects the application, transport, and network layers of the OSI model. Selected functions are presented in Table 3. To describe attacks characterized by a large number of connections to the target node, a window lasting two seconds (DoS-attacks) was selected, as well as a window of 100 connections to the same node (probe).

Table 3.
Important traffic settings for network and application layers in IoT

Features	Description	Type
Characteristics of the TCP compound		
duration	Connection time (s)	Numerical
protocol_type	Transport layer protocol	Text
service	Application layer service	Text
flag	Status of connection	Binary
src_bytes	Incoming stream, byte	Numerical
dst_bytes	Outbound stream, byte	Numerical
land	The addresses are the same, 0 otherwise	Binary
wrong_fragment	Number of incorrect fragments	Numerical
urgent	Number of urgent packages	Numerical
Session Features		
hot	Number of “hot” indicators	Numerical
num_failed_logins	Number of failed login attempts	Numerical
logged_in	Successful entry	Binary
root_shell	Access with administrative credentials	Binary
num_root	Number of access attempts with administrative credentials	Numerical
num_shells	Number of attempts to use the command line	Numerical
Stats in 2 seconds / 100 connections		
count / dst_host_count	Number of connections with a matching host	Numerical
serror_rate/ dst_host_serror_rate	% connection with error “SYN”	Numerical
rerror_rate / dst_host_same_src_ port_rate	% connections with “REJ” error /% connections with the same source port	Numerical

same_srv_rate / dst_host_same_srv_ rate	% of connections with the same service	Numerical
diff_srv_rate / dst_host_diff_srv_ rate	% connection to various services	Numerical
srv_serror_rate / dst_host_srv_serror _ rate	% connections with “SYN” error	Numerical
srv_rerror_rate / dst_host_srv_rerror _ rate	% connections with error “REJ”'	Numerical
srv_diff_host_rate / dst_host_srv_diff_ host_ rate	% connections with different hosts	Numerical

The first step was to process the data from the database because for the algorithms to work smoothly, all attributes must have numeric values distributed between zero and one. To do this, text attributes were converted to binary, while numeric - normalized to the minimum and maximum values.

After that, the data of the training sample were sent to the input of the building block of the classification model, which forms the basis of the knowledge base, by various methods of CM. The attack detection module then classified the test set entries based on the appropriate model according to the criteria contained in the knowledge base and assigned a network activity class label. Based on the coincidence of evaluation and actual labels of classes, the effectiveness of attack detection was evaluated according to the following criteria:

1. The total percentage of correctly classified attacks A (accuracy):

$$A = \frac{TP+TN}{N}, \quad (2)$$

where *TP* is the number of true-positive records, *TN* is the number of true-negative records, *N* is the total number of classified records.

2. The accuracy of the classification *P* (precision):

$$P = \frac{TP}{TP+FP}, \quad (3)$$

where *FP* is the number of false-positive records.

3. Completeness of classification *R* (recall):

$$R = \frac{TP}{TP+FN}, \quad (4)$$

where *FN* is the number of false-negative entries.

The traffic parameters used to describe the data link attack signatures are shown in Table 4.

Table 4.

Important traffic settings for network and application layers in IoT

Features	Description	Type
802.11 Protocol Features		
frame_ type/subtype	Frame Type / Subtype	Text
protocol_type	Link Protocol Type	Text
source_address	Source MAC Address	Text
destination_address	Destination MAC address	Text
Length	Frame size, bytes	Numerical
SSID	SSID tag value	Text
sequence_number	Frame number	Numerical
fragment_number	Fragment Number	Numerical
DS_status	Distributed system sharing	Numerical
more_fragments	More fragments for transmission, 0 otherwise	Binary
retry	Retransmission of the previous frame, 0 otherwise	Binary
pwr_mgt	The client is in power saving mode, 0 otherwise	Binary
more_data	Buffered frames for transmission, 0 otherwise	Binary

protected_flag	Frame data is encrypted, 0 otherwise	Binary
order_flag	Processing frames strictly in order, 0 otherwise	Binary
duration	ACK + SIFS Transmission Duration, μs	Numerical
chan_number	Channel number	Numerical
signal	The signal level of the transmitter,%	Numerical
TX_rate	Baud Rate, Mbps	Numerical
cipher	Used encryption algorithm	Textual
reason_code	Deauthentication Reason Code	Numerical
Statistics in 2 seconds		
mng_frm_count	The number of management personnel	Numerical
ctrl_frm_count	The number of control frames	Numerical
probe_count	Number of connection requests	Numerical
frag_count	The average number of fragmented packets	Numerical

The experiments were carried out according to the algorithm shown in Fig. 3.

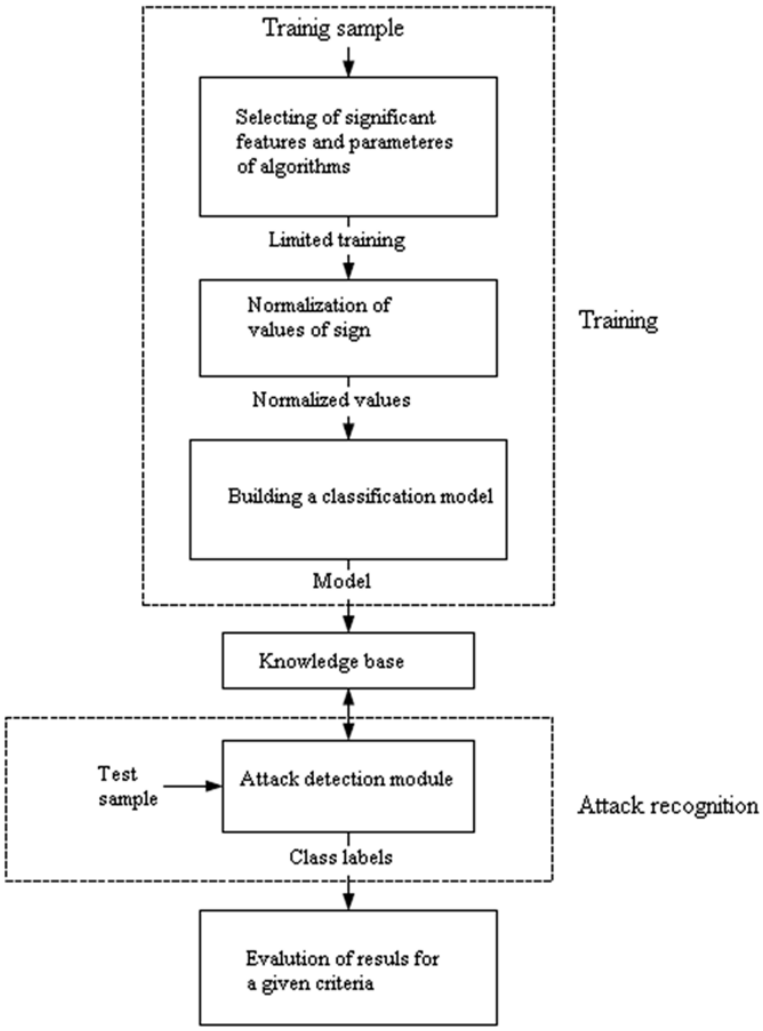

Figure 3: Algorithm for attack detection in sensorless systems of IoT

The support vector method was implemented using the SVS C-SVC library LibSVM, and the radial basis function (RBF) was used as the kernel function. The maximum learning error was limited to 10-5.

The classification results using various DM methods are shown in Tables 5 and 6.

When classified by the method of k-nearest neighbors experimentally, as the optimal parameters of the algorithm, we chose a value of k equal to five. The neural network was implemented as a

multilayer perceptron with two hidden layers. Training lasting 1500 cycles was performed using the algorithm of inverse error propagation. The maximum learning error is 10^{-7}.

Decision trees were constructed using the standard RapidMiner operator, the minimum threshold for forming a new node was four, the minimum number of node leaves was one, and the maximum number of levels was 10.

Table 5.

Network application layer attack performance indicators in IoT, %

Group	Network activity class	Support Vector Method		*k*-nearest neighbors		Neural network		Decision trees	
		fullness	accuracy	fullness	accuracy	fullness	accuracy	fullness	accuracy
DoS	neptune	98.97	99.98	97.25	97.50	99.36	99.98	97.32	99.93
normal	normal	96.56	92.28	96.55	93.63	97.07	87.25	97.10	90.98
R2L	guess_passwd	76.69	100.00	66.86	95.48	66.37	97.03	65.72	99.88
DoS	smurf	100.00	99.70	97.59	100.00	95.19	99.53	100.00	100.00
Probe	satan	93.74	76.47	94.83	76.76	90.75	81.84	96.19	80.62
U2R	buffer_overflow	25.00	62.50	35.00	100.00	0.00	0.00	25.00	62.50
DoS	back	98.05	98.60	99.44	100.00	96.10	97.73	77.16	92.33
R2L	warezmaster	59.11	99.11	82.20	99.74	16.10	98.06	63.56	100.00
DoS	pod	95.12	72.22	95.12	72.22	82.93	70.83	95.12	46.99
Probe	nmap	98.63	93.51	97.26	91.03	79.45	90.62	98.63	74.23
Probe	ipsweep	97.16	93.84	97.16	74.86	97.87	79.31	99.29	88.05
probe	portsweep	91.08	56.30	85.35	73.22	89.17	61.67	84.71	54.07
DoS	teardrop	83.33	21.28	83.33	14.08	75.00	18.75	100.00	24.49
DoS	land	57.14	100.00	57.14	100.00	0.00	0.00	14.29	100.00
Average		83.61	83.27	84.65	84.89	70.38	70.19	79.58	79.58

Table 6

Link Level Attack Performance Indicators in the wireless network of IoT

Class	Support Vector Method		k-nearest neighbors		Neural network		Decision trees	
	Fullness	accuracy	fullness	accuracy	fullness	accuracy	fullness	accuracy
Normal	98.03	92.49	97.65	99.26	94.37	99.38	95.48	95.11
rogue_client	100.00	37.56	6.22	20.00	32.44	20.00	100.00	69.02
EAPOL_logoff_flood	8.82	100.00	26.85	100.00	0.12	100.00	44.08	100.00
auth_flood	85.14	94.03	100.00	93.67	100.00	92.50	97.30	100.00
EAPOL_start_flood	100.00	100.00	100.00	50.58	100.00	44.14	100.00	100.00
deauth_flood	100.00	99.10	100.00	99.75	100.00	84.39	100.00	100.00
caffe_latte	0.00	0.00	100.00	100.00	100.00	70.97	100.00	100.00
Chopchop	100.00	62.86	100.00	100.00	100.00	3.28	100.00	2.27
client_fragment	97.44	99.77	100.00	99.89	100.00	96.98	100.00	100.00
AP_fragment	98.73	97.01	99.75	98.25	100.00	98.26	100.00	100.00
data_replay	99.82	98.13	100.00	99.98	99.96	99.53	100.00	100.00
MAC_spoofing	100.00	6.63	100.00	10.91	0.00	0.00	0.00	0.00
evil_twin_AP	100.00	100.00	100.00	64.78	100.00	94.30	100.00	94.90
EAP_replay	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
beacon_flood	100.00	100.00	100.00	99.95	99.91	100.00	100.00	99.86
RTS/CTS_flood	99.82	99.82	100.00	84.64	100.00	91.49	100.00	91.68
fake_auth	55.56	100.00	66.67	85.71	77.78	10.45	100.00	100.00
Average	84.90	81.61	88.07	82.79	82.62	70.92	90.40	85.46

As can be seen from Table 5, the methods of supporting vectors and k-nearest neighbors showed similar results in the process of detecting attacks, the decision tree and the neural network worked

somewhat worse. The low detection rate of certain types of attacks, such as master-master, guess_passwd, buffer_overflow, and land, is due to the uneven distribution of training samples for different classes—the predominance of common signatures and attacks in the DoS and Probe categories. For the same reason, some attacks were misclassified, so the results are not presented in Table 5. However, according to Table 6, the k-nearest neighbor method and decision tree are superior to SVM and neural networks in solving the problem of link-level attacks.

Thus, the analysis of experimental data shows that the algorithms used to detect network attacks in IoT have different values of attack detection efficiency, depending on the type of network activity and the level of the OSI model on which the attack is implemented.

6. Conclusion

The article proposes to use a combination of four algorithms and one classifier, which determines the final class of network activity by weighted voting.

The study allows to classify network attacks occurring in wireless LANs in the Internet of Things and to build the architecture of the proposed attack detection system, which is based on the use of DM methods to recognize network attacks on the database and compare these methods during experiments to detect network attacks in IoT.

The selected methods have shown high accuracy and completeness of detection of cyberattacks during experiments, and the developed system of detection of attacks in wireless IoT networks can have practical application. The obtained results provide the development of sound recommendations for eliminating the identified bottlenecks and improving the security of the IoT network. Based on these recommendations, the user makes changes to the configuration of the real network or its model, and then, if necessary, repeats the process of vulnerability analysis and security assessment. Thus, the required level of computer network security is ensured at all stages of the IoT life cycle.

The architecture and principles of operation of the proposed system for detecting attacks in wireless IoT networks will be the basis for further research. The scope of further research includes improving network attack models and assessing the level of IoT protection, in particular: metric security systems and rules for their calculation, development of system components, modification of the approach to wireless network security analysis, and further experimental evaluation of proposed solutions for IoT networks.

7. References

[1] A. Olusola, A. Oladele, D. Abosede, Analysis of KDD'99 Intrusion Detection Dataset for Selection of Relevance Features, World Congress on Engineering and Computer Science 1 (2010) 162–168.

[2] T. Nguyen, B. Nguyen, H. Pham, An efficient solution for preventing Dis'ing attack on 802.11 networks, in: International Conference on Green Technology and Sustainable Development, 2012 pp. 395–403.

[3] O. Belej, N. Nestor, O. Polotai, J. Sadeckii, Features of application of data transmission protocols in wireless networks of sensors, in: 3-rd International Conference Advanced information and communication technologies, 2019, pp. 317–322. doi:10.1109/AIACT.2019.8847878.

[4] S. Mulay, P. Devale, G. Garje, Intrusion Detection System using Support Vector Machine and Decision Tree, International Journal of Computer Applications 3.3 (2010) 40–43. doi:10.1109/ICNIT.2010.5508557.

[5] T. Sun, J. Zhang, Y. Yang, Review on the development and future trend of the intrusion detection system (IDS), in: International Conference on Communication and Electronics Systems (ICCES), 2016, pp. 1-6. doi:10.1109/CESYS.2016.7889907.

[6] M. R. Ahmed, H. Cui, X. Huang, Smart integration of cloud computing and MCMC based secured WSN to monitor the environment, in: 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory, and Aerospace & Electronic Systems, 2014, pp.1–5. doi:10.1109/VITAE.2014.6934449.

[7] W. Han, Z. Tian, Z. Huang, D. Huang, Y. Jia, Quantitative Assessment of Wireless Connected Intelligent Robot Swarms Network Security Situation, IEEE Access 7 (2019) 134293–134300. doi:10.1109/ACCESS.2019.2940822.
[8] S. P. Dongare, R. S. Mangrulkar, Implementing energy-efficient technique for defense against Gray-Hole and Black-Hole attacks in wireless sensor networks, in: International Conference on Advances in Computer Engineering and Applications, 2015 pp. 167–173. doi:10.1109/ICACEA.2015.7164689.
[9] M. A. Alsheikh, S. Lin, D. Niyato, H. Tan, Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications, IEEE Communications Surveys & Tutorials 16.4 (2014) 1996–2018. doi:10.1109/COMST.2014.2320099.
[10] Y. El Mourabit, A. Toumanari, A. Bouirden, H. Zougagh, R. Latif, Intrusion detection system in Wireless Sensor Network based on mobile agent, in: Second World Conference on Complex Systems (WCCS), Agadir, 2014, pp. 248–251. doi:10.14569/IJACSA.2015.060922.
[11] I. Sreeram, V. P. K. Vuppala, HTTP flood attack detection in application layer using machine learning metrics and bio-inspired bat algorithm, Applied Computing, and Informatics 15 (2019) 1–5. doi:10.1016/j.aci.2017.10.003.
[12] S. Nandita, S. Jaydeep, S. Jaya, S. Moumita, Designing of an online intrusion detection system using rough set theory and Q-learning algorithm, Neurocomputing 11.1 (2013) 161–168. doi:10.1016/j.neucom.2012.12.023.