IRSTI 44.01.77 https://doi.org/10.58805/kazutb.v.3.24-482

ANALYSIS OF REAL-WORLD AND SIMULATION MODELS AND ALGORITHMS FOR DETECTING ATTACKS IN WIRELESS SENSOR NETWORKS

[1,2]Y. Mardenov ✉, [3]Zh. Iztaev, [3]Hu Wen-Tsen, [1,2]D. Mardenova, [1,2]D. Baumuratova

[1]International Science Complex ”Astana”, Astana, Kazakhstan,

[2]Astana International University, Astana, Kazakhstan,

[3]M.Auezov South Kazakhstan State University, Shymkent, Kazakhstan

✉Корреспондент-автор: emardenov@gmail.com

Presented are real-world and simulation models, methods, and tools for simulating attacks on Wireless Sensor Networks (WSNs) intended for use in network vulnerability research. A comparative analysis was conducted to identify their advantages and disadvantages. The research demonstrated that integrating real-world and simulation approaches contributes to increased accuracy and reliability in attack detection. Recommendations are proposed for developing flexible and scalable simulation models, improving the efficiency of attack detection algorithms, and regularly updating models in accordance with changing WSN operating conditions and emerging threats.

Keywords: WSN, Real-world models, Simulation models, WSN attack detection, Attack detection algorithms, Comparative analysis of detection tools, Integration of detection methods, Network security.

АНАЛИЗ НАТУРНЫХ И ИМИТАЦИОННЫХ МОДЕЛЕЙ И АЛГОРИТМОВ ВЫЯВЛЕНИЯ АТАК БСС

[1,2]Е. Марденов✉, [3]Ж. Изтаев, [3]Ху Вен-Цен, [1,2]Д. Марденова, [1,2]Д. Баумуратова

[1]Международный научный комплекс «Астана», Астана, Казахстан,

[2]Международный университет «Астана», Астана, Казахстан,

[3] Южно-Казахстанский государственный университет имени М. Ауэзова, Шымкент, Казахстан,

e-mail: emardenov@gmail.com

В данной статье представлен анализ натурных и имитационных моделей и алгоритмов выявления атак на беспроводные сенсорные сети (БСС). Описаны разработанные натурные и имитационные модели, методы и инструменты для имитации атак, а также результаты экспериментальных исследований. Сравнительный анализ выявляет преимущества и недостатки каждого подхода, подчеркивая необходимость интеграции натурных и имитационных методов для достижения наибольшей точности и надежности в обнаружении атак. В статье предложены рекомендации по развитию гибких и масштабируемых имитационных моделей, улучшению алгоритмов обнаружения атак и регулярному обновлению моделей в соответствии с изменяющимися условиями и угрозами. Результаты исследования подчеркивают важность комбинированного использования натурных и имитационных подходов для повышения уровня безопасности БСС.

Ключевые слова: Беспроводные сенсорные сети (БСС), Натурные модели, Имитационные модели, Выявление атак, Алгоритмы обнаружения, Сравнительный анализ, Интеграция методов, Безопасность сетей

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРДІҢ ТАБИҒИ ЖӘНЕ СИМУЛЯЦИЯЛЫҚ МОДЕЛЬДЕР МЕН ШАРУАЛДАРДЫ АНЫҚТАУ АЛГОРИТМДЕРІН ТАЛДАУ

[1,2]Е. Марденов, [3]Ж. Изтаев, [3]Ху Вэн-Цен, [1,2]Д. Марденова, [1,2]Д. Баумуратова

[1] «Астана» халықаралық ғылыми кешені, Астана, Қазақстан,

[2]Астана халықаралық университеті, Астана, Қазақстан,

[3] М.Әуезов атындағы Оңтүстік Қазақстан мемлекеттік университеті, Шымкент, Қазақстан,

e-mail: emardenov@gmail.com

Бұл мақалада сымсыз сенсорлық желілерге шабуылдарды анықтаудың табиғи және имитациялық модельдері мен алгоритмдерін талдау ұсынылған. Әзірленген табиғи және имитациялық модельдер, шабуылдарды модельдеу әдістері мен құралдары және эксперименттік зерттеулердің нәтижелері сипатталған. Салыстырмалы талдау шабуылдарды анықтауда ең жоғары дәлдік пен сенімділікке қол жеткізу үшін табиғи және имитациялық әдістерді біріктіру қажеттілігін көрсете отырып, әрбір тәсілдің артықшылықтары мен кемшіліктерін анықтайды. Мақалада икемді және масштабталатын модельдеу модельдерін дамыту, шабуылдарды анықтау алгоритмдерін жақсарту және өзгеретін жағдайлар мен қауіптерге сәйкес модельдерді үнемі жаңарту бойынша ұсыныстар берілген. Зерттеу нәтижелері қауіпсіздік деңгейін жақсарту үшін табиғи және имитациялық тәсілдерді біріктіріп қолданудың ма-ңыздылығын көрсетеді сымсыз сенсорлық желілер.

Түйін сөздер: Сымсыз сенсорлық желілер, табиғи модельдер, модельдеу модельдері, шабуылдарды анықтау, анықтау алгоритмдері, салыстырмалы талдау, әдістерді біріктіру, желі қауіпсіздігі

Introduction. Wireless Sensor Networks (WSNs) are widely and comprehensively utilized, playing a crucial role in addressing various practical tasks in military, industrial, and domestic spheres. WSNs represent a multifunctional communication foundation of cyber-physical systems with artificial intelligence elements, providing connectivity between various sensor devices and systems that can collect, process, and transmit environmental data in real-time. This foundation enables effective automatic monitoring and control of various processes and objects over extensive and hard-to-reach areas [1, 2].

However, the use of WSNs is associated with certain risks due to their security vulnerabilities. Attacks by malicious actors on such networks can lead to serious consequences, including data interception, tampering, and disruption of the functionality of technical equipment, particularly sensor devices that are fundamental elements of WSNs. Consequently, there is increasing importance in developing effective measures to counter potential threats within WSN security frameworks.

A critical measure to combat these threats is the development of efficient methods for detecting, recogni-zing, and preventing network attacks. Specifically, analytical and simulation models of attacker actions on WSNs allow for the study of processes within WSNs induced by these attacks. Such models are based on mathematical and statistical descriptions of attacker and defender behaviors using real network data, parameters, and characteristics. They enable the creation of virtual environments for comprehensive simula-tion of WSNs, including the operation of sensor nodes, communication processes between nodes over radio channels, data reception and transmission, and routing [1, 3, 4].

This study aims to conduct testing and comparative analysis of natural and simulation models of attacks on WSNs, attack detection algorithms, and to develop recommendations for their effective implementation.

Materials and methods. *Analytical review of literary sources on the research issue.*

There are several different types of attacks that can occur in WSNs.

Threats to confidentiality involve interception and observation, where attackers intercept data or analyze traffic to obtain confidential information. Threats to integrity are associated with data modification, source impersonation, message replay, and message denial, which lead to data distortion and incorrect network operation. Attackers can alter messages, spoof sources, replay intercepted data, or deny sending/receiving messages. Availability threats aim to disrupt message delivery, causing network service denial. These attacks include Denial of Service (DoS), node capture, and resource depletion attacks, leading to node overload or network disconnection. Such attacks can severely disrupt network operation, highlighting the importance of protecting against them. [2, 4, 5]

The paper presents [6] a new intrusion detection model for WSNs using fuzzy neural networks and feedforward neural networks. Experimental results show that the proposed model achieves detection rates averaging 97.8% with maximum detection accuracy of 98.8%. Evaluations were compared against benchmark models based on support vector machines (SVM), decision trees (DT), and random forest (RF) models.

Authors [7] introduced detection of multiple attacks in wireless sensor networks using artificial neural networks. The dataset is split into training and testing using a multi-layer perceptron artificial neural network to detect ten classes of attacks, including DoS attacks. Research using benchmark datasets UNSW-NB, WSN-DS, NSL-KDD, and CICIDS2018 showed that the proposed system achieves an average detection

In article [8], the use of spatial information for detecting and localizing multiple attacks across single and multiple nodes is presented. A scalable and energy-efficient anomaly detection mechanism based on clusters (SEECAD) is described for detecting DoS attacks without key management schemes to enhance network lifespan. Detection speed, false alarm rate, packet delivery ratio, overhead costs, energy consumption, and average packet delay are various performance metrics used to evaluate network performance.

In [9], an enhanced high-performance secure routing protocol based on clustering is proposed. A key feature of this protocol is its consideration of aspects such as energy consumption, packet reduction, congestion management, encrypted data transmission, and monitoring of malicious nodes to improve data management quality. To demonstrate the feasibility of the proposed method, performance metrics such as ransomware attack detection level, ergodic residual energy per round, early clone attack detection, throughput maximization, delay, maximum throughput, and network lifespan maximization were used.

The works [10] conducted modeling to demonstrate that the proposed EdDSA-XOR functionality reduces time and energy costs by 0.13% and 0.07% respectively, compared to other methods. Node authentication in the network was tested against ”man-in-the-middle” attacks.

The paper proposes [11] an effective method for detecting black hole and Sybil attacks using the Adaptive Taylor Sail (Adaptive Taylor-SFO) algorithm. The BSS nodes are modeled in the network, followed by routing using Adaptive Taylor-SFO. The router was developed by integrating the Adaptive concept with the Taylor series and the Sail Fish optimizer (SFO) to select the optimal route considering adaptability metrics such as delay, energy, and distance. Black hole and Sybil attack detection is performed by the Deep stacked automatic encoder. Thus, the proposed system effectively classifies normal, black hole, and Sybil attacks. The analysis of the reviewed works made it possible to determine the most common types of attacks on WSNs (Table 1), the mechanisms of their impact, possible consequences and methods of mitigating the consequences.

Table 1 - Most common attacks on WSN

№	Attack name	Mechanism of action	Consequences	Mitigation Strategies
1	Routing attack [6]	Routing attacks involve manipulating routing mechanisms to redirect or block data flows. Attackers exploit vulnerabilities across various layers of the network protocol stack. Examples include black hole attacks, where malicious nodes discard received data, and wormhole attacks, where attackers create shortcuts between remote nodes.	Data loss. Network segment-ation. Resource exhaustion.	Secure routing protocols. Anomaly detection. Cooperative verification. Hop count verification. Location verification.
2	The man in the middle attack [10]	Man-in-the-middle attack involves an attacker secretly intercepting and relaying messages between two communicating nodes without their knowledge. The attacker can manipulate the contents of the messages or simply eavesdrop on them. Man-in-the-middle attacks exploit the absence of secure communication channels and can occur at various protocol levels, including application, transport, and network layers.	Data falsification: Unauthorized access leading to breach of confidentiality	Encryption. Public Key Infrastructure (PKI). Certificate revocation. Timestamps and one-time passwords. Intrusion detection systems.
3	Sibyl [12]	Sybil attack involves creating a network of malicious nodes that impersonate legitimate nodes. The attacker's goal is to inject false information or disrupt network communication. These attacks can undermine data accuracy, routing efficiency, and overall network functionality.	Data integrity Routing mani-pulation Resource exhaustion	Behavioral analysis Trust-based systems Physical layer measurements Reputation mechanisms Cryptographic methods
4	Eaves-dropping [13]	In an eavesdropping attack, an attacker is placed within the range of two or more sensor nodes using the transmission of unencrypted or weakly encrypted data. The attacker passively intercepts data packets without changing the functionality of the network. Eavesdropping can occur at various levels of the communications stack, from the physical layer to the application layer.	- Data confidenti-ality - Data integrity - Network mapping	- Encryption - Secure key exchange - Frequency hopping - Intrusion detection - Secure protocols
5	Denial of Service (DoS) [14,15]	A DoS attack exploits vulnerabilities in WSNs to reduce their performance or even disable them. Attackers employ various methods such as flooding the network with excessive traffic or exploiting protocol vulnerabilities. In the context of WSNs, attacks can target nodes, communication channels, or the sink node responsible for aggregating data.	Data loss Resource depletion Network partitioning Delayed responses	Intrusion detection Rate limiting Traffic filtering Energy consumption management Collaborative defense

Empirical models and attack detection algorithms.

Description of the empirical models used for attack detection

Table 2 - Full-scale experiments to detect attacks and their results

№	Name	Description	Results
1.	jamming attack	Nodes of the network were deployed in an open space with various obstacles. A jamming attack was initiated using a powerful radio transmitter, creating interference within a specific frequency range.	It was found that the jamming attack significantly reduces signal strength and increases packet loss frequency. The detection system was able to identify the attack based on signal strength and packet loss analysis, achieving a detection accuracy of 92%.
2.	resource exhaustion attack	Nodes in the experiment were programmed to perform energy-intensive tasks. The attacker sent a large number of false requests to the nodes to accelerate their battery discharge.	Nodes with depleted resources ceased normal operation. The detection model based on energy consumption monitoring successfully identified the attack with 87% accuracy, enabling timely network protection measures to be implemented.
3.	replay attack	The experiment involved nodes equipped with built-in authentication mechanisms. The attacker retransmitted previously intercepted legitimate messages.	The detection system based on timestamps and authentication algorithms successfully identified repeated messages with 95% accuracy, preventing the execution of false commands.

Table 3 - Evaluation of the effectiveness of full-scale models and algorithms

accuracy	**detection time**
The ability of the model to correctly identify attacks and minimize false positives was evaluated in the conducted experiments. Accuracy ranged from 87% to 95%, depending on the type of attack and the algorithm applied.	The time required to identify an attack after its onset. Natural models demonstrated the ability to detect attacks in real time, which is critical for preventing damage.
resource consumption	**adaptability**
The volume of computational and energy resources required for algorithm operation. Efficient algorithms minimize resource consumption, which is particularly crucial for sensor nodes with limited batteries.	The ability of the model and algorithms to adapt to changes in the environment and new types of attacks. Natural models have demonstrated good adaptability when new nodes are added or when the network topology changes.

Natural models for detecting attacks in WSNs involve physically implemented networks where nodes and sensors are deployed in real operational conditions. These models utilize real devices such as microcontrollers, radio modules, and sensors that interact within realistic environmental settings.

The primary advantage of natural models lies in their ability to accurately reproduce real network operation scenarios, including potential external interferences and physical attacks.

Research on natural models for attack detection in wireless sensor networks includes functional and quantitative characteristics. Attack detection methods are categorized into signature-based, anomaly-based, and hybrid approaches, covering attacks on availability, confidentiality, integrity, and authentication. Hardware and network characteristics of sensors and nodes, data processing algorithms, and monitoring systems play a crucial role. Quantitative metrics include detection accuracy, detection time, energy consumption, throughput, delay, and scalability.

For instance, platforms like TinyOS and Contiki are used to test intrusion detection systems, achieving 95% accuracy with low false positive rates. Machine learning-based systems such as K-means and SVM can achieve classification accuracies up to 98%. Distributed detection methods include autonomous algorithms that depend on node density and algorithm complexity [15, 16]. Table 2 presents empirical experiments on attack detection and their outcomes.

The effectiveness of full-scale models and attack detection algorithms is assessed based on several key parameters (Table 3)

Thus, natural models and intrusion detection algorithms in WLANs are effective tools for studying and protecting networks, ensuring high accuracy and timely detection of attacks in real operational conditions.

Imitative models and intrusion detection algorithms

Description of Developed Simulation Models. Simulation models are software tools designed to replicate the operations of Wireless Sensor Networks (WSNs) and simulate various attack scenarios in a controlled environment. Within the scope of the conducted research, simulation models were tested that accurately reproduce the behavior of sensor nodes, communication protocols, and interactions with the external environment. These models are based on the following principles:

1. Multi-layered architecture of the model: The simulation model includes physical, data link, network, and application layers, enabling detailed reproduction of all aspects of Wireless Sensor Network (WSN) operation.

2. Network topology modeling: Supports various topologies such as mesh, star, and tree, allowing exploration of how topology affects resilience to attacks.

3. Parameter flexibility: The model allows configuration of node parameters such as transmitter power, data transmission rate, and energy consumption, crucial for investigating different attack scenarios.

All simulation models are built using diverse mathematical and computational methods. These models facilitate testing and analyzing network behavior under attack, evaluating detection accuracy, and justifying the realism of simulated conditions (Table-4).

Model adequacy assessment involves comparing simulation results with real-world data, including topology parameters, traffic intensity, and attack frequency. A model is considered adequate if its behavior does not statistically differ from real data, often verified using tests like the Kolmogorov-Smirnov test. An example application of such models could include testing intrusion detection systems on the TinyOS platform, achieving a detection accuracy of 95% with a false positive rate of less than 2%, utilizing a hybrid approach to enhance accuracy and minimize energy consumption.

Methods and tools for simulating attacks on wireless sensor networks

For implementing simulation models, a number of modern tools and methods were utilized to ensure high accuracy and scalability of the research. The key tools include:

1. NS-3 (Network Simulator 3): A powerful tool for network simulation that allows reproduction of a wide range of protocols and attack scenarios on WLANs. NS-3 provides detailed modeling of node behavior and interactions between nodes.

2. MATLAB/Simulink: Used for mathematical

modeling and analysis of attack detection algorithms. MATLAB facilitates the development and testing of complex algorithms, as well as the analysis of data obtained from simulations.

3. Omnet++: A tool for modeling and simulating networks, offering high flexibility in network parameter configuration and attack scenarios. Omnet++ supports extensibility, enabling integration of custom models and algorithms.

These tools collectively support comprehensive modeling, simulation, and analysis of wireless sensor networks (WSNs), enabling researchers to evaluate the performance and effectiveness of various security mechanisms against different types of attacks.

Table 4 - Composition and structure of models

№	Model	Composition and structure of models	Mathematical description
1	Network layer	*Graph model: Sensors and nodes are represented as a graph* $G(V,E)$ G(V,E), where V V - a set of vertices (nodes), and E E - many edges (communication channels). *Topology:* The parameters of the network topology are defined, including the distance between nodes, node density, and network type (e.g., star, tree, mesh network).	$G(V,E)=\{(v_i,v_j) \mid v_i,v_j\in V, e_{ij}\in E\}$ (1) where $V=\{v_1,v_2,\ldots,v_n\}$ - many nodes, $E=\{e_{ij}\}$ E={e_{ij}} - many communication channels.
2	Traffic model	*Data flow:* The distribution of traffic between nodes is described. This is achieved using probabilistic models such as Poisson distribution or Markov models.	λij=Rate($vi\to vj$) (2) where λ_{ij} - traffic intensity between nodes v_i and v_j, which may follow a Poisson distribution: (3)
3	Attack model	*Types of attacks:* Models are defined for various types of attacks, such as DoS attacks, data interception attacks, and data integrity attacks. *Attacker behavior:* The strategy of the attacker is determined, including the frequency and intensity of attacks.	(4) where d - distance to target, θ - interception angle.
4	Detection model	*Methods:* Implementation includes detection algorithms such as signature-based, anomaly-based, and hybrid methods. *Machine learning algorithms:* Utilized for traffic classification, such as K-means, SVM, neural networks.	Anomalous method: (5) where x_i x_i - measured value, μ_i - average value, w_i - weight coefficient. Machine learning algorithms: K-means: (5) where J - loss function, k - number of clusters, $x_j^{(i)}$ - data points, μ_i - cluster centroids

Results and discussion. Results of simulation experiments and their analysis. Within the

framework of conducted simulation experiments, various types of attacks on WLANs were simulated, including jamming attacks, resource exhaustion attacks, replay attacks, and spoofing attacks. The results of the experiments enabled a detailed analysis of the effectiveness of the proposed models and attack detection algorithms (Table 5).

Analysis of the results showed that the developed simulation models and algorithms are highly effective in detecting attacks on WSNs. The experiments conducted allowed for a detailed study of network behavior under various types of attacks and proposed algorithms that demonstrate high accuracy and promptness in detection. The results confirm the feasibility of using simulation models in the research and development of protection systems for wireless sensor networks.

Table 5 - Composition and structure of models

№	Attack	Description of the experiment	Results
1.	jamming attack	An experiment to simulate a jamming attack was conducted using a powerful transmitter in Omnet++, a platform for modeling network systems. The experiment involved creating a wireless sensor network of 100 nodes with a random topology and a transmission radius of 50 meters. The experiment consisted of three stages: network initialization without attack, introduction of the jamming transmitter, and data collection. The collected data included received signal strength indicator (RSSI), packet loss, and transmission delay, amounting to approximately 10,000 records. Data processing was performed using statistical methods and machine learning algorithms such as K-means and SVM. The data processing methodology included data filtering, analysis of signal strength levels, and anomaly classification [17, 18].	The results showed that the jamming attack significantly reduces communication quality and increases latency. Simulation algorithms were able to detect the attack with 94% accuracy by analyzing signal strength and packet loss rates. The experiment demonstrated the possibility of using this technique in real wireless sensor networks.
2.	resource exhau-stion attack	A simulation experiment for a resource exhaustion attack was conducted using the NS-3 network simulator. The experimental setup included a wireless sensor network comprising 50 nodes, each equipped with a limited battery. The experiment was planned by creating the network, setting battery parameters, and launching a series of attacks involving sending a large number of false requests to the nodes. During the experiment, data on energy consumption, node response time, and failure rate were collected. Approximately 5000 data records were gathered, covering all stages of the attack. Data processing was carried out using an energy consumption monitoring methodology developed and described in [19]. This methodology included data filtering, analysis of energy consumption time series, and detection of deviations from normal behavior.	Algorithms based on this methodology were able to identify abnormal behavior with an accuracy of 89% and an average attack detection time of 2.3 seconds. The effectiveness of the methodology was confirmed by its high accuracy and rapid detection of attacks. The experiment demonstrated that the proposed methodology is effective for application in real-world conditions of wireless sensor networks.

№	Attack	Description of the experiment	Results
3.	replay attack	Experimental studies aimed at examining replay attacks were conducted using a model created in the Simulink environment. In this experiment, the model simulated the repeated transmission of intercepted messages, mimicking a scenario where an attacker could re-execute previously executed commands. The experimental setup consisted of a network model including several nodes and data transmission mechanisms configured to implement replay attacks. The experiment planning involved configuring model parameters, defining attack characteristics, and selecting detection methods. During the experiment, data related to message timestamps, as well as parameters of authentication and integrity verification methods, were collected. The total amount of gathered data was about 2,000 records, covering various attack scenarios and the system's responses to them. The data were processed using algorithms based on analyzing message timestamps and authentication methods. The data processing methodology included filtering out repeated messages and verifying their compliance with expected time intervals [19].	The experimental results showed that algorithms based on timestamps and authentication methods successfully detected replayed messages with an accuracy of 97%, significantly reducing the risk of executing false commands and enhancing the effectiveness of the replay attack defense system.
4.	spoofing	Experimental studies focused on spoofing attacks were conducted using Simulink software. The experiment was designed by creating scenarios in which an attacker sent false messages, pretending to be legitimate network nodes, with the aim of infiltrating the system. Parameters of the transmitted messages, such as node identifier, message content, and timestamp, were recorded for data collection. The total amount of data collected was approximately 3,000 records, covering various attack scenarios and network responses. For data analysis, algorithms for node identity verification and behavior analysis developed by the experiment's authors were applied. The data processing methodology included the identification of anomalous nodes, comparison of their behavior with samples of normal functioning, and detection of deviations [20].	As a result of the experiment, the model was able to effectively detect spoofing attacks with 92% accuracy. The system's response time to detect the attack was 1.8 seconds, demonstrating the high reactivity and efficiency of the developed algorithms. The obtained results confirm the effectiveness of the proposed spoofing attack protection methodology and its readiness for practical application in real network systems.

Comparative analysis of full-scale and simulation approaches.

Methodology for Comparing Physical and Simulation Models.

To conduct a comparative analysis of physical and simulation models, the following methodological steps were developed and applied:

Selection of Representative Attack Scenarios: Typical attack scenarios were chosen, such as jamming, resource exhaustion attacks, replay attacks, and spoofing. These scenarios cover a wide range of threats to wireless sensor networks (WSNs).

Construction of Physical Models: The implementation of physical models involved deploying sensor nodes in real operational conditions. Various network topologies, such as mesh and star, were used to ensure a diversity of conditions. Real devices were subjected to attack impacts to collect data on network behavior.

Creation of Simulation Models: Simulation models were developed using tools like NS-3 and Omnet++, allowing for accurate reproduction of the conditions and behavior of sensor nodes, as well as attack impacts. These models were configured to match the conditions of the physical experiments.

Comparison of Physical and Simulation Models: The comparison was conducted based on several criteria, including attack detection accuracy, response time, resource consumption, and adaptability to changes in network conditions (Table 6).

Table 6 - Composition and structure of models

accuracy	detection time
The model's ability to correctly identify attacks and minimize false positives. Accuracy was measured as the ratio of correctly detected attacks to the total number of attacks.	The time required to identify an attack after it has begun. Fast detection is critical to minimizing the damage from attacks.
resource consumption	**adaptability**
The amount of computing and energy resources required to run detection algorithms. This criterion is especially important for WSN nodes with limited batteries and computing power.	The ability of the model and algorithms to adapt to changes in network conditions and new types of attacks. This includes the model's ability to work across different network topologies and load changes.

Table 7 - Results of comparative analysis, identified advantages and disadvantages of models

	Advantages:	**Flaws:**
Full-scale models	- Highly realistic: Full-scale models accurately reflect actual operating conditions, including physical disturbances and unforeseen factors. - Relevance of data: Data collected in field experiments are direct results of the operation of real devices and protocols.	- High costs: Deploying and maintaining full-scale models requires significant financial and time resources. - Limited scalability: It is difficult and expensive to scale up field experiments to large networks or different scenarios.
Simulation models	- Flexibility and scalability: Simulation models are easily customized and scalable for different scenarios and network topologies. - Low costs: Simulation experiments are carried out in a software environment, which significantly reduces costs compared to full-scale experiments.	- Limited realism: Simulation models may not fully account for all real-world physical and environmental factors, which may lead to variations in results. - Dependence on model accuracy: The effectiveness of simulation models is highly dependent on the accuracy of reproducing real-world conditions and network behavior.

In general, both approaches have their strengths and weaknesses, but their combination can provide the most complete and reliable analysis of attacks on WSNs. Full-scale models provide high accuracy and data relevance, while simulation models offer flexibility and cost-effectiveness. The optimal solution is to use full-scale experiments to verify and calibrate simulation models, which allows you to combine the advantages of both approaches.

Conclusions. Analysis of full-scale and simulation models and algorithms for identifying attacks on WSNs shows that both approaches have their own unique advantages and disadvantages. Full-scale models provide highly accurate and up-to-date data because they reproduce real-life network operating conditions. However, their use is associated with high costs and limited scalability. Simulation models, in contrast, offer flexibility and cost-effectiveness, allowing easy adjustment of parameters and scale-up of experiments, but may not fully account for all real-world physical factors.

Based on the presented data, we can conclude that the combined use of full-scale and simulation approaches is optimal in the context of ensuring the security of wireless sensor networks. The integration of natural and simulation methods makes it possible to jointly use their advantages, ensuring high accuracy and reliability of attack detection algorithms. Using field data to calibrate and verify simulation models plays an important role in achieving high accuracy in network vulnerability analysis. Recommendations for improving models and algorithms, including developing flexible and scalable simulation models, improving attack detection algorithms, and regularly updating models, are aimed at increasing the effectiveness of the attack detection system. This combined use of methods and the development of infrastructure for field experiments seem to be the most effective ways to improve the security of wireless sensor networks in the face of rapidly changing threats. This work by the staff of the International Scientific Complex ”Astana” is carried out with the financial support of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19680345).

References

1. Lei Zou, Zidong Wang, Bo Shen, Hongli Dong, Guoping Lu, Encrypted Finite-Horizon Energy-to-Peak State Estimation for Time-Varying Systems Under Eavesdropping Attacks: Tackling Secrecy Capacity, IEEE/CAA Journal of Automatica Sinica. -2023. Vol. 10(4). -P. 985-996. DOI 10.1109/JAS.2023.123393.

2. A. Adamova, T. Zhukabayeva and Y. Mardenov Machine Learning in Action: An Analysis of its Application for Fault Detection in Wireless Sensor Networks // 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023, P.506-511. DOI 10.1109/SIST 58284.2023.10223548.

3.G.P.S. Kumar, J. R. R. Kumar and S. R. T, Design of Secure Communication Methodologies for WSN Assisted IoT Applications, 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India.// -2022. -P.1-5. DOI 10.1109/ASIANCON55314.2022.9908931.

4. S.A.H. Antar et al. Classification of Energy Saving Techniques for IoT-based Heterogeneous.Wireless Nodes //Procedia Comput. Sci. -2020.- Vol.171. - P. 2590-2599

5. Kalaivanan Karunanithy et al. Cluster-tree based energy efficient data gathering protocol for industrial automation using WSNs and IoT// J. Indust. In format. Integrat.// -2020.- Vol.19. DOI 10.1016/j.jii. 2020.100156

6. Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A. et al. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks //Soft Comput. -2023. Vol. 27.- P. 4157-4168. DOI 10.1007/s00500-022-06915-1

7. J. Panda, and S. Indu Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using

Artificial Neural Network// Wireless Communications and Mobile Computing.–2023.-Vol. 7. - P.1-29. DOI 10.1155/2023/2744706

8. Premkumar, M., Ashokkumar, S.R., Jeevanantham, V. et al. Scalable and Energy Efficient Cluster Based Anomaly Detection Against Denial of Service Attacks in Wireless Sensor Networks.// Wireless Pers Commun. -2023.- Vol.129.- P.2669-2691.DOI 10.1007/s11277-023-10252-3

9. Roberts M.K., Ramasamy P. An improved high performance clustering based routing protocol for wireless sensor networks in IoT// Telecommun Syst. -2023.- Vol. 82.- P. 45-59. DOI 10.1007/s11235-022-00968-1

10. Yuvaraj, N., Raja, R.A., Karthikeyan, T. et al. Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) Using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack// Wireless Pers Commun. -2022.- Vol. 123. - P. 71715-1731 DOI 10.//1007/s11277-021-09209-1

11. M. Kumar and J. Ali, Adaptive Taylor-Sail Fish Optimization based deep Learning for Detection of Black Hole and Sybil Attack in Wireless Sensor Network// International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India. -2023. - P. 1237-1244. DOI 10.1109/ICSCDS56580.2023.10104946.

12. Orman, A., Üstün, Y. & Dener, M. Detailed analysis of sybil attack in wireless sensor networks // International Journal of Sustainable Engineering and Technology.-2023.-Vol.7(1)-P.41-54. https://dergipark.org.tr/en/pub/usmtd/issue/78577/1305047

13. Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, From Industry 4.0 to Agriculture 4.0: current status, enabling technologies, and research challenges// IEEE Transactions on Industrial Informatics. -2021.-Vol. 17(6)- P. 4322-4334. DOI 10.1109/TII.2020.3003910

14. A. Williams, P. Suler,J. Vrbka Business process optimization, cognitive decision-making algorithms, and artificial intelligence data-driven internet of things systems in sustainable smart manufacturing//Journal of Self-Governance and Management Economics. -2020. Vol.8(4).-P. 39-48. DOI 10.22381/JSME8420204

15. Wendi Rabiner Heinzelman, Anantha Chandrakasan,Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks//In Proceedings of the 33rd annual Hawaii international conference on system sciences. -2000. - P. 10.

16. Ibrahim Alrashdi, Ali Alqazzaz, Raed Alharthi, Esam Aloufi, Mohamed A Zohdy Hua Ming. Fbad: Fog-based attack detection for iot healthcare in smart cities //In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). -2019. –P. 515-522. DOI 10.1109/UEMCON47517.2019.8992963

17. Chen M., Liu W., Zhang, N., Li J., Ren Y., Yi M., Liu A. GPDS: A Multi-Agent Deep Reinforcement Learning Game for Anti-Jamming Secure Computing in MEC Network// Expert Syst. Appl. -2022.- Vol.210. DOI 10.1016/j.eswa.2022.118394

18. Abdullah, Manal et al. Energy Efficient Ensemble K-means and SVM for Wireless Sensor Network. International //Inter.J. of Computers and Technology. -2013.- Vol.11(9).- P. 3034-3042. DOI10.24297/ijct.v11i9.3409

19. Desnitsky, V.; Kotenko, I.; Zakoldaev, D. Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices// Electronics. -2019. Vol. 8(5). DOI 10.3390/electronics8050500

20. Chhimwal, Mrs & Rawat, Deepesh. (2021). Comparison between Different Wireless Sensor Simulation Tools// IOSR Journal of Electronics and Communication Engineering. -2021. Vol.5(2).-P.54-60.

Information about the authors

E. Mardenov - Director of the Department of Information Technology at Astana International University, Research Fellow at Astana International Scientific Complex, Astana, Kazakhstan, e-mail: emardenov @gmail.com

Zh. Iztaev - Candidate of Pedagogical Sciences, Associate Professor at M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan, e-mail: Zhalgasbek71@mail.ru;

Hu Wen-Cen - Professor, M. Auezov South Kazakhstan State University, Leading Researcher at Astana International Scientific Complex, Astana, Kazakhstan,e-mail: qbcba@bk.ru;

D. Mardenova - Lecturer at Astana International University, Junior Research Fellow at Astana International Scientific Complex, Astana, Kazakhstan. e-mail: mardenovadana@gmail.com;

D. Baumuratova - PhD, Senior Lecturer at Astana International University, Junior Research Fellow at Astana International Scientific Complex, Astana, Kazakhstan. e-mail: dilaram_baumuratova@aiu.edu.kz

Сведения об авторах

Е.Марденов - директор департмаента информационных технологий Международного университета Астана, научный сотрудник Международного научного комплекса Астана, Астана, Казахстан, e-mail: emardenov@gmail.com;

Ж. Изтаев - Кандидат педагогических наук, доцент Южно-Казахстанский государственный университет им. М. Ауезова, Шымкент, Казахстан, e-mail: Zhalgasbek71@mail.ru;

Ху Вен-Цен - профессор · Южно-Казахстанский государственный университет им. М. Ауезова, ведущий научный сотрудник Международного научного комплекса Астана, Астана, Казахстан, e-mail: qbcba@bk.ru;

Д. Марденова - преподаватель Международного университета Астана, младший научный сотрудник Международного научного комплекса Астана, Астана, Казахстан, e-mail: mardenovadana@gmail.com;

Д. Баумуратова - PhD, старший преподаватель Международного университета Астана, младший научный сотрудник Международного научного комплекса Астана, Астана, Казахстан, e-mail: dilaram_baumuratova@aiu.edu.kz