ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№1
2026

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

1 (357)

JANUARY – MARCH 2026

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).
Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.
Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*
Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

COMPUTER SCIENCE

МАЗМҰНЫ

ИНФОРМАТИКА

СОДЕРЖАНИЕ

ИНФОРМАТИКА

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 1.
Namber 357 (2026). 461–475

https://doi.org/10.32014/2026.2518-1726.423

IRSTI 50.41.25
UDC 004.942

Zhukabayeva T.K.[1], Benkhelifa E.[2], Mardenov Y.M.[1], Baumuratova D.[1], Karabayev N.[1], 2026.
[1]L.N. Gumilyov Eurasian National University, Kazakhstan;
[2]Staffordshire University, UK.
E-mail: emardenov@gmail.com

DECISION SUPPORT FOR RESPONDING TO ATTACKS IN CYBER-PHYSICAL INDUSTRIAL INTERNET-OF-THINGS SYSTEMS

Zhukabayeva Tamara — Professor, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Kazakhstan,
E-mail: t.zhukabayeva@astanait.edu.kz, https://orcid.org/0000-0001-6345-5211;
Benkhelifa Elhadj — Professor, Digital, Tech, Innovation & Business, Staffordshire University, UK,
E-mail: e.benkhelifa@staffs.ac.uk, https://orcid.org/0000-0001-6168-2664;
Mardenov Yerik — Researcher, L.N. Gumilyov Eurasian National University, Astana International University, Kazakhstan,
E-mail: emardenov@gmail.com and https://orcid.org/0000-0001-9284-9797;
Baumuratova Dilaram — Researcher, PhD, L.N. Gumilyov Eurasian National University, Kazakhstan,
E-mail: baumuratova.d@gmail.com and https://orcid.org/0000-0001-6429-6435;
Karabayev Nurdaulet — Researcher, L.N. Gumilyov Eurasian National University, Kazakhstan,
E-mail: 020419501012@enu.kz and https://orcid.org/0000-0001-9284-9797.

Abstract. Industrial Internet-of-Things (IIoT) systems have emerged as a foundational technology underpinning a wide range of modern applications, including environmental monitoring, healthcare systems, industrial automation, and smart infrastructures. Their inherent advantages incorporate scalability, low energy consumption, intelligence and programmability, rapid data acquisition, reliability, low cost, and the absence of maintenance requirements. At the same time, they attract the attention of attackers, making the task of ensuring the security of such networks crucial. This study introduces a comprehensive decision support methodology for responding to cyberattacks in IIoT systems, including systems using edge computing principles, based on analytical modeling for the analysis of networks, attacks, and countermeasures. The methodology also employs machine learning, rules, and multi-criteria optimization for attack detection and countermeasure selection. It consists of three stages: data collection

on events occurring in the system, detection of attacks and anomalies, and selection of countermeasures for the identified attacks. Within the framework of the methodology, models of networks, attacks, and countermeasures, specific for IIoT systems, are presented. The main components and topology of IIoT systems are considered within the network model. The main types of attacks and possible countermeasures for IIoT systems are identified to specify the models of attacks and countermeasures. The algorithm for countermeasure selection within the proposed methodology based on rules and multi-criteria optimization and using the specified models is described. The application of the methodology is demonstrated through an example. The advantages and limitations of the proposed methodology are analyzed, and directions for future research are outlined.

Key words: IIoT systems, cyberattacks, countermeasures, decision support, response

For citations: Zhukabayeva T.K., Benkhelifa E., Mardenov Y.M., Baumuratova D., Karabayev N. Decision support for responding to attacks in cyber-physical industrial internet-of-things systems. Academic Scientific Journal of Computer Science, 2026. — No.1. – P. 461–475. DOI: https://doi.org/10.32014/2026.2518-1726.423

Financing. *This work by the staff of L.N. Gumilyov Eurasian National University is carried out with the financial support of the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489127).*

Жукабаева Т.К.[1], Бенхелифа Э.[2], Марденов Е.М.[1], Баумуратова Д.[1], Карабаев Н.[1], 2026.

[1]Л.Н. Гумилёв атындағы Еуразия ұлттық университеті, Астана, Қазақстан;
[2]Стаффордшир университеті, Ұлыбритания.
E-mail: emardenov@gmail.com

КИБЕРФИЗИКАЛЫҚ ӨНЕРКӘСІПТІК ИНТЕРНЕТ ЗАТТАРЫ ЖҮЙЕЛЕРІНДЕГІ ШАБУЫЛДАРҒА ӘРЕКЕТ ЕТУ КЕЗІНДЕ ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ

Жукабаева Тамара — профессор, ақпараттық технологиялар факультеті, Л.Н. Гумилёв атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail**:** t.zhukabayeva@astanait.edu, https://orcid.org/0000-0001-6345-5211;
Бенхелифа Эльхадж — профессор, Digital, Tech, Innovation & Business мектебі, Стаффордшир университеті, Ұлыбритания,
E-mail: e.benkhelifa@staffs.ac.uk, https://orcid.org/0000-0001-6168-2664;
Ерик Марденов — зерттеуші, Л.Н. Гумилёв атындағы Еуразия ұлттық университеті, Астана халықаралық университеті, Астана, Қазақстан,
E-mail: emardenov@gmail.com, https://orcid.org/0000-0001-9284-9797;

Диларам Баумуратова —PhD, Л.Н. Гумилёв атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
E-mail: baumuratova.d@gmail.com, https://orcid.org/0000-0001-6429-6435;
Нурдаулет Карабаев – зерттеуші, Л. Н. Гумилёв атындағы Еуразия ұлттық университеті, Астана, Казахстан,
Электронная почта: E-mail: 020419501012@enu.kz and https://orcid.org/0000-0001-9284-9797.

Аннотация. Өнеркәсіптік интернет заттары жүйелері (Industrial Internet of Things, IIoT) қоршаған ортаны мониторингтеу, денсаулық сақтау жүйелері, өнеркәсіптік автоматтандыру және ақылды инфрақұрылымдар сияқты заманауи қолданбалардың кең ауқымының негізін құрайтын базалық технологияға айналды. Олардың негізгі артықшылықтарына масштабталуы, төмен энергия тұтынуы, интеллектуалдылығы мен бағдарламалануы, деректерді жинаудың жоғары жылдамдығы, сенімділігі, төмен құны, сондай-ақ техникалық қызмет көрсетуді қажет етпеуі жатады. Сонымен қатар, мұндай жүйелер қаскөйлердің назарын өзіне аударады, бұл олардың қауіпсіздігін қамтамасыз ету мәселесінің өзектілігін арттырады. Осы зерттеуде IIoT жүйелеріндегі кибершабуылдарға әрекет ету кезінде шешім қабылдауды қолдауға арналған кешенді әдістеме ұсынылады, оның ішінде шеткі есептеу (edge computing) қағидаттарын қолданатын жүйелер де қамтылған. Әдістеме желілерді, шабуылдарды және қарсы шараларды талдауға арналған аналитикалық модельдеуге негізделген, сондай-ақ шабуылдарды анықтау және қарсы шараларды таңдау үшін машиналық оқыту әдістерін, ережелерді және көпкритерийлі оңтайландыруды пайдаланады. Ұсынылған әдістеме үш кезеңнен тұрады: жүйеде орын алатын оқиғалар туралы деректерді жинау; шабуылдар мен аномалияларды анықтау; анықталған шабуылдар үшін қарсы шараларды таңдау. Әдістеме аясында IIoT жүйелеріне тән желілердің, шабуылдардың және қарсы шаралардың модельдері ұсынылған. Желілік модельде IIoT жүйелерінің негізгі компоненттері мен топологиясы қарастырылады. Шабуылдар мен қарсы шаралар модельдерін нақтылау үшін IIoT ортасына тән негізгі шабуыл түрлері мен ықтимал қарсы әрекеттер айқындалған. Әзірленген модельдерді қолдана отырып, ережелер мен көпкритерийлі оңтайландыруға негізделген қарсы шараларды таңдау алгоритмі сипатталған. Әдістеменің қолданылуы практикалық мысал арқылы көрсетілген. Ұсынылған тәсілдің артықшылықтары мен шектеулері талданып, болашақ зерттеулердің негізгі бағыттары айқындалған.

Түйін сөздер: IIoT жүйелері, кибершабуылдар, қарсы шаралар, шешім қабылдауды қолдау, әрекет ету

Жукабаева Т.К.[1], Бенхелифа Э.[2], Марденов Е.М.[1], Баумуратова Д.[1], Карабаев Н.[1], 2026.
[1]Евразийский национальный университет имени Л.Н. Гумилёва,
Астана, Казахстан;
[2]Стаффордширский университет, Великобритания.
E-mail: emardenov@gmail.com

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПРИ РЕАГИРОВАНИИ НА АТАКИ В КИБЕРФИЗИЧЕСКИХ ПРОМЫШЛЕННЫХ СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Жукабаева Тамара — профессор, факультет информационных технологий, Евразийский национальный университет имени Л. Н. Гумилёва, Казахстан,
E-mail**:** t.zhukabayeva@astanait.edu, https://orcid.org/0000-0001-6345-5211;
Эльхадж Бенхелифа — профессор, Digital, Tech, Innovation & Business, Стаффордширский университет, Великобритания
E-mail: e.benkhelifa@staffs.ac.uk, https://orcid.org/0000-0001-6168-2664;
Ерик Марденов — исследователь, Евразийский национальный университет имени Л.Н. Гумилёва, Международный университет Астана, Казахстан,
E-mail: emardenov@gmail.com, https://orcid.org/0000-0001-9284-9797;
Диларам Баумуратова — исследователь, PhD, Евразийский национальный университет имени Л.Н. Гумилёва, Казахстан
E-mail: baumuratova.d@gmail.com, https://orcid.org/0000-0001-6429-6435;
Нурдаулет Карабаев — исследователь, Евразийский национальный университет имени Л.Н. Гумилёва, Казахстан,
Электронная почта: E-mail: 020419501012@enu.kz and https://orcid.org/0000-0001-9284-9797.

Аннотация. Промышленные системы интернета вещей (Industrial Internet of Things, IIoT) являются базовой технологией, лежащей в основе широкого спектра современных приложений, включая промышленную автоматизацию, системы мониторинга, здравоохранение и интеллектуальную инфраструктуру. Ключевыми преимуществами IIoT являются масштабируемость, энергоэффективность, высокая скорость обработки данных, программируемость и надёжность. Вместе с тем такие системы представляют собой привлекательную цель для кибератак, что обусловливает необходимость разработки эффективных методов обеспечения их безопасности. В исследовании предложена комплексная методология поддержки принятия решений при реагировании на кибератаки в системах IIoT, включая среды с использованием пограничных вычислений (edge computing). Методология основана на аналитическом моделировании сетей, атак и контрмер, а также включает методы машинного обучения, экспертные правила и подходы многокритериальной оптимизации для обнаружения атак и выбора оптимальных мер реагирования. Предложенная методология включает три основных этапа: сбор и анализ данных о событиях в системе, обнаружение атак и аномалий, а также выбор контрмер для нейтрализации выявленных угроз. В рамках исследования разработаны модели сетевой

архитектуры, типов атак и соответствующих контрмер, характерных для IIoT-среды. Описан алгоритм выбора контрмер, основанный на правилах и многокритериальной оптимизации с использованием предложенных моделей. Практическое применение методологии продемонстрировано на прикладном примере. Проведён анализ преимуществ и ограничений предложенного подхода, а также определены направления для дальнейших исследований.

Ключевые слова: системы IIoT, кибератаки, контрмеры, поддержка принятия решений, реагирование

Introduction and Related Work. IIoT systems are spatially distributed sensor nodes capable of collecting data, processing it, and interacting via wireless channels (Tossa et al., 2025). At present, they are applied in smart home management, transportation and logistics, industry, agriculture, environmental monitoring, urban surveillance, entertainment, healthcare, and energy, as well as in security and battlefield monitoring (Kardi et al., 2019).

«Ideal» IIoT systems are scalable, consume little energy, are intelligent and programmable, provide rapid data acquisition, are reliable, low-cost, and require no maintenance. However, they also attract the attention of attackers. In particular, passive attacks those aimed at stealing information on IIoT systems are discussed in (Keerthika et al., 2021) (eavesdropping and traffic analysis). Active attacks those aimed at damaging the network by altering or replacing data are considered in (Verma et al., 2022) (denial of service), (Sánchez et al., 2021) (masquerade attack), (Hu et al., 2022) (replay attack), (Hu et al., 2014) (selective forwarding attack), (Sujihelen et al., 2022) (node replication), (Al-Ahmadi et al., 2022) (wormhole attack), (Faris et al., 2023) (Sybil attack), (Teng et al., 2023) (sinkhole attack), (Allimuthu et al., 2022) (rushing attack), and (Beddoe et al., 2013) (message modification). The types of attacks on IIoT systems are further classified in (Keerthika et al., 2021) and (Verma et al., 2020).

One of the key challenges in deploying IIoT systems is ensuring cybersecurity (Jadhav et al., 2017). Possible countermeasures are outlined in (Turakulovich et al., 2019) and (Mamdouh et al., 2018). Among them are security measures that should be incorporated during the system design stage, such as the use of secure data transmission protocols (Turakulovich et al., 2019) (such measures for all identified attacks are discussed in (Keerthika et al., 2021)). However, these alone cannot completely eliminate the possibility of a successful attack. Therefore, it is also necessary to integrate protection mechanisms into the system that enable the detection of cyberattacks and the implementation of countermeasures, for example, through the use of machine learning (Mamdouh et al., 2018). This study focuses on decision support issues based on such protection mechanisms.

This paper proposes a decision support methodology for responding to cyberattacks in IIoT systems, based on analytical modeling for simulating the system, attacks, and countermeasures; machine learning for attack detection; rules

and multi-criteria optimization for countermeasure selection. The application of the methodology is demonstrated through an example. The advantages and limitations of the proposed methodology are analyzed, and directions for future research are outlined. Thus, the main contributions of this research are as follows: (1) a decision support methodology for responding to cyberattacks in IIoT systems, based on analytical modeling, machine learning, and rules and multi-criteria optimization; (2) analytical models of system, attacks, and countermeasures considering specificity of IIoT systems, and considering the types of attacks and appropriate countermeasures; (3) algorithm for countermeasure selection based on rules and multi-criteria optimization and using the specified models; (4) demonstration of applicability of the proposed methodology on the toy example.

The paper is organized as follows. Relevant studies are briefly reviewed in the introduction. Section 2 presents the key definitions and problem statement. Section 3 describes the proposed decision support methodology for responding to cyberattacks in IIoT systems. Section 4 provides an example of the methodology's application and a discussion.

Materials and Methods

IIoT systems. A IIoT system can be formalized as follows:

$$IS = <N, C>, \quad (1)$$

where

N – nodes,

C – wireless links between them.

A node consists of core and additional components (Tossa et al., 2025). The core components include:

Data acquisition component (consisting of a physical sensing device that collects data from the local environment and an Analog-to-Digital Converter, ADC) collects analog data from the local environment and converts it into a digital format understandable by the processor,

Data processing component, including ones using edge computing (a processor complemented with Random Access Memory) manages the operation of other components and analyzes/processes the data obtained from the data acquisition component,

Communication component (which can be optical or radio-frequency) transmits and receives data in the wireless medium,

Power supply component (a small, limited-capacity battery).

The additional components may include GPS (Global Positioning System), a mobility system, and an energy generator.

According to (Tossa et al., 2025), depending on the application domain and architecture, the following types of nodes are distinguished:

Standard node includes a data transmission component and a data processing component;

Sensor node (source) a standard node with a data acquisition or detection component;

Actuator node a standard node with a component for performing specific mechanical tasks;

Gateway a standard node that relays traffic into the network;

Base station a standard node with a serial converter connected to a second communication component for relaying data from nodes to users or other networks

Various architectures of IIoT systems are distinguished, including:

Flat architecture all nodes have equal energy, computing resources, and memory, perform identical roles, and each node can interact with any other,

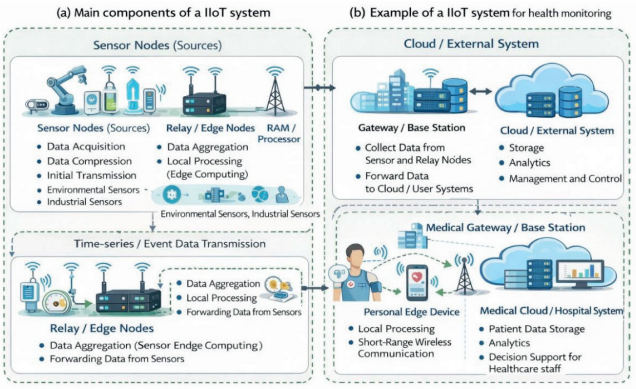
Hierarchical architecture nodes possess different resources and perform different roles, and Multitier architecture a hierarchical architecture in which nodes are grouped into clusters according to their functionality.

Depending on the architecture, the role of each network node is defined: source, relay, or data collection node. Typically, a IIoT system consists of a base station (data collection node) interacting with multiple sensors (sources and relays) (hierarchical architecture). A sensor (source) collects data, compresses it, and transmits it to the base station (data collection node) either directly or through other sensors (relays). The base station forwards the data to the system. An example of such an architecture is shown in Figure 1 (a - main components of a IIoT system and the connections between them, b - an example of a IIoT system for health monitoring).

The following features of IIoT systems are significant for developing a decision support methodology for responding to cyberattacks in such systems:

Heterogeneity in terms of energy sources, data processing capabilities, communication ranges, and sensing modalities, which complicates the deployment process of IIoT systems;

Constraints related to network lifetime, coverage, energy/memory/ computational resources, and data transmission time.

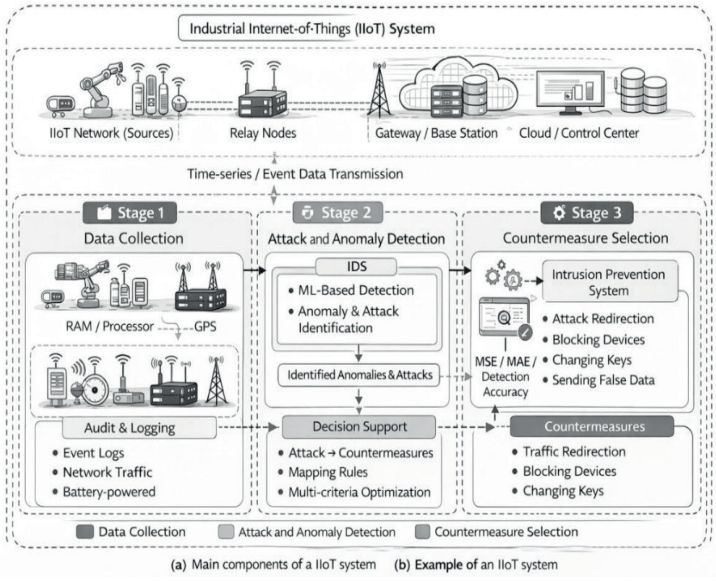


a) Main components of a IIoT system b) Example of a IIoT system for health monitoring

Figure 1 – Hierarchical architecture of a IIoT system.

Problem Statement of the Study. Given: a IIoT system (IS), a set of events – E, a set of attacks on the IS – A, a set of security mechanisms – SMP, and a set of countermeasures – CM. It is necessary to develop a decision support methodology for responding to cyberattacks in IIoT systems that enables the mapping of the set of attacks A onto the set of countermeasures CM: F: A → CM, taking into account resource and privilege constraints.

Decision Support for Responding to Cyberattacks in IIoT systems. The proposed decision support methodology for responding to cyberattacks in IIoT systems is based on analytical modeling for simulating the system, attacks, and countermeasures; machine learning for attack detection; rules; and multi-criteria optimization for countermeasure selection. The methodology consists of three stages: data collection on events occurring in the system, detection of attacks and anomalies, and selection of countermeasures for the identified attacks (Figure 2).



a) Main components of a IIoT system b) Example of an IIoT system

Figure 2 – Decision support methodology for responding to cyberattacks.

For data collection, it is proposed to implement auditing and logging; for detecting attacks and anomalies an intrusion detection system based on machine learning; and for countermeasure selection an intrusion prevention system based on rules and multi-criteria optimization.

Models. First, we define a set of models based on the relationships between the objects and subjects involved in the decision-making process, including network objects (nodes and links between them), their vulnerabilities and weaknesses, known exploits and attacks, incidents, as well as countermeasures (Figure 3). In the event of a security incident, protection mechanisms which may be network objects

or components of such objects are employed to implement countermeasures (for example, a firewall can be used to block a connection).

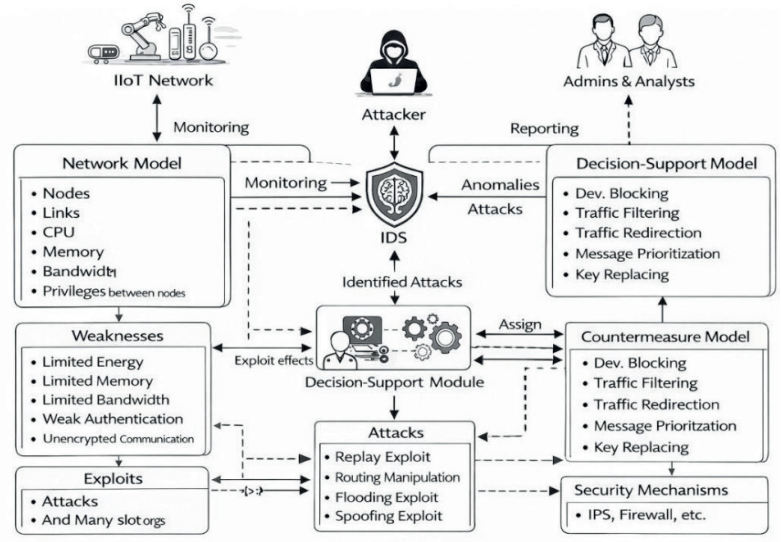


Figure 3 – Relationships between objects and subjects involved in the decision-making process for response.

Thus, it is necessary to extend the set of possible node roles in the network with security mechanisms, such as intrusion detection and prevention systems (Figure 4).

To account for the possible roles of network nodes as well as embedded security mechanisms, we define the elements of the network model from Equation 1 ($IS = <N, C>$) as follows:

N – network nodes, $N = \{\cup_i n_i\}$, where i – number of system node, $n_i = <name, role, SM>$, where name is the node identifier, role is the node's role determining available resources (energy, memory, computing capacity) and privileges (user/administrator/owner), and SM denotes the security mechanisms available for this node, $SM = \{\cup_i sm_i\}$, where i – number of security mechanism, $sm_i = <name, CM>$, where CM – the set of countermeasures related to the security mechanism sm_i;

C – wireless and wired links between them, $C = <prot, trCh>$, where *prot* is the transmission protocol, and *trCh* is the bandwidth.

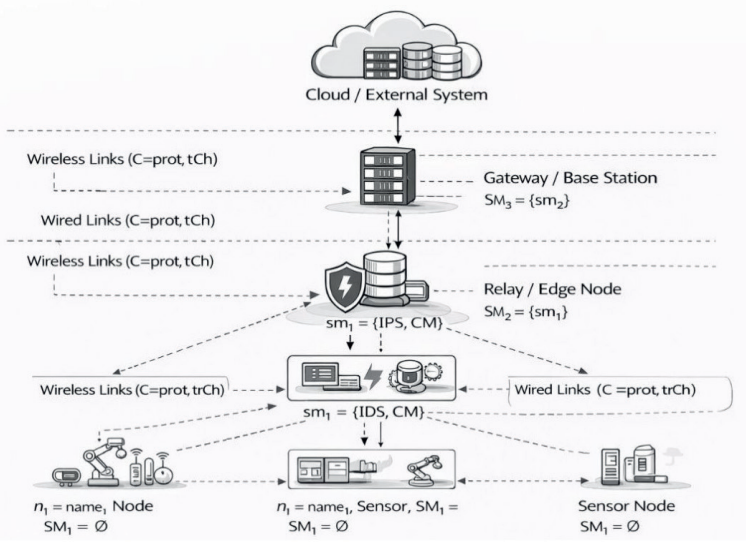


Figure 4 – Hierarchical architecture of a IIoT system with security mechanisms.

To identify possible security mechanisms and countermeasures, it is necessary to define the potential attacks. In (Shahzad et al., 2017), the authors highlight the following threats to IIoT systems and their corresponding attacks:

Confidentiality threat (unauthorized access to information; in IIoT system terms a message transmitted over the wireless network can be read and understood by an attacker): Eavesdropping (information gathering from carriers, wiretapping, interception of electromagnetic/radio frequency signals, traffic analysis, staff negligence), Interaction (data theft, replay attack, masquerade attack, integrity violation, man-in-the-middle attack, bypassing security mechanisms, physical intrusion, authorization violation), System compromise (trapdoor attack, Trojan attack, service spoofing, viruses/worms).

Integrity threat (unauthorized modification or theft of information; in IIoT system terms a message transmitted over the network is altered or forged): Modification (denial, interception/modification), Interaction (see above), System compromise (see above).

Availability threat (denial of service or prevention of authorized access; in IIoT system terms – inability to transmit a message or for a node to use resources): Denial of Service (integrity violation, resource exhaustion), Interaction (see above), System compromise (see above).

Non-repudiation threat (denial of an action that has occurred or claiming that an action has not occurred; in IIoT system terms providing information to an unauthorized/unauthenticated or fake sensor): Reposting, Theft/modification, Interaction (see above), System compromise (see above).

In (Shahzad et al., 2017), the authors highlight the following possible security measures and countermeasures according to the types of threats:

Confidentiality (counteracting unauthorized access to information): passwords and certificates (key and certificate management must be ensured), firewalls with access control lists, auditing and logging, intrusion detection systems, antivirus/spyware software.

Integrity (counteracting unauthorized modification or theft of information): passwords and certificates (key and certificate management must be ensured; compared to confidentiality measures, digital signatures and checksums are additionally introduced), firewalls with access control lists, auditing and logging, intrusion detection systems, antivirus/spyware software.

Availability (counteracting denial of service or prevention of authorized access): backup during and recovery after an attack, security and vulnerability incident reporting, bandwidth limitation, access management, firewalls with access control lists, auditing and logging, backups and recovery, intrusion detection systems, antivirus/spyware software, network and system management.

Non-repudiation (counteracting denial that an action took place or claims that it did not): passwords and certificates (key and certificate management must be ensured), auditing and logging (for legal proceedings).

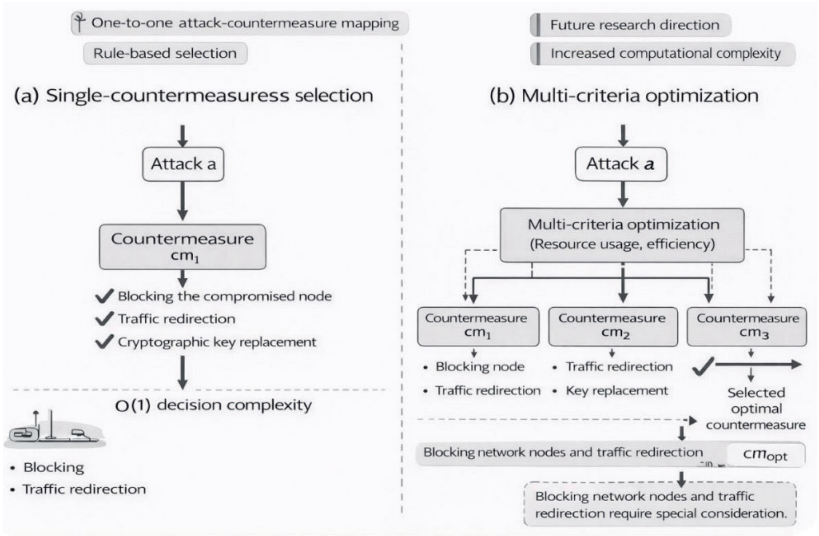


Figure 5 – Comparison of single-countermeasure selection and multi-criteria optimization in the proposed decision-support methodology.

The security mechanisms applied during the operational phase include:

• Firewalls with access control lists (measures: blocking access to a specific node, blacklisting, message prioritization, bandwidth limitation, and traffic redirection),

• Audit and logging (a passive measure, i.e., used for data collection but not involved in supporting response decision-making),

• Intrusion detection systems (a passive measure, i.e., used for detecting attacks but not involved in supporting response decision-making, performing monitoring to identify attacks and anomalies),

• Antivirus/anti-spyware software (blocking malicious software),

• Network and system management (access control, bandwidth limitation).

Within the intrusion prevention subsystem of the security system (Figure 4), it is proposed to implement the selection of countermeasures for different types of attacks based on rules, using Table 1 (Keerthika et al., 2021).

Table 1 – Countermeasures in IIoT systems

Attack	**Threat to**	**Countermeasures**
Denial of Service (Verma et al., 2022)	availability	message prioritization
Jamming	availability	Spread spectrum, region mapping and traffic redirection
Physical Attack	availability	traffic redirection
Spoofing, Routing Information Forgery	availability, integrity, confidentiality, non-repudiation	Block compromised node and reconnect, change key
Selective Forwarding (Hu et al., 2014)	availability	traffic redirection
Sink Hole Attack (Teng et al., 2023)	availability	Block compromised node and redirect traffic
Black Hole Attack	availability, integrity, confidentiality, non-repudiation	traffic redirection
Sybil Attack (Faris et al., 2023)	availability, integrity, confidentiality, non-repudiation	Block nodes and redirect traffic
Wormhole Attack (Al-Ahmadi et al., 2022)	availability, integrity, confidentiality, non-repudiation	traffic redirection
HELLO Flood Attack	availability	message prioritization, traffic redirection
Acknowledgment Spoofing (Verma et al., 2020)	integrity, confidentiality, non-repudiation	Block fake node, reconnect with legitimate node, change key
Neglect and Greed Attack (Verma et al., 2020)	availability	Recover message transmission algorithm
Homing Attack (Verma et al., 2020)	confidentiality	Collect information, encryption
Node Takeover Attack	availability, integrity, confidentiality, non-repudiation	Block fake node, reconnect with legitimate node, change key
Node Failure Attack	availability	traffic redirection, restore node
Monitoring and Eavesdropping (Keerthika et al., 2021)	confidentiality	Collect information, encryption
Traffic Analysis (Keerthika et al., 2021)	confidentiality	Collect information, encryption
Attacker Masking	availability, integrity, confidentiality, non-repudiation	Collect information, encryption, restore message transmission algorithm

Node Replication (Sujihelen et al., 2022)	integrity	Block fake node, reconnect with legitimate node, change key
False Knot	availability	Block fake node, reconnect with legitimate node, change key
Replay Attack (Hu et al., 2022)	confidentiality, non-repudiation	Blocking fake node, reconnect with legitimate node, change key
Rushing Attack (Allimuthu et al., 2022)	availability	Blocking fake node, restoring message transfer algorithm, change key
Vampire Attack	Threat to	Replacing nodes, redirecting traffic

Considering Table 1, let us introduce two additional models: the attack model and the countermeasure model. The attack model is defined as:

$A = \{\cup_i a_i\}$, where i – number of attack, $a_i = <type, n_j>$, where type – type of attack, n_j – attacked network objects.

The countermeasure model is defined as:

$CM = \{\cup_i cm_i\}$, where i – number of countermeasure, $cm_i = <name, Pr, R>$, where *name* – name of the countermeasure, *Pr* – required privileges, *R* – required resources.

Algorithm. Since the number of countermeasure options for each type of attack is relatively small, the following rule-based algorithm is proposed for the countermeasure selection stage of the decision-support methodology:

Input data: *IS* system, attack *a*.

1. Map *a* to the *IS* using *n*.

2. Select all *cm* for *a* : *CM* <- *cm* #using rules defined on the basis of Table 1.

3. Map *CM* to countermeasures in *SM* : *CM_lim* #to define available countermeasures.

4. From *CM_lim*, select the optimal *CM_opt* considering *Pr* and *R*.

Output data: countermeasures *CM_opt*.

Results. Let us consider the application of the methodology using a simple example. Suppose that the network shown in Figure 1(b) is subjected to a spoofing attack or a routing information spoofing attack. A security system is deployed in the network (as shown in Figure 4). The implementation of the methodology proceeds as follows:

Stage 1. Based on the information collected by the auditing and logging component, the intrusion detection system uses machine learning to identify an attack or anomaly, namely, a routing information spoofing attack. It reveals that one of the sensor nodes *n* is malicious.

Stage 2. Using Algorithm 1 (*IIoT* system and attack *a* are input data). On the 1st step map *a* to the IIoT system using *n*. The output of this step is malicious node $n = <name, role, SM>$.

On the second step the countermeasures *cm* against *a* are determined using rules defined on the basis of Table 1: IF "a routing information spoofing attack" THEN action "Blocking the compromised node and redirecting traffic, key replacement.". There is only one response option *cm* "Blocking the compromised node and redirecting traffic, key replacement.". Step 3 of the algorithm consists in mapping *cm* to countermeasures in *SM* and obtaining *CM_lim = cm*. Step 4 is skipped as soon as there is only on countermeasure cm in the *CM lim* list. Implementation of this measure *cm* only requires administrator rights and user interaction for key replacement. Thus, final list of countermeasures *CM_opt* contains one countermeasure "Blocking the compromised node and redirecting traffic, key replacement." For implementation against the detected routing information spoofing attack.

Discussion. For the system to operate effectively, it is necessary to implement data collection and processing, as well as methodologies for detecting attacks and anomalies. Machine learning–based methods, such as those described in (Ahmad et al., 20122), have demonstrated good performance. This constitutes one of the directions for future research.

At present, most attacks in Table 1 have only one corresponding countermeasure, which does not require additional optimization in terms of resource usage and efficiency, and ensures low algorithmic complexity of O (1). It should be noted that the methodology can be easily extended with new countermeasures. In such cases, a multi-criteria optimization algorithm will be required to select the most suitable countermeasure, which also represents a future research direction.

In addition, algorithms for blocking network nodes and redirecting traffic deserve special attention.

Conclusion.

This study addressed the problem of decision support for responding to cyberattacks in IIoT systems. The architecture and key features of IIoT systems were analyzed. The main types of attacks and possible countermeasures were identified. A decision support methodology for responding to cyberattacks in IIoT systems was proposed, based on analytical modeling of the system, attacks, and countermeasures; machine learning for attack detection; rules; and multi-criteria optimization for countermeasure selection. Within the methodology, models of the system, attacks, and countermeasures, as well as an algorithm for countermeasure selection, were developed. The application of the methodology was demonstrated on a test example. Future work will focus on implementing attack and anomaly detection based on machine learning, analyzing the specifics of multi-criteria optimization in countermeasure selection, and examining in greater detail measures and algorithms related to traffic redirection.

References

Ahmad R., Wazirali R., & Abu-Ain T. (2022) Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors, 22(13), — 4730 p. https://doi.org/10.3390/s22134730(in Eng.)

Al-Ahmadi S. (2022) A Novel Energy-efficient Wormhole Attack Prevention Protocol for WSN based on Trust and Reputation Factors. Proceedings of the 11th International Conference on Sensor Networks. — P. 191–201. https://doi.org/10.5220/0010951400003118 (in Eng.)

Allimuthu U., & Mahalakshmi K. (2022) Efficient Mobile Ad Hoc Route Maintenance Against Social Distances Using Attacker Detection Automation. Mobile Networks and Applications, 28(1). — P. 128–159. https://doi.org/10.1007/s11036-022-02040-3 (in Eng.)

Beddoe M.A., & Guruswamy K. (2013) *U.S. Patent No. 8,601,585*. Washington, DC: U.S. Patent and Trademark Office.

Faris M., Mahmud M.N., Salleh, M.F.M., & Alnoor A. (2023). Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management, 15. https://doi.org/10.1177/18479790231157220 (in Eng.)

Hu B., Tang W., & Xie Q. (2022) A two-factor security authentication scheme for wireless sensor networks in IoT environments. Neurocomputing, 500, 741–749. https://doi.org/10.1016/j.neucom.2022.05.099 (in Eng.)

Hu Y., Wu Y., & Wang H. (2014) Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN. Wireless Sensor Network, 06(11). — P. 237–248. https://doi.org/10.4236/wsn.2014.611023 (in Eng.)

Jadhav R., & V., V. (2017) Security Issues and Solutions in Wireless Sensor Networks. International Journal of Computer Applications, 162(2), 14–19. https://doi.org/10.5120/ijca2017913256 (in Eng.)

Kardi A., & Zagrouba R. (2019) Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal, 4(6). — P. 229–243. https://doi.org/10.25046/aj040630 (in Eng.)

Keerthika M., & Shanmugapriya D. (2021) Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Global Transitions Proceedings, 2(2). — P. 362–367. https://doi.org/10.1016/j.gltp.2021.08.045 (in Eng.)

Mamdouh M., I. Elrukhsi M.A., & Khattab A. (2018) Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey. 2018 International Conference on Computer and Applications (ICCA). — P. 215–218. https://doi.org/10.1109/comapp.2018.8460440 (in Eng.)

Sánchez J.D.V., Urquiza-Aguiar L., Paredes M.C.P., & Osorio D.P.M. (2020) Survey on physical layer security for 5G wireless networks. Annals of Telecommunications, 76(3–4). — P. 155–174. https://doi.org/10.1007/s12243-020-00799-8 (in Eng.)

Shahzad F., Pasha M., & Ahmad A. (2017) A survey of active attacks on wireless sensor networks and their countermeasures. arXiv Preprint. https://doi.org/10.48550/arXiv.1702.07136 (in Eng.)

Sujihelen L., Boddu R., Murugaveni S., Arnika Ms., Haldorai A., Reddy P.C.S., Feng S., & Qin J. (2022) Node Replication Attack Detection in Distributed Wireless Sensor Networks. Wireless Communications and Mobile Computing, 2022(1). Portico. https://doi.org/10.1155/2022/7252791 (in Eng.)

Teng Z., Li M., Yu L., Gu J., & Li M. (2023) Sinkhole Attack Defense Strategy Integrating SPA and Jaya Algorithms in Wireless Sensor Networks. Sensors, 23(24). — 9709 p. https://doi.org/10.3390/s23249709 (in Eng.)

Tossa F., Faga Y., Abdou W., Ezin E.C., & Gouton P. (2025) Wireless Sensor Network Deployment: Architecture, Objectives, and Methodologies. Sensors, 25(11). — 3442 p. https://doi.org/10.3390/s25113442 (in Eng.)

Turakulovich K.Z., & Tokhirovich S.L. (2019) Analysis of Security Protocols in Wireless Sensor Networks. 2019 International Conference on Information Science and Communications Technologies (ICISCT). — P. 1–4. https://doi.org/10.1109/icisct47635.2019.9012015 (in Eng.)

Verma R., & Bharti S. (2020) A Survey of Network Attacks in Wireless Sensor Networks. Information, Communication and Computing Technology. — P. 50–63. https://doi.org/10.1007/978-981-15-9671-1_4 (in Eng.)

Verma V., & Jha V.K. (2022) A Survey of Recent Research Methodologies for the Security Provisioning in Wireless Sensor Networks. International Journal of Information Security and Assurance Engineering, (IJISAE). (in Eng.)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Ответственный редактор *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Т. Апендиев*
Верстка на компьютере: *Г.Д. Жадырановой*

Подписано в печать 31.03.2026.
Формат 60x881/8.
20,0 п.л. Заказ 1.

«Central Asian Academic Research Center» LLP
Алматы, Шевченко к-сі, 28