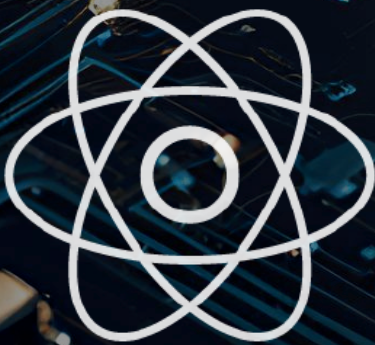


# JOURNAL OF ENGINEERING RESEARCH & SCIENCES

# JENRS



[www.jenrs.com](http://www.jenrs.com)  
ISSN: 2831-4085

**Volume 3 Issue 5**  
**May 2024**

# EDITORIAL BOARD

## Editor-in-Chief

**Prof. Paul Andrew**  
Universidade De São Paulo, Brazil

## Editorial Board Members

**Dr. Jianhang Shi**

Department of Chemical and Biomolecular Engineering, The Ohio State University, USA

**Dr. Sonal Agrawal**

Rush Alzheimer's Disease Center, Rush University Medical Center, USA

**Dr. Unnati Sunilkumar Shah**

Department of Computer Science, Utica University, USA

**Prof. Anle Mu**

School of Mechanical and Precision Instrument Engineering, Xi'an University of Technology, China

**Dr. Xuejun Qian**

Great Lakes Bioenergy Research Center (QLBRC), University of Wisconsin-Madison, USA

**Dr. Qiong Chen**

Navigation College, Jimei University, China

**Dr. Jianhui Li**

Molecular Biophysics and Biochemistry, Yale University, USA

**Dr. Lixin Wang**

Department of Computer Science, Columbus State University, USA

**Dr. Prabhash Dadhich**

Biomedical Research, CellfBio, USA

**Dr. Żywiołek Justyna**

Faculty of Management, Czestochowa University of Technology, Poland

**Dr. Anna Formica**

National Research Council, Istituto di Analisi dei Sistemi ed Informatica, Italy

**Prof. Kamran Iqbal**

Department of Systems Engineering, University of Arkansas Little Rock, USA

**Dr. Ramcharan Singh Angom**

Biochemistry and Molecular Biology, Mayo Clinic, USA

**Dr. Qichun Zhang**

Department of Computer Science, University of Bradford, UK

**Dr. Mingsen Pan**

University of Texas at Arlington, USA

**Ms. Madhuri Inupakutika**

Department of Biological Science, University of North Texas, USA

## Editorial

In the rapidly evolving landscape of technology and global trade, innovative research continues to drive advancements and address critical challenges. This editorial highlight three significant papers that contribute to the fields of customs clearance, cybersecurity, and next-generation communication systems. Each paper offers unique insights and solutions, demonstrating the importance of interdisciplinary research in fostering progress and enhancing practical applications.

There is a complex process of customs clearance in foreign trade, presenting a mathematical model to improve control and efficiency. By examining existing methods for solving linear programming problems with variable coefficients and studying customs risks, the authors propose a novel approach using threshold matrices. This method aids in identifying reliability risks, and the development of a control algorithm for customs values further underscores the practical implications of this research. The results showcase the potential for improved accuracy and reliability in customs processes, offering valuable tools for practitioners [1].

The growing sophistication of phishing attacks, focusing on the browser-in-the-browser (BitB) technique. This novel attack exploits single sign-on popups to deceive users and steal credentials. Through comprehensive analysis and experimental scenarios from both attacker and victim perspectives, the study highlights the technical intricacies and social engineering tactics employed in BitB attacks. The authors propose effective countermeasures to detect and mitigate these attacks, filling a critical gap in cybersecurity research. This pioneering study enhances awareness and provides practical strategies for protecting sensitive information [2].

The advancements and challenges of 5G and 6G communication systems, emphasizing the role of optical wireless communication (OWC) technologies. The authors discuss the superior capabilities of 6G over 5G in terms of capacity, connectivity, latency, security, energy efficiency, user experience, and reliability. The integration of IoT and the tactile internet presents additional complexities, necessitating innovative solutions. OWC technologies, such as Visible Light Communication (VLC), Light Fidelity (LiFi), Optical Camera Communication (OCC), and Free Space Optics (FSO), are identified as promising candidates to meet these demands. This comprehensive review underscores the potential of OWC technologies in the successful deployment of 5G/6G and IoT systems, providing a roadmap for future research and development [3].

In summary, these three papers collectively contribute to enhancing global trade processes, strengthening cybersecurity defenses, and advancing communication technologies. The innovative solutions and practical applications presented in each study underscore the importance of continuous research and development in addressing contemporary challenges. As technology and global trade continue to evolve, such interdisciplinary research will play a crucial role in shaping a more efficient, secure, and connected world.

### References:

- [1] I. Mukhtorov, T. Abduraxmonov, A. Saidov, "Mathematical Model of Optimum Management of the Customs Control Process and Expert System for Ensuring Data Reliability," *Journal of Engineering Research and Sciences*, vol. 3, no. 5, pp. 1–13, 2024, doi:10.55708/js0305001.
- [2] K. Alessa, B. Alhetelah, G. Alazman, A. Bader, N. Alhomeed, L. Almubarak, F. Almulla, "Browser-in-the-Browser (BitB) Attack: Case Study," *Journal of Engineering Research and Sciences*, vol. 3, no. 5, pp. 14–22, 2024, doi:10.55708/js0305002.

- [3] R. Khalid, M. Naqi Raza, "Analyzing the Impact of Optical Wireless Communication Technologies on 5G/6G and IoT Solutions: Prospects, Developments, and Challenges," *Journal of Engineering Research and Sciences*, vol. 3, no. 5, pp. 23–36, 2024, doi:10.55708/js0305003.




**Editor-in-chief**

**Prof. Paul Andrew**

## CONTENTS

<i>Mathematical Model of Optimum Management of the Customs Control Process and Expert System for Ensuring Data Reliability</i> Ilkhom Mukhtorov, Takhir Abduraxmonov, Abdusobir Saidov	01
<i>Browser-in-the-Browser (BitB) Attack: Case Study</i> Khalid Alissa, Bushra Alhetelah, Ghadeer Alazman , Asma Bader, Noor Alhomeed , Layan Almubarak , Fajer Almulla	14
<i>Analyzing the Impact of Optical Wireless Communication Technologies on 5G/6G and IoT Solutions: Prospects, Developments, and Challenges</i> Ramsha Khalid, Muhammad Naqi Raza	23

# Mathematical Model of Optimum Management of the Customs Control Process and Expert System for Ensuring Data Reliability

Ilkhom Mukhtorov<sup>1</sup>, Takhir Abduraxmonov<sup>2</sup>, Abdusobir Saidov<sup>\*,3</sup>

<sup>1</sup>Customs Committee of the Republic of Uzbekistan, First Deputy Chairman, Tashkent, Uzbekistan

<sup>2</sup>Customs Committee of the Republic of Uzbekistan, of Information and Communication Technologies and Cybersecurity, Tashkent, Uzbekistan

<sup>3</sup>Customs Institute, Department of Information Technology and Mathematics, Tashkent, Uzbekistan

\*Corresponding author: Abdusobir Saidov, 100017, Chilanzar block, 20-17-6, Tashkent, Uzbekistan, Email: [abdusobir59@gmail.com](mailto:abdusobir59@gmail.com)

**ABSTRACT:** The article considers the issue of modeling the multi-step process of customs clearance of goods in foreign trade. A mathematical model of control of the process under consideration has been developed. A brief review of existing methods for solving the linear programming problem with variable coefficients of the target function is given. The essence of customs risks has been studied and a method for identifying customs risks of reliability using threshold matrixes has been proposed. An algorithm for controlling the reliability of the customs value of goods is developed and the results of the implementation of this algorithm are given

**KEYWORDS:** customs clearance, mathematical modeling, linear optimization, objective function with a variable coefficient, customs risks, threshold matrix, reliability criteria

## 1. Introduction

International trade has long been considered the fundamental form of international economic relations. The pace of globalization in the first quarter of the XXI century confirms the role of international trade as the main driver of socio-economic development of countries. Analysis of the dynamics of international trade in the period from 2000 to 2015 shows that the export of developed countries increased from \$4.243212 trillion to \$8.613816 trillion (+103.00%), developing countries - from \$2.059532 trillion to \$7.344534 trillion (+256, 61%), countries with economies in transition - from 149.573 billion dollars to 525.571 billion dollars (+251.38%). On average, the volume of exports of world trade goods increased by 254.2% [1].

At the same time, the customs services of the countries participating in international trade play an important role in the international supply chain. There is a theory in the scientific literature, according to which any customs system successively passes several separate phases of its activity, characterized by the specificity of its relations both with foreign trade participants and with the state. Today, the customs systems of developed countries are in the "customs for foreign trade participants" phase, while for most developing countries the "customs for the government" phase is characteristic, and in a number of disadvantaged and underdeveloped countries, the "customs for themselves" phase is observed. [2].

Conversely, the faster a country's customs service approaches the "customs for foreign trade participants" phase of development, the faster the country approaches the level of developed countries. Today, the development of the activities of the customs service of each country is possible only through the use of modern information and communication technologies. Therefore, such requirements are imposed to the methods of customs service management as orientation of models on artificial intelligence, possibility of synthesis of adaptive control system and application to complex analysis of multilevel system.

From this point of view, the task of optimal management of the process of organizing customs control and customs clearance of non-trading goods is relevant.

## 2. The problem of optimal management of the customs clearance process

The purpose of any type of control is to change the state of the control object in accordance with a predetermined task. Control methods should answer the question, "how can we construct an algorithm that can control a given object in a way that achieves a predetermined goal?". To do this, the developer needs to know how the control object will respond to different influences, that is, the control object model is needed.

There are many definitions to the concept of "model". One of them is close to our question: "A model is an object that allows you to study the behavior of another object, which is called the original". The model and the original should be similar so that the conclusions drawn from studying the model can be applied to the original[3].

As noted above, in order to study the control object, it is necessary to know how it reacts to various influences on it. If we denote these influences as "input" signals for the control object, then the changes occurring under the influence of these "input" signals can be regarded as "output" signals. That is, the object interacts with the external environment using "incoming" and "outgoing" signals.

If the documents submitted to the customs authorities in this process are taken as "inputs" for modeling the multi-stage customs clearance process and denote them by  $X(t)$ , then customs clearance will be carried out in accordance with these documents. In this case, you can take as an "output" signal the information received as a result of customs clearance, and designate it  $Y(t)$  (Fig. 1.)

here:

$c(t), r(t), v(t)$ - set of impacts of customs clearance results to management;

$c(t)$  - objects of organization of customs control (goods, vehicles, persons), documents, additional information flows, etc.;

$r(t)$  - risks that may affect the process (information, human, financial and other resources);

$v(t)$  - obstacles to achieving the goal (refusal, etc.).

This set of influences moves the customs clearance system  $Z(t)$  towards a given goal and generates a vector of output results  $Y(t)$ . From a mathematical point of view, the function  $Y(t)$  is the reaction of the control object - the customs clearance process - to external influences.

Optimal management of the multi-stage customs clearance process can be carried out with respect to a number of objectives. In particular, optimization is envisaged in relation to one of the following goals:

- ensuring the completeness of revenues to the state budget, i.e. maximization of revenues to the state budget;
- minimize the amount of arrears that may not go to the state budget, that is, possible damage to the budget;
- Reduction of expenses of the entrepreneur - participant of foreign trade, i.e. minimization of damage caused to him in the process of customs clearance;
- minimize time for customs clearance processes;
- other purposes.

The purpose of this study is the optimal management of the customs clearance process, as well as minimizing the time spent on this process. Because it will ultimately lead to minimization of time for the customs clearance process, as well as to maximize revenues to the state budget and minimize the costs of the entrepreneur - participant of foreign trade.

It is known that in the general case the question of linear optimization can be expressed as follows [4]:

$$\max(\min) f(x) = \sum_{k=1}^n c_k x_k \tag{1.1}$$

$$\left. \begin{aligned} \sum_{k=1}^n a_{jk} x_k &= b_j, & \text{if } j &= \overline{1, m_1} \\ \sum_{k=1}^n a_{jk} x_k &\geq b_j, & \text{if } j &= \overline{m_1 + 1, m_2} \\ \sum_{k=1}^n a_{jk} x_k &\leq b_j, & \text{if } j &= \overline{m_2 + 1, m} \\ x_k &\geq 0, & k &= \overline{1, n} \end{aligned} \right\} \tag{1.2}$$

In this research paper, in the formation of a mathematical model of optimal control of the process of multi-stage customs clearance in relation to the time consumed, it is proposed to use the stages of customs clearance shown in Table 1.

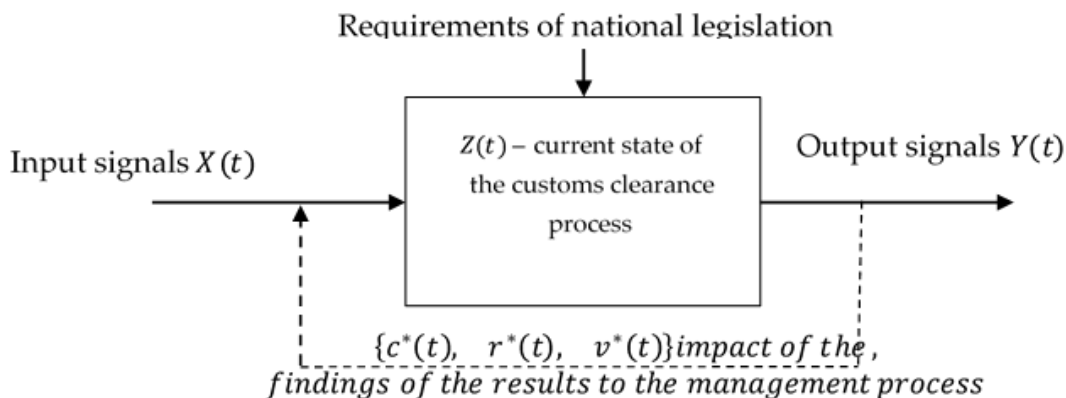


Figure 1: The main factors of the customs clearance process

Table 1. "Customs Clearance Process: Task Execution Matrix"

Estimated execution time	Function names	Implementer
$t_1$	Preparation of necessary primary documents for customs clearance	Foreign trade participant or customs broker
$t_2$	Determination of the code of goods according to the harmonized system Commodity nomenclature	
$t_3$	Calculation of the customs value of goods	
$t_4$	Calculation of customs payments	
$t_5$	Preparation of cargo customs declaration	
$t_6$	Ensuring customs payments	
$t_7$	Submit a preliminary declaration to the customs authorities prior to the arrival of the shipment	
$t_8$	Cargo delivery under customs control	Carrier
$t_9$	Storage related to customs inspection procedures	Customs warehouse jointly with a foreign trade participant and the customs service
$t_{10}$	Delay of goods due to inability to release due to technical or other reasons	
$t_{11}$	Storage initiated by the owner of the goods	
$t_{12}$	Request additional documents when necessary	Customs Service
$t_{13}$	Direct the cargo to the appropriate (red, yellow or green) customs control lane based on the analysis of submitted documents and risk profiles	
$t_{14}$	Implementation of procedures either according to the principles of red road customs	
$t_{15}$	Implementation of procedures either on the basis of the yellow road customs	
$t_{16}$	Implementation of procedures either according to the principles of green road customs	
$t_{17}$	Control over the completeness of receipt of customs payments	
$t_{18}$	Release of cargo into free circulation or for export in accordance with the established procedure	

The presented list of functions is grouped into four main blocks. These functions are performed by customs authorities, foreign trade participants and enterprises providing services in the customs field. The organization of customs clearance is characterized by a large number of operations performed, the complexity of which is determined by a combination of factors: type of goods, country of origin, declared customs value of the goods,

From the above table it follows that the process of multi-stage customs clearance covers 18 stages, of which stages 1-7 are performed by a foreign trade participant or a customs broker, stage 8 - by a cargo carrier, stages 9-11 - stages are performed by owners of customs warehouses, and for execution 12 - 18 - the stages are responsible for the employees of the customs service. That is, in formula (1.1),  $n = 18$ .

$$f(t) = \sum_{k=1}^{18} r_k t_k \rightarrow \min \quad (1.3)$$

where:  $r_k = r_k(X)$  – the level of risk of execution of the k-stage;

$X = X(x_1, x_2, \dots, x_{58})$  – vector,  $x_i$  elements of which are determined depending on the value of the corresponding columns of the cargo customs declaration. In practice, the level of risk of customs clearance is determined depending on the documents submitted for customs clearance, including the cargo customs declaration.

At the same time, the estimated time of duration of the customs clearance process for responsible executors is determined by normative and directive documents, in particular, documents approved by the Cabinet of

Ministers of the Republic of Uzbekistan. If we denote them as  $b_1, b_2, b_3$  and  $b_4$ , respectively, conditions (1.2) will come to the following form:



$$\left. \begin{aligned}
 0 < \sum_{k=1}^n a_{jk} t_k \leq b_1; a_{jk} = 1 \quad \text{if} \quad j = \overline{1, m_1} \\
 0 < \sum_{k=1}^n a_{jk} t_k \leq b_2; a_{jk} = 1 \quad \text{if} \quad j = \overline{m_1 + 1, m_2} \\
 0 < \sum_{k=1}^n a_{jk} t_k \leq b_3; a_{jk} = 1 \quad \text{if} \quad j = \overline{m_2 + 1, m_3} \\
 0 < \sum_{k=1}^n a_{jk} t_k \leq b_4; a_{jk} = 1 \quad \text{if} \quad j = \overline{m_3 + 1, m_4} \\
 t_k \geq 0, k = \overline{1, n}
 \end{aligned} \right\} (1.4)$$

here:  $n=18, m_1=7, m_2=8, m_3=11, m_4=18$ .

$a_{jk}=0$  at the values of index  $j$ , which are not included in conditions (1.4)

The above formulas (1.3) and (1.4) give a mathematical model of the problem of optimal control of the process of multi-stage customs clearance.

### 3. Analysis of existing methods for solving the linear programming problem with variable coefficients

The obtained results (1.3) and (1.4) show that the mathematical model of the problem of optimal control of the process of multistage customs clearance has the form of a linear programming problem with variable coefficients of the objective function. Currently, there are a number of effective methods available for solving the linear programming problem.

In particular, for constant values of the coefficients ( $r_k$ ) of the objective function (1.3) under the limiting conditions (1.4), a number of methods are used in practice to determine its minimum value. These include methods such as the simplex method, the deployment of a function on algebraic polynomials, Fourier series, the use of spline functions, and others. A sufficient number of computer programs for numerical solution of this problem have been implemented.

However, the features of the problem of optimal control of the multi-stage customs clearance process, which is described in (1.3) - (1.4) are variable coefficients of the target function. The functions  $r_k = r_k(X)$  which represent the degree of risk of the  $k$  - process, is a function of the variables of the cargo customs declaration. This requires a specific approach to solve this problem.

In particular, the 3rd and 4th stages "calculation of the customs value of goods" and "calculation of the amounts of customs payments" of Table 1. are important stages in the customs clearance process in ensuring the fulfillment of fiscal tasks assigned to the customs authorities.

This fact indicates the relevance of improving mathematical modeling of the customs clearance process and its comprehensive study.

At the same time, the study of scientific papers on the study of similar problems showed that a sufficient number of studies have been carried out and certain methods have been developed for solving the problem of linear programming with variable coefficients.

For example, the work of [6] is one of the relatively early studies in this area. The problem of parametric programming of the following form is considered:

$$\left. \begin{aligned}
 f(X) = \sum_{j=1}^n c_j x_j, \quad X = \{x_j\}, \quad c_j \in \mathfrak{S} \\
 \sum_{k=1}^n a_{ij} x_j = b_i; \quad i = \overline{1, m} \\
 x_j \geq 0, \quad j = \overline{1, n}
 \end{aligned} \right\} (2.1)$$

here:  $c_j$  - elements of some ordered functional prospace  $\mathfrak{S}$ ,  $a_{ij}, b_i$  - known,  $x_j$  - unknown real numbers,  $X$  - plan of the problem (non-negative solution of the problem (2.1)) Plan  $X^*$  is optimal if for any plan  $X$   $f(X) \leq f(X^*)$ . Note that the values of the target function (2.1) belong to the space  $\mathfrak{S}$ , in which the usual properties of numerical inequalities are known to hold.

The existence of a solution to problem (2.1) is proved in this paper by introducing the concept of resolving combinations of problem (2.1), considered as elements of the space  $\mathfrak{S}$ , are comparable with the zero of this space, i.e., if  $x \in \mathfrak{R}$ , then one and only one of three relations holds:  $x > 0$ ,  $x < 0$ , and  $x = 0$ . Under these conditions, the following theorem is proved:

**Theorem.** The problem (2.1) with a non-empty set of plans and a target function bounded from above, satisfying the condition: all solving combinations of coefficients of the target function are comparable to zero, has a solution.

However, the paper does not provide a methodology for determining the existing solution.

In [7], a parametric programming problem of the following kind is considered:

$$\left. \begin{aligned}
 \min(\max) z(x) = \sum_{j=1}^n c_j(x) x_j \\
 \sum_{j=1}^n a_{ij}(x) x_j \geq b_j(x), \quad i = \overline{1, m}
 \end{aligned} \right\} (2.2)$$

here  $a_{ij}(x)$ ,  $b_i(x)$  and  $c_j(x)$  - some piecewise constant argument functions  $x = (x_1, x_2, \dots, x_n)$ .

The functions  $a_{ij}(x)$ ,  $b_i(x)$  and  $c_j(x)$  are defined on the same set  $G = \{x \in G \subset R_n\}$ . There exists a finite partition  $G = \cup G_k$ , ( $k=1, l$ ) such that the functions are constant in each subset  $G_k$ , and  $G_k$  and  $G_{k+1}$  can intersect only along their boundaries.

By requiring that in problem (1)-(2) the target function  $z(x)$  and the constraint functions:

$$f_i(x) = \sum_{j=1}^n a_{ij}(x)x_j - b_j(x), \quad i = \overline{1, m}$$

be continuous and convex, by a simple enumeration of a finite number of regions  $G_k$ , in each the usual linear programming problem is solved.

The work [8] is devoted to the study of the problem of parametric programming of the following form:

here:  $X=(x_1, \dots, x_n)^T$  -  $n$ -dimensional vector of unknown variables, which satisfies the constraints (2.3), forming the set of admissible solutions of the problem;

$$\left. \begin{aligned} f(X) &= c_1(t)x_1 + c_2(t)x_2 + \dots + c_n(t)x_n \rightarrow \underset{x \in D}{extr} \\ A(t)X &\leq b(t) \\ x_j &\geq 0, \quad j = \overline{1, n} \end{aligned} \right\} (2.3)$$

$b(t)=(b_1(t), b_2(t), \dots, b_m(t))^T$  and  $C(t)=(c_1(t), \dots, c_n(t))^T$  - parametric vectors of free terms of constraints and coefficients of the target function, respectively;

$A(t)_{n \times m}=(a_{ij}(t))$ ,  $i=1 \dots n$ ,  $j=1 \dots m$  is an  $n \times m$ -dimensional matrix of parametric constraint coefficients. The functional dependence on the parameter  $t$  can be either linear or nonlinear.

In the work on the basis of simplex method and differential transformations the methods of solving linear programming problems with parametric coefficients of the target function and right parts of constraints are considered, allowing to organize simple iterative calculations and excluding the solution of systems of inequalities.

$$\left. \begin{aligned} \max F &= \max \sum_{j=1}^n c_j x_j \\ \sum_{j=1}^n a_{ij} x_j &\begin{cases} \leq \\ = \\ \geq \end{cases} b_j, \quad i = \overline{1, m} \\ x_j &\geq 0, \quad j = \overline{1, n} \end{aligned} \right\} (2.4)$$

In this case, it is assumed that the parametric functions  $X=(x_1, \dots, x_n)^T$ ,  $b(t)=(b_1(t), b_2(t), \dots, b_m(t))^T$  and  $C(t)=(c_1(t), \dots, c_n(t))^T$  are sufficiently smooth, have smooth differentials, and have explicit expressions.

In the studies of the authors [9] and [10] the linear programming problem with variable parameters is considered, in which not only variables included in its composition, but also coefficients, as well as the right part and parameters (coefficients at variables) of the target function can change.

An approach is proposed that allows solving linear programming problems with interdependent variable coefficients using the simplex method.

The formulation of the problem is as follows:

here:  $m$  - number of restrictions,

$n$  - number of variables,

and additional restrictions on variable coefficients:

$$\left. \begin{aligned} a_{ij}^- &\leq f_{ij} a_{ij} \leq a_{ij}^+ \\ s_k^- &\leq \sum_{i=1}^m d_{kij} a_{ij} \leq s_k^+; \quad k = \overline{1, K} \\ \sum_{i=1}^m p_{lij} a_{ij} &= r_l; \quad l = \overline{1, L} \\ c_j^- &\leq f_{ij} c_j \leq c_j^+ \end{aligned} \right\} (2.5)$$

In the constraint system (2.4)-(2.5), all parameters  $a_{ij}^-$ ,  $a_{ij}^+$ ,  $s_k^-$ ,  $d_{kij}$ ,  $s_k^+$ ,  $p_{lij}$ ,  $r_l$ ,  $c_j^-$ ,  $c_j^+$ ,  $f_{ij}$  are constants set during the problem formulation process. Conditions (2.5) are sometimes called interval conditions and problem (2.4) is an interval linear programming problem with interdependent variable coefficients.

Under these conditions, the following lemma is proved by constructive method:

Lemma. Let in the linear programming problem (2.4) - (2.5) there are variable coefficients that depend on a parameter of the form  $a_{ij}=a_{ij}(t_j)$ , having a domain of definition on a certain interval  $[\alpha_j; \beta_j]$  and continuously differentiable on it. Then the simplex method applied to solve such a problem converges if the above constraints are satisfied.

The proof is constructive in the sense that it substantiates the execution of all stages of the implementation of the simplex method, taking into account condition (2.5). The essence of the proposed method is that at each step the number of the column entering the basis at the next iteration of the simplex method algorithm is determined and calculations are performed on the points of minimum of the function  $a_{ij}(t)$  In [11], the following parametric programming problem was considered:

$$\left. \begin{aligned} \sum_{i=1}^n c_i x_i + c_0 &\leq Z, \\ \sum_{k=1}^n a_{ik} x_k &\leq b_i, \quad i = \overline{1, m} \\ x_j &\geq 0, \quad j = \overline{1, n} \\ Z_{\min} - ? &, \quad x_i(Z_{\min}) - ? \end{aligned} \right\} \quad (2.6)$$

To solve the linear parametric programming problem, it is assumed that the coefficients change insignificantly with respect to their average values, as, for example, the cost of goods depending on the exchange rate or inflation rate. In such cases, when the relative changes in the coefficients are of the order of 10% or less, it is proposed to use the asymptotic perturbation method. Its essence is reduced to the search for the decomposition of the desired functions into functional series, the rapidity of convergence of which depends on the "smallness parameter" of the relative change of the functions affecting the problem.

The algorithm for solving the problem is as follows. We assume solutions of the problem (2.6) in the form of series consisting of corrections of the corresponding order:

$$\begin{aligned} Z &= Z^0 + Z^1 + Z^2 + \dots; \\ x_i &= x_i^0 + x_i^1 + x_i^2 + \dots; \end{aligned}$$

The values of  $Z^k$  and  $x_i^k$  are determined in an iterative way, assuming  $Z^0$  and  $x_i^0$  as the first approximation in the iteration process. The values of  $Z^0$  and  $x_i^0$  are the solution of a simple linear programming problem (1), when their average values  $a_{ij}^0$ ,  $b_i^0$  and  $c_j^0$  are taken instead of the variable coefficients  $a_{ij}(x)$ ,  $b_i(x)$  and  $c_j(x)$ .

For example, if  $c_j(x)$  is continuous in the interval  $[0;1]$ , then we take as its mean value:

$$c_j^0 = \int_0^1 c_j(x) dx \quad (2.7)$$

The above brief overview shows that the problem of linear programming with variable coefficients is a well-known problem that has sufficient applications and is being studied everywhere. A certain number of methods for solving this problem have been developed, which are successfully applied depending on the problem formulation and application area.

#### 4. Trigger graph model of the process and customs risk criterion

Based on the results of the above analysis, we can say that all methods of solving the linear programming problem with variable coefficients imply certain

requirements for the ratio of the coefficients of the target function. First, an explicit form and smoothness of the parametric function are required. Second, when applying some methods of solving this problem, additional conditions such as continuity and differentiability of the given function are required.

However, in the case of the problem of optimal control of the customs clearance process, the parametric coefficients of the target function do not have an explicit expression and the above conditions cannot be required. Consequently, there are certain difficulties in applying the available methods to solve the problem, and it is required to explore new approaches.

Based on the latter findings, to minimize the target function (1.3) under conditions (1.4), it is proposed to ensure minimization of the coefficients of the target function  $r_k(X)$ , which represent the degree of risk of the  $k$  – process. Without violating the conditions of the stated problem and generality, we can assume that:

$$r_k(X) \geq 0, \quad k = \overline{1, 18} \quad (3.1)$$

The task of minimizing the coefficients of the target function  $r_k(X)$  gives rise to the task of investigating the essence of customs risks

The above studies have led to the fact that customs risks from the mathematical point of view is a function of many variables, is not presented in an explicit form, there are considerable uncertainties in its characteristics in terms of smoothness, continuity, differentiability and other qualities.

Before moving on to research on the specifics of the customs risk, it is important to consider the essence of the risk as a whole, since it is inherent in various fields of activity. There are many approaches to defining the concept of "customs risk". For example, the working group of the World Customs Organization, preparing the document "World Customs Organization Compendium on Customs Risk Management" in 2011, gave the following definition: "Risk: the result of doubts arising in relation to objects" [12]. In scientific literature it is defined as follows: "Risk is the probability of violation of customs legislation associated with evasion of payment of customs duties and taxes due" [13].

In these or other definitions of customs risk, which are observed in previously published scientific papers, the "probability of violation of customs legislation" passes as the main predicate. This means that the mathematical expression of customs risk must necessarily include the "probability of violation of customs legislation" model.

Based on the above, in order to develop a mathematical approach to this definition, it is necessary to study customs legislation both at the national level and at the

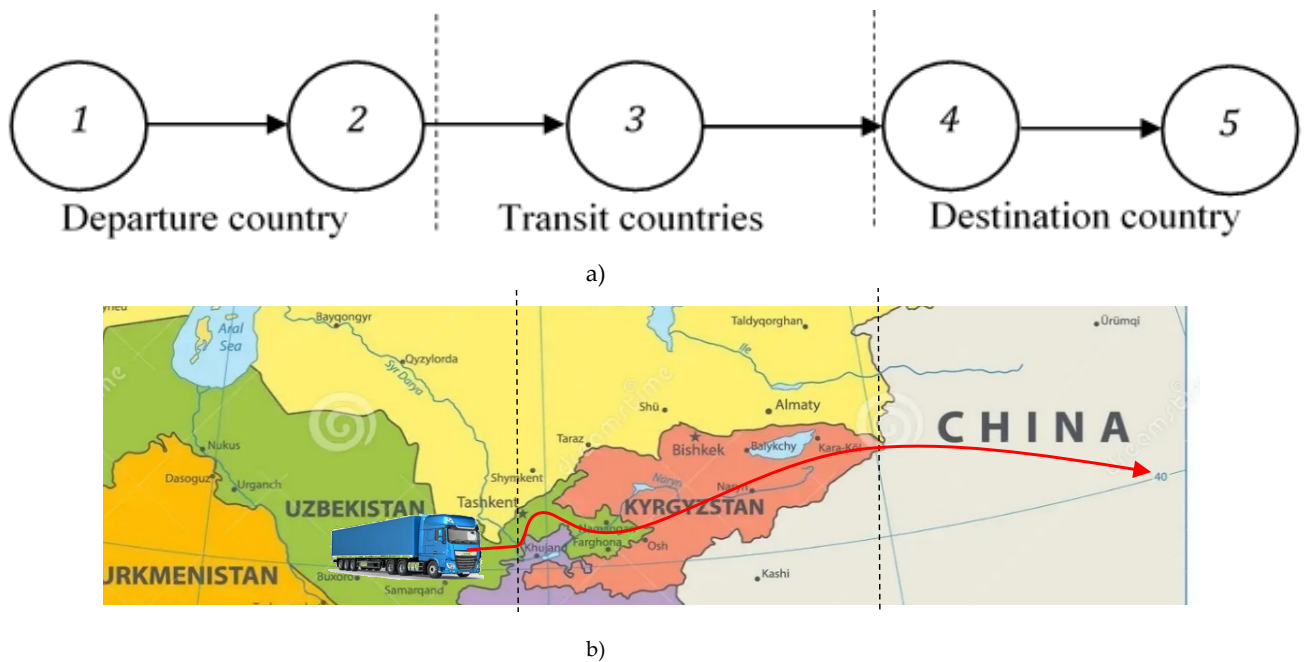


Figure 2: Simplified graph model (a) and explanatory scheme (b) of the process of foreign trade operations (author's development)

international level. At the same time, the importance of studying international conventions in the field of customs should be emphasized, as the process of a foreign trade operation is directly related to foreign partners.

Fig. 2. shows a simplified graph model (a) and an explanatory scheme (b) of the process of foreign trade operations.

An analysis of the customs legislation on the day of the present research shows the following. By the beginning of the second half of 2023, more than 2216 normative legal documents related to the regulation of the activities of customs authorities of the Republic of Uzbekistan were in force (Table 2).

Table 2: Information on legal documents related to the regulation of the activities of the customs authorities of the Republic of Uzbekistan

Type of normative document	Amount
Laws of the Republic of Uzbekistan	57
Codes of the Republic of Uzbekistan	12
Decrees of the President of the Republic of Uzbekistan	322
Resolutions of the President of the Republic of Uzbekistan	767
Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan	1011
Orders of the Cabinet of Ministers of the Republic of Uzbekistan	11
legal acts registered with the Ministry of Justice of the Republic of Uzbekistan	36
<b>Total</b>	<b>2216</b>

(author's development)

Despite the fact that there is such an extensive customs legal framework, the main task of the customs authorities of the Republic of Uzbekistan is to protect the economic

security of the country and almost all the rules of this framework are focused on the following two main tasks [14]:

- a) fulfillment of the fiscal task - ensuring the completeness of customs payments collection;
- b) prevention, detection and suppression of violations of customs legislation, including smuggling.

The study of customs legislation and practical experiments showed that between the above-mentioned main tasks of managing foreign trade operations, in terms of procedure, there is an irreconcilable contradiction. This contradiction is manifested in the following:

- a) the key parameter for increasing customs payments is the time spent on customs clearance of foreign trade goods: the less time spent on customs clearance of a particular foreign trade cargo, the more cargo will be cleared for a certain period of time, hence, more customs payments will be made to the state budget during this period.

At the same time, the number of violations of customs legislation and the volume of goods of illegal circulation are increasing, since the time for a detailed study of the consignment of goods being processed remains minimal.

- b) the key parameter for reducing customs law violations is also the time spent on customs clearance of foreign trade goods: the more time to study a specific consignment of foreign trade cargo, the less chance there is to commit violations of customs legislation.

At the same time, the amount of revenues to the state budget from customs payments decreases, as the foreign trade turnover for a certain period of time decreases.

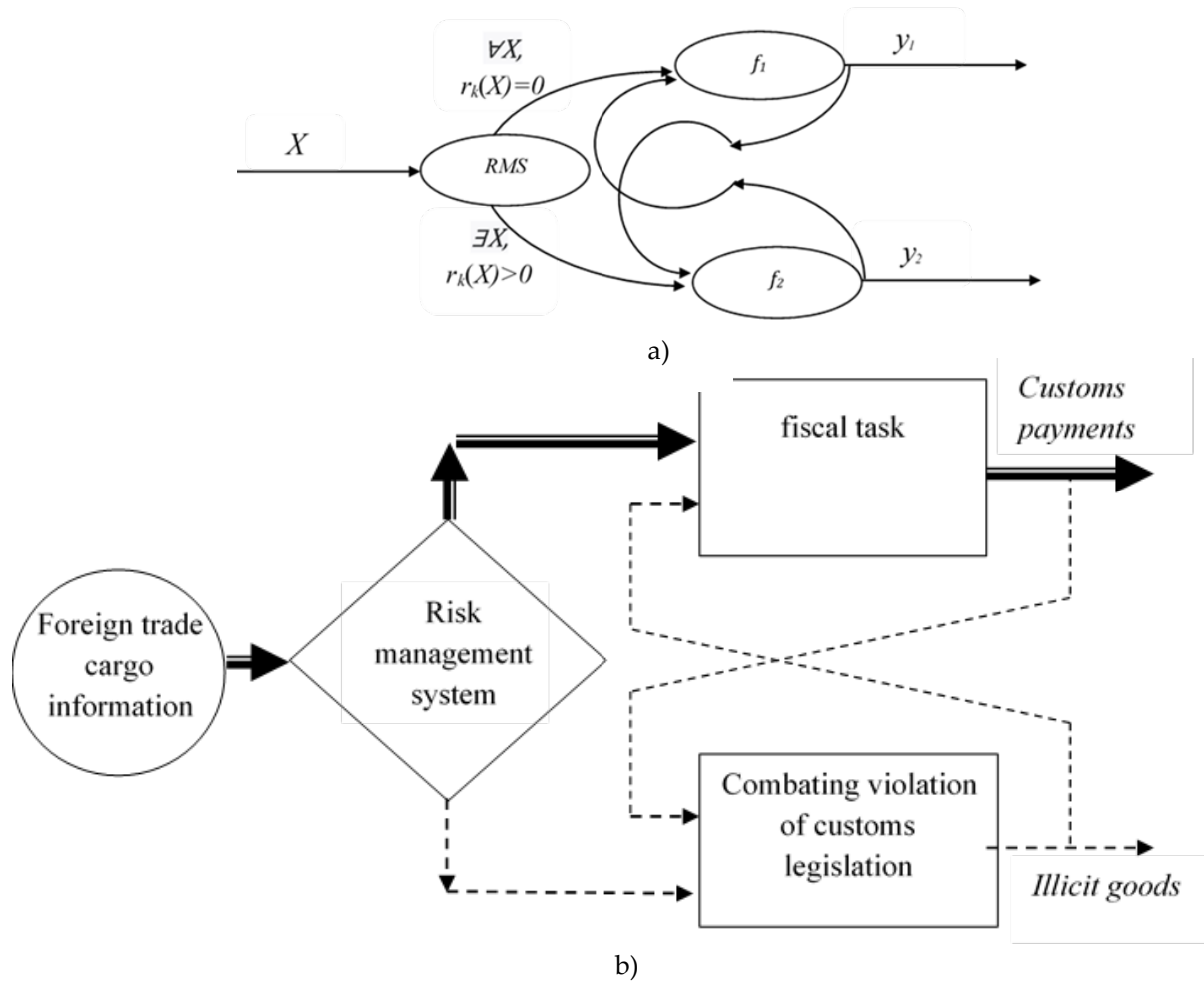


Figure 3: Trigger graph model (a) and its explanatory scheme (b) of the main tasks of foreign trade operations management (author's development)

To minimize irreconcilable contradictions between the main tasks of managing foreign trade operations in procedural terms, in practice, a customs risk management system is used. Trigger graph model of the main tasks of foreign trade operations management with application of risk management system is shown in Fig.3.

It should be noted that both functions - the function  $y_1$ , which reflects the volume of receipt of customs payments, and the function  $y_2$ , which reflects the volume of illegal goods (customs law violations) are functions of time, i.e.  $y_i = y_i(t)$ . Both functions are inversely proportional to the ratio of customs clearance time, i.e.

$$y_i = \varphi_i \left( \frac{1}{t} \right), \text{ where } \varphi_i - \text{linear functions, } i = 1, 2 \quad (3.2)$$

On the other hand, the conducted experiments showed that with an increase in the volume of goods of illegal circulation (offenses of the customs legislation), the receipts of customs payments decrease, i.e. functions  $y_1$  and  $y_2$  are inversely proportional to each other:

$$y_1 = \psi_i \left( \frac{1}{y_2} \right), \text{ where } \psi_i - \text{linear function} \quad (3.3)$$

The mathematical contradiction reflected in (3.2) and (3.3) gives rise to the need for an optimization problem about the choice of time for customs clearance of foreign

trade goods. It is required for each batch of goods to review the duration of customs clearance time and choose it so that there would be maximum receipt of customs payments and minimum volume of goods of illegal turnover (violations of customs legislation).

This task can be solved only if the following conditions are met:

- a) choose the minimum time for customs clearance, in the absence of customs risk;
- b) choose the time of customs clearance sufficient to ensure the minimization of the customs risk, if it is detected.

### 5. Risk assessment of the reliability of customs information

We mentioned above that in the scientific literature there is a theory according to which any customs system successively goes through several separate phases of its activity, characterized by the specifics of its relations both with foreign trade participants and with the state. Three phases of development are noted: the customs systems of developed countries are in the "customs for foreign trade participants" phase, in most developing countries the phase "customs for the government" is characteristic, and in

a number of underdeveloped countries there is a “customs for themselves” phase.

Proceeding from the fact that the Republic of Uzbekistan is carrying out large-scale works on transferring the customs service to the phase "customs for foreign trade participants", the authors of this paper study customs risks, categorizing them into three classes:

- a) customs risks for business;
- b) customs risks of economic security;
- c) corruption risks.

a) when it comes to the customs risk for business, it means the submission of an unreliable customs declaration by the business to the customs authorities. Analysis of the database of violations of customs legislation for several years shows that every 4th fact about such violation is the result of false declaration.

Despite the fact that at the present stage of development of foreign trade, favorable conditions are created for a law-abiding participant in foreign trade, the laws react rather harshly towards them if they have submitted an unreliable customs declaration to the customs authorities. The consequence of such phenomena for them can sometimes be undesirable, severe and long-lasting.

Therefore, the primary task of the customs service of the Republic of Uzbekistan today is to minimize customs risks for business.

b) the customs risk of economic security is the probability of violation of customs legislation by a participant in foreign trade, associated with evasion of payment of due customs duties and taxes.

c) corruption risks shall mean abuse of official powers, receiving and giving bribes, bribery, mediation in bribery, commercial bribery or other illegal use by a customs officer of his/her official position contrary to the legitimate interests of the state, in order to obtain benefits for himself/herself or for third parties.

Thus, the first step in solving the problem of optimal management of the customs clearance process (1.3) - (1.4) is to minimize the implicit function  $r_k(X)$ , which represent the degree of risk of unreliable declaration of foreign trade goods, i.e. minimization of customs risks for business. To solve this problem it is necessary to assess the reliability of information about the goods on all its parameters, i.e. it is required to conduct a multivariate analysis of information about the goods. Information about the goods is fully reflected in the cargo customs declaration.

The research of the authors of this paper has shown that the customs cargo declaration is one of the fundamental documents of the customs clearance process.

It is formalized in the form of a multidimensional matrix  $X$ , which is the source of state customs statistics [15].

$$X = \begin{matrix} & \begin{matrix} x_{11L} & x_{12L} & \dots & x_{140L} \end{matrix} \\ \begin{matrix} \dots \\ x_{111} & x_{121} & \dots & x_{1401} \\ x_{111} & x_{121} & \dots & x_{1401} \\ x_{211} & x_{221} & \dots & x_{2401} \\ \dots & \dots & \dots & \dots \\ x_{5811} & x_{5821} & \dots & x_{58401} \end{matrix} & \end{matrix} \quad (4.1)$$

A brief characterization of the customs cargo declaration is as follows:

- a) number of columns - 58;
- b) the level of detail of each column of the cargo customs declaration is determined depending on the complexity of the task, but not more than 40;
- c)  $L$  - the total number of cargo customs declaration per year.

It should be noted that each layer of this matrix corresponding to  $l=l_0$  reflects a separate cargo customs declaration. It can be labeled as follows:

$$X_0 = \begin{pmatrix} x_{11l_0} & x_{12l_0} \dots & x_{140l_0} \\ x_{21l_0} & x_{22l_0} & x_{240l_0} \\ \vdots & \ddots & \vdots \\ x_{581l_0} & x_{582l_0} \dots & x_{5840l_0} \end{pmatrix} \quad (4.2)$$

Assessing the validity of information about the goods for all its parameters requires controlling and assessing the validity of all elements of the matrix (4.2). The study of existing methods for solving this problem showed that the problem of identifying unreliable customs declarations is a special case of the general and, as you know, ancient problem of identifying false information, i.e. how to distinguish "truth" from "falsehood".

This famous problem is mentioned in many ancient writings, beginning with Aristotle (384 BC), who is the founder of logic as a science [16]. One of the great scientists who devoted his entire conscious life to the study of the task of distinguishing "truth" from "falsehood" is Imam al-Bukhari. His book Al-Jami'as-Sahih has been tested for over 11 centuries and is considered the most authentic book today [17].

The concept of information reliability has different meanings in philosophy, the theory of forensic evidence, epistemology, logic, probability theory, psychology, natural science and other areas. There is no single

definition of the term, although many famous philosophers have tried to give their own definition of the term. In logic and philosophy, reliability often acts as a synonym for the concept of "truth" and characterizes indisputable, firmly substantiated and demonstrative knowledge.

A "threshold matrix" (TM) is proposed to determine the concept of reliability of the elements of the customs cargo declaration (4.2.) (4.3.).

$$H = \begin{matrix} & \begin{matrix} \eta_{112} & \eta_{122} & \dots & \eta_{1402} \end{matrix} \\ \begin{matrix} \eta_{111} & \eta_{121} & \dots & \eta_{1401} \end{matrix} & \begin{matrix} \eta_{111} & \eta_{121} & \dots & \eta_{1401} \\ \eta_{211} & \eta_{221} & \dots & \eta_{2401} \\ \dots & \dots & \dots & \dots \\ \eta_{5811} & \eta_{5821} & \dots & \eta_{58401} \end{matrix} \end{matrix} \quad (4.3)$$

here:  $\eta_{ij1}, \eta_{ij2}$  - some positive real numbers or textual information.

Definition 1. Each element of the matrix is  $x_{ijl_0} \in X_0$  called reliable if the following condition is satisfied

$$\eta_{ij1} \leq x_{ijl_0} \leq \eta_{ij2} \quad (4.4)$$

where:  $1 \leq i \leq 58, 1 \leq j \leq 40$ .

Definition 2: If all elements of the matrix  $x_{ijl_0} \in X_0$  are reliable, then the customs cargo declaration is called reliable.

Conditions (4.4) are called *criteria*, and the elements of the "Threshold Matrix" are called *indicators* of the reliability of the cargo customs declaration.

From Definition 1-2, the following statement is easily proved:

Statement 1. If at least one element of the matrix  $x_{ijl_0} \in X_0$  does not satisfy the conditions (4.4), then the corresponding cargo customs declaration is unreliable. To assess the reliability of a cargo customs declaration, the authors of this work propose the following function:

$$\rho_{ij} = \begin{cases} e^{\eta_{ij1} - x_{ijl_0}}, & \text{if } \eta_{ij1} \geq x_{ijl_0} \\ 1, & \text{if } \eta_{ij1} \leq x_{ijl_0} \leq \eta_{ij2} \\ e^{x_{ijl_0} - \eta_{ij2}}, & \text{if } x_{ijl_0} \geq \eta_{ij2} \end{cases} \quad (4.5)$$

here:  $1 \leq i \leq 58, 1 \leq j \leq 40$ .

The function  $\rho_{ij}$  can be estimated as follows: when the conditions  $\eta_{ij1} \leq x_{ijl_0} \leq \eta_{ij2}$  are satisfied for all  $1 \leq i \leq 58, 1 \leq j \leq 40$

function value  $\rho_{ij} = 1$ ; otherwise,  $-\rho_{ij} > 1$ . In other words, the function  $\rho_{ij}$  reflects the quantitative assessment of the reliability of the element  $x_{ijl_0} \in X_0$  of the cargo customs declaration. Then the matrix  $\rho$  (4.6) is the matrix of the reliability of the cargo customs declaration  $X_0$ .

$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} \dots & \rho_{140} \\ \rho_{21} & \rho_{22} & \rho_{240} \\ \vdots & \ddots & \vdots \\ \rho_{581} & \rho_{582} \dots & \rho_{5840} \end{pmatrix} \quad (4.6)$$

with the above notations, the following theorem is proved:

Theorem 1. In order for the cargo customs declaration  $X_0$  to be reliable, it is necessary and sufficient to fulfill the following condition:

$$P = \prod_{i=1}^{58} \prod_{j=1}^{40} \rho_{ij} = 1 \quad (4.7)$$

$P$  is the coefficient of reliability of the customs cargo declaration  $X_0$ . It follows from (4.5) and (4.7) that the coefficient  $P$  takes on the values  $P=1$  only if for all  $1 \leq i \leq 58, 1 \leq j \leq 40$  the conditions  $\eta_{ij1} \leq x_{ijl_0} \leq \eta_{ij2}$  are satisfied, otherwise  $P > 1$ .

### 6. Algorithm of control of risks of reliability of calculation of customs payments

To verify the above results, let's consider the tasks of controlling the risks of reliability of the calculation of customs payments. The amount of customs payments for the import of goods is determined as follows:

$$S = D + E + V$$

where:  $D$ - the amount of customs duty,  $E$ - the amount of excise tax,  $V$ - the amount of value-added tax on goods. They are determined mainly by the so-called "ad valorem rates". This means that the amount of each of the above types of customs payments is determined depending on the established rate in percentage terms. For example, the rate of value added tax in the Republic of Uzbekistan is set at 12% of the customs value of the goods.

The formulas for calculating them are as follows:

$$D = d c;$$

$$E = e c;$$

$$V = 0.12 (c + D + E).$$

where:  $c$  is the customs value of the goods,  $d$  is the rate of customs duty,  $e$  is the rate of excise tax.

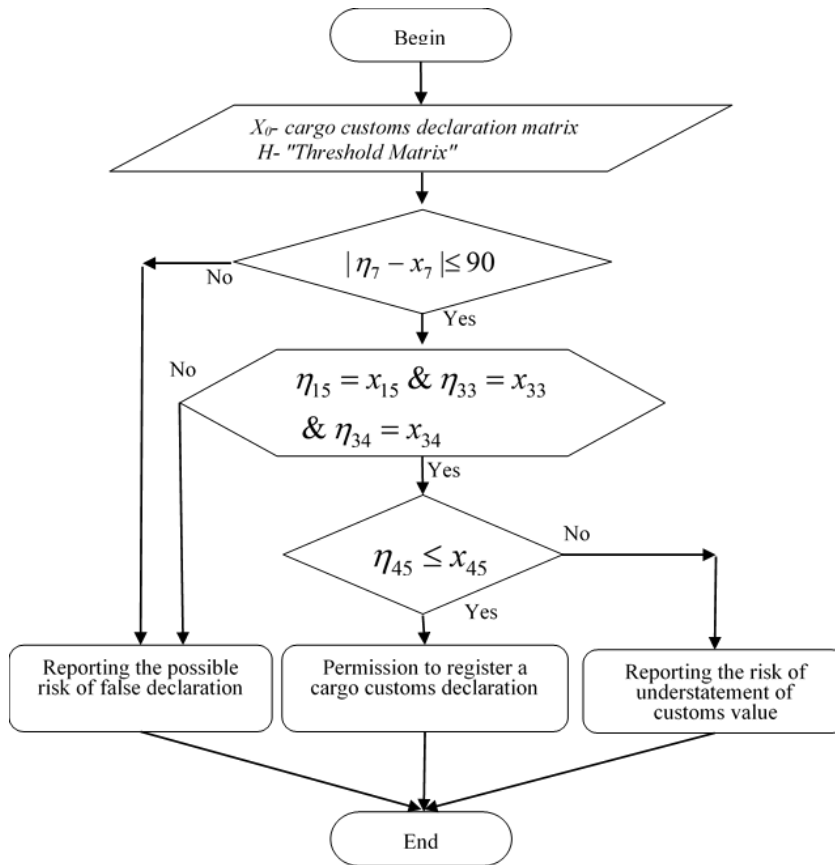


Figure 4: Algorithm for controlling the customs value of goods

After simple arithmetic transformations, you can get:  
 $S=D+E+V= c (d+ e+0.12(1 + d + e)).$

Hence, it can be seen that the amount of customs duties on imports of a particular good depends directly on the customs value of the good c. The lower the customs value of the goods, the lower the receipt of customs payments to the state budget.

Considering this circumstance, the "Threshold Matrices" were formed in the form of "Price Information Bulletins". The table reflects the following data:

- η7- date of registration of the customs value of goods;
- η33- commodity code in accordance with the Harmonised System (HS);
- η15 – code of the country of departure of the goods;
- η34 – country of origin code;
- η45- customs value of goods.

The other elements of the "threshold matrix" for the considered criterion of the reliability of the customs value of goods are of little importance.

Then conditions (4.4) have the following form:

$$|\eta_7 - x_7| \leq 90$$

$$\eta_{15} = x_{15}$$

$$\eta_{33} = x_{33}$$

$$\eta_{34} = x_{34}$$

$$\eta_{45} \leq x_{45}$$

Taking into account the above designations, an algorithm for controlling the customs value of goods has been developed (Fig. 4)

It should be noted that the "Price Information Bulletin" is a characteristic feature of the national legislation of the Republic of Uzbekistan, and is not observed in the practice of the customs services of other countries.

## 7. Conclusion

In conclusion, I would like to note that the authors of this article conducted research on minimizing customs risks for business. This is due to the fact that large-scale work is being carried out in the Republic of Uzbekistan to organize the work of the customs service on the principle of "customs for participants in foreign trade". Because, the faster the country's customs service approaches the stage of development "customs for foreign trade participants," the faster the country approaches the level of developed countries.

When it comes to customs risk for a business, it means submitting an unreliable customs declaration to the customs authorities on the part of the business. An analysis of violations of customs legislation over several years shows that every 4th fact of such a violation is the result of an unreliable declaration. It is known that for an unreliable declaration, punishment is provided up to criminal. The consequences of such an incident can sometimes be undesirable, severe and long-term for business.



The research carried out within the framework of this article showed that the task of identifying unreliable customs declarations is a special case of the general and, as we know, ancient task of identifying false information, i.e. how to distinguish “truth” from “falsehood”.

To determine the reliability of a cargo customs declaration, the authors proposed a “threshold value matrix” method, which in fact forms a “knowledge base” of a production expert system that represents knowledge in the form of “IF-THEN” rules. The block diagram of the algorithm for one of these rules is shown above in Fig. 4.

The software of this expert system determines existing errors in the customs cargo declaration as they are received by the customs authorities via the Internet and automatically informs the foreign trade participant about this. No administrative or criminal sanctions will be applied to a foreign trade participant who promptly and voluntarily corrects errors.

Currently, 53 logical rules have been established in the knowledge base to control the reliability of the customs value of goods, which make it possible to localize such customs risks. As a result of the implementation of these rules in 2022, in 88 thousand 897 cases, the risks of “unreliability of the customs value of goods” and debts to the state budget in the equivalent of more than 9 million 968.8 thousand US dollars were prevented.

### Conflict of Interest

The authors declare no conflict of interest.

### Acknowledgment

We thank the editor of the Journal of Engineering Research and Sciences and the anonymous reviewers for their valuable comments. All errors and omissions remain the responsibility of the authors.

### References

- [1]. A. O. Rudneva, "International trade: specifics and prospects of participation of developed, developing and transition countries," *MIR (Modernization. Innovation. Development)*, vol. 8, no. 3, 430-438, 2017, doi: 10.18184/2079-4665.2017.8.3.
- [2]. A.D. Ershov, "Formation of customs services in foreign economic activity," *Scientific notes of the St. Petersburg branch of the Russian Customs Academy*, no. 1(23), 174-192, 2005.
- [3]. S.V. Zvonarev, "Fundamentals of mathematical modeling: textbook," Yekaterinburg: Ural University Press, 112 p., 2019.
- [4]. R.I. Ibyatov, "Optimization methods in problems of mathematical modeling," methodological guidelines, Kazan: Kazan State Agrarian University Publishing House, 32 p., 2016.
- [5]. R. V. Fedorenko, "Methodology of management of service complexes in the customs sphere," *Dissertation for the degree of Doctor of Economics*, Samara, 2015. <https://www.sseu.ru/wp-content/uploads/2015/06/Dissertatsiya-Fedorenko-R.V.pdf>. (dissertation in Russian with an abstract in English)
- [6]. A.G. Pinsker, "A linear programming problem with variable coefficients of the purpose function," *Sib Math J*, vol. 20, 466-468,

1979, doi: 10.1007/BF00969958. (article in Russian with an abstract in English)

- [7]. M. O. Gavrilova, "On problems of linear programming with piecewise constant coefficients," *Scientific journal "Bulletin of the Perm State Technical University. Chemical technology and biotechnology"*, Perm, No. 9, 172-179, 2010.
- [8]. A. G. Avetisyan, L. S. Gyulzadyan, "A method for solving problems of parametric linear programming based on differential transformations," *Scientific journal "Izvestia of the Tomsk Polytechnic University"*, vol. 324, No. 2, 25-30, 2014.
- [9]. D.A. Salimonenko, "A method for solving a linear programming problem with variable coefficients in the form of parametric functions," *Scientific journal "Vestnik of the Bashkir University"*, Ufa, vol. 20, No. 1, 25-29, 2015.
- [10]. D.A. Salimonenko, A.M. Ziganshin, V.A. Mudrov, Yu.D. Salimonenko, "On interdependent variable coefficients in linear programming problems," *Scientific journal "Mathematical Structures and Modeling"*, Omsk, vol. 2, no. 58, 96-111, 2021, doi: 10.24147/2222-8772.2021.2.96-111.
- [11]. S.P. Kravchuk, I.S. Kravchuk, O.V. Tatarnikov, E.V. Shved, "Perturbation method for solving linear programming problems with a parameter," *Scientific journal "Fundamental Research"*, Moscow, No. 5, 299-303, 2015.
- [12]. WCO, "Customs Risk Management Compendium," Brussels, Belgium, June 2011, <http://www.wcoomd.org>.
- [13]. S.E. Tamrazyan, "Customs Risks: Essence, Management and Evaluation," *Scientific journal "Economics and Management in the XXI century: development trends"*, No. 23, 168-172, 2015.
- [14]. A.A. Saidov, F.A. Khakimova, T.T. Abdurakhmonov, "The concept and model of the 'soft component' of the risk management system of customs authorities," *Scientific journal "Bulletin of the Russian Customs Academy"*, Moscow (Russia), No. 3, 100-109, 2022, doi: 10.54048/20727240\_2022\_03\_100 (article in Russian with an abstract in English).
- [15]. A.A. Saidov, "Classical Methods of Controlling the Reliability of Information and Features of Their Application to Customs," *Monograph*, Tashkent, 498 p, 2021. (monograph in Russian with an abstract in English)
- [16]. Aristotle, "Metaphysics," Translation from Greek by P. D. Pervov and V. V. Rozanov, Moscow: Institute of Philosophy, Theology and History of St, Thomas, 232 p., 2006.
- [17]. Muhammad ibn Ismail al-Bukhari, "Al-Jami' as-sahih," Translation by Vladimir (Abdullah) Nirsha, Moscow (Russia), Umma Publishing House, 448 p., 2017.

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).



**ILKHOM MUKHTOROV** - First Deputy Chairman of the Customs Committee under the Ministry of Economy and Finance of the Republic of Uzbekistan. Project Manager of the Customs Risk Management System. Scientific interests are connected with the intellectualization of the processes of organization of customs control. Author of the concept "Export in three steps", is the author of the monograph on factorial data analysis.










**TAKHIR ABDURAXMONOV** - Chief Inspector of the Department of Information and Communication Technologies and Cybersecurity of the Customs Committee of the Republic of Uzbekistan, participated in the work of the group on the development of the customs information system "Electronic Declaration". Her research interests include monitoring the reliability of customs information, digitalization of customs control processes and interdepartmental

interaction within the framework of the customs expert information system..



**ABDUSOBIR SAIDOV** - Abdusobir Saidov - Head of the Department of Information Technology and Mathematics, Customs Institute of the Customs Committee under the Ministry of Economy and Finance of the Republic of Uzbekistan. Doctor of technical sciences, professor. Scientific research is devoted to ensuring the reliability of customs information, is the author of several monographs on this topic

# Browser-in-the-Browser (BitB) Attack: Case Study

Khalid Alissa<sup>1\*</sup> , Bushra Alhetelah<sup>1</sup> , Ghadeer Alazman<sup>1</sup> , Asma Bader<sup>2</sup> , Noor Alhomeed<sup>2</sup> , Layan Almubarak<sup>2</sup> , Fajer Almulla<sup>2</sup> 

<sup>1</sup>SAUDI ARAMCO Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

<sup>2</sup>Department of Networks and Communication, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

\*Corresponding author: Khalid Alissa, Address, Email: [kaalissa@iau.edu.sa](mailto:kaalissa@iau.edu.sa)

**ABSTRACT:** Phishing attacks are becoming more sophisticated daily, taking advantage of victims' lack of awareness to steal sensitive information. The browser-in-the-browser (BitB) attack is a novel and sophisticated phishing technique that uses a single sign-on (SSO) popup window that mimics a legitimate browser login to steal a user's credentials. In addition, an attacker can customize the URL shown in the header of the fake login popup to appear as a legitimate link with a padlock symbol. This attack is relatively dangerous as it steals sensitive information and is designed in a way that is hard to detect using HTML, CSS, JavaScript, and social engineering techniques. This paper aims to study and analyze BitB. Also, conduct an experiment on the BitB attack scenario from the attacker and victim's points of view and recommend countermeasures to detect the attack. The results of BitB attack analysis and experiments show that BitB attacks require basic knowledge of phishing tools and programming languages to be implemented by attackers and achieve their goal of stealing sensitive information that allows them to move on to the next stage of their attacks. Further, this paper will be the first academic paper to study a new type of attack due to the lack of available research and documentation, making it a crucial contribution to the field.

**KEYWORDS:** Phishing Attacks, Browser Attacks, Browser-in-the-Browser Attack, SSO

## 1. Introduction

Day after day, attackers develop and innovate techniques to deceive users maliciously and cleverly. The Browser-in-the-Browser (BitB) attack is a web attack that simulates a login page with a spoofed legitimate domain to steal user credentials, unlike the traditional phishing websites, which mimic the original web page and have deceptive URLs [1]. This attack mainly targets the Single Sign-On authentication model to obtain sensitive information, specifically the credentials of users [2]. This attack severely threatens web users because users trust Single Sign-On authentication. After all, it saves time and is available on most websites, oblivious to the risks they may face if they do not take countermeasures. Moreover, the BitB attack offers the ability to spoof a legitimate URL by using HTML, CSS, and JavaScript to build a fake Single

Sign-On window displayed to the users, proving that it is easy to fabricate identical popups [3]. The BitB attack is a recent phishing attack in the browser, such as man-in-the-browser and browser-in-the-middle. However, the picture-in-picture attack, in which the attacker embeds a fake website within a legitimate website, and the BitB attack share some things in common [4]. For example, picture-in-picture has an actual outer window and a fake inner window, but the main difference (BitB) uses only the SSO window as a fake one. The Picture-in-Picture fake window is the whole website [5].

Attackers used a BitB attack to target the government and companies' websites, sending them a phishing link with a similar user interface and an inner browser containing a legitimate URL to request the user's credentials, which would later be used to access the user's

account [6]. In the Indian government, systems were blocked and to unlock them needs to pay INR 30000 [6]. Furthermore, in Ukraine, thousands of modems were disconnected from the network affecting the operations of 5,800 wind turbines belonging to the German company. There are temporary techniques done manually to detect BitB attempts on the webpages, such as the SSO popup windows, which cannot be dragged outside the outer window or maximized [7]. Also, the padlock icon in the browser header is a fake picture to mimic valid SSL certificates, and the popup theme differs from the browser or operating system theme [8]. The mentioned indicators require full awareness from the users and professionals in order to detect this type of attack, so it requires real-time solutions to increase awareness and reduce the attack risk before the user becomes a victim.

This paper presents a detailed analysis of the Browser-in-the-Browser attack, addressing a significant gap in knowledge in the field of cybersecurity. By providing the first published paper on this topic, it shows its risk and method of operation, in addition to the experimental results of the attack and ways to address it. The rest of the paper is organized as follows: Section 2 provides an overview of phishing and similar attacks to the BitB attack. Section 3 provides detailed background on the BitB attack, attack implementation requirements, and experimental results of a possible attack scenario. Section 4 concludes the paper.

## 2. Overview of Phishing

Phishing is the practice of stealing online users' financial and personal information by spoofing legitimate organizations [9]. According to the Anti Phishing Working Group (APWG) 1st Quarter, 2022 report, they recorded around one million phishing attacks. This was the worst phishing quarter that APWG has observed [10]. The phishing attack goes through a life cycle from the planning phase until the launch of the attack or the fraud. Planning is the first phase of the attack where the attacker plans to get the maximum earnings with minimum threats and identify the target. Then, the collection phase is where the attacker gathers information about the target and the methods that will be used in the attack. Finally, the attacker conducts fraud and steals the user's sensitive information [11].

Phishing attacks may result in the theft of data, mainly personal information including login information

and passwords for various online accounts. Mostly, phishers design fake web pages to look like legitimate web pages and have different but deceptive URLs [1]. However, today's attack works differently. The used URL looks correct and safe to the victim. The pop-up can display correct addresses when users hover the mouse over the webpage content links as our main research topic Browser-in-the-Browser attack [7]. So, looking into the URL is not enough as professionals were saying it is.

One of the solutions that help to detect phishing attacks is the browser plugins which are client-side detections that use different detection techniques such as blacklisting, and pattern matching [11]. For example, DontFishMe is a browser plugin that is used to detect online banking phishing websites to alert users before doing any financial transaction. Also, web shield-phishing protection is a plugin that alerts the users if the website is phishing or suspicious by red and green colours in sequence [11].

### 2.1. Browser-based Phishing Attacks

Web browser-based attacks use browsers, IT parts of web services and content management systems to gather login credentials, steal users' payment details, or infect systems with malware. It is an example of fileless attacks which are dangerous to organizations and difficult to detect. Most of them use browser third-party plug-ins like JavaScript Flash, and ActiveX since behavioural monitoring always leaves some exposure window and there are no links or files for security systems to identify [12]. Browser attacks are very popular and are likely to be successful on systems that have not been adequately hardened against them [13]. It has become an almost daily activity due to the rapid growth of the Internet and the development of the web to become a universal interface for creating many applications [14]. Some of the most popular browsers, like Mozilla Firefox, Microsoft's Edge, and Chrome, now come with at least a basic level of defence against these attacks.

#### 2.1.1. Man-in-the-Middle Attack (MitM)

Man-in-the-Middle (MitM) attack is a web browser-based attack in the field of computer security. This could begin with phishing tactics and in some cases coupled with browser attacks [15]. (MitM) attacks compromise the actual data that flows between endpoints, and the confidentiality, availability, and

integrity of the data itself [16]. The diversity of existing MitM attacks gives witness to the popularity of this attack category. Man-in-the-Browser (MitB) and Browser-in-the-Middle (BitM) are examples of the most common (MitM) attacks aimed at web services.

### 2.1.2. Man-in-the-Browser Attack (MitB)

The Man-in-the-Browser (MitB) attack is a browser-based attack that uses trojan horses as extensions to target web browsers. The trojan horse does not begin working until the victim connects to the institution's one-time pad (OTP) or public key infrastructure (PKI). Once the victim enters their credentials, the attacker will alter the exterior of the browser's contents. Such attacks usually target banking organizations and web financial institutions. The victim will not notice the change since it is happening in a real-time manner. This attack is dangerous because the anti-virus cannot detect it and can skip traditional authentication mechanisms such as OTP or two-step verification [17].

### 2.1.3. Man-in-the-Middle Attack (BitM)

Browser-in-the-Middle (BitM) is like (MitM) in the way it monitors the data flow between the service it accesses and the client, but it avoids some of MitM's common flaws. It could begin with phishing techniques and be combined with the Man-in-the-Browser (MitB) attack in some cases. One of its features is that there is no need for malware to be installed on the victim's machine, and the emphasis is on giving the attacker complete control [13]. The BitM attack replaces the victim's browser with a malicious transparent browser, acting and looking like the desired web page of the target site (e.g., a social network, a banking application, etc.), and hosted on the attack platform, over which the attacker has complete control, and keeping the victim completely unaware of the substitution. The victim will be able to browse the target web application while using a transparent web browser that has been unknowingly exposed by the malicious web server.

## 2.2. Picture-in-the-Picture Attack

A Picture-in-Picture attack is one of the phishing techniques that was recorded by APWG (Anti-Phishing Working Group) [4] in which the attacker embeds a fake website within a legitimate website as illustrated in Figure 1. This method is as effective as other phishing attacks such as homograph attacks which is using

similar characters to the original domain [18]. Moreover, the main reason behind the name of the Picture-in-Picture attack is that the attacker uses the fake browser address as an image inside the legitimate browser to mislead and lure the users that they are dealing with real websites to steal their sensitive information [19].

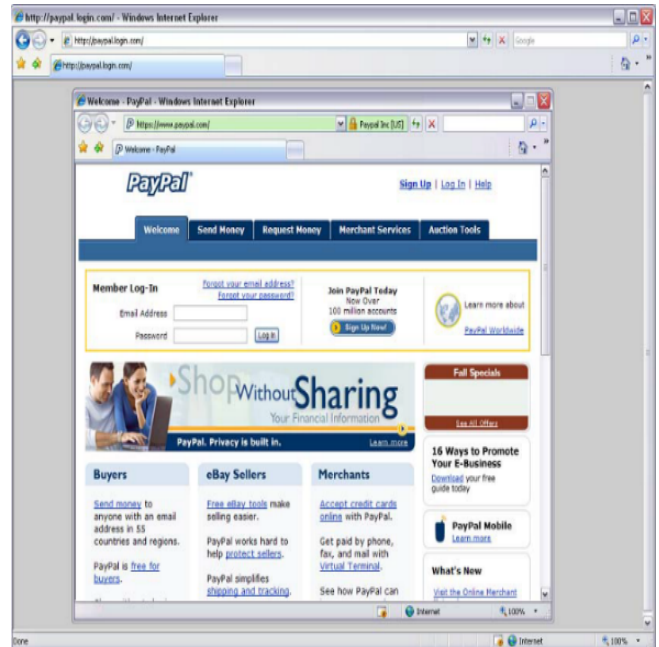


Figure 1: Picture-in-Picture attack. The outer window is real, and the inner window is fake [19].

Furthermore, several indicators help to detect the picture-in-picture attack [5]:

- Maximize the inner window: The fake inner windows cannot be maximized but is not a reliable sign of detection since there are many legitimate websites that use popups with a fixed size.
- Customize browser theme: Some of the browsers such as Chrome and Firefox provide the ability to change your browser's colours, so if the inner browser is mismatched with the outer browser, then that is a strong indication that there is something suspicious.
- Drag the inner window: The inner window in the picture-in-picture attack cannot be dragged outside the outer windows which could be a good indication of the attack but does not provide additional information about the legitimacy of the window.

One of the detection techniques that will help to mitigate the picture-in-picture attack is PhotoAuth is a two-factor authentication method that prevents real-time phishing attacks by taking picture of the browser address as a second authentication factor of the user authentication to detect the multiple browsers open

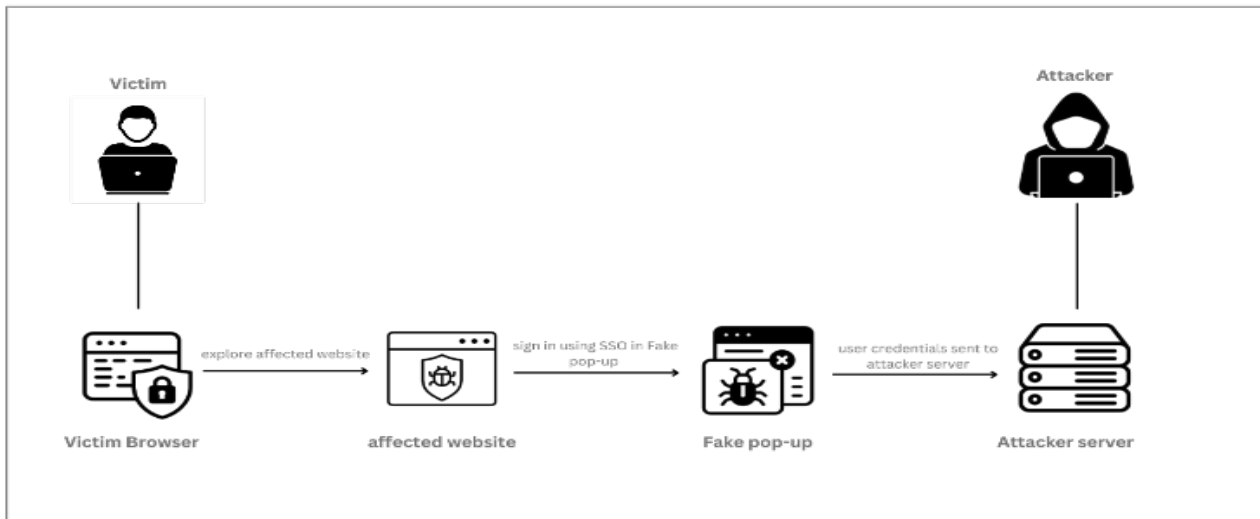


Figure 2: Browser-in-the-Browser (BitB) attack

and determine if the user visiting a real browser or phishing one [18].

### 2.3. Browser-in-the-Browser Attack (BitB)

A new attack recently appeared known as a Browser-in-the-Browser attack (BitB), which was first reported by a researcher called “Mr.d0x” [8]. This attack takes benefit of the popular third-party single sign-on options rather than the normally time-consuming process of filling out information to create a new account. The BitB attack is used in advance and is a more sophisticated phishing attack that going to trick users, by displaying a fake pop-up window containing a login panel on the visited website, which enables users to log in to several websites using a single account [3].

Among BitB attack features, when users want to sign up on a compromised site, they will be served with a fake bogus pop-up that looks and feels exactly like a legitimate Single Sign-On (SSO) authentication window. The BitB attack simulates a known company that provides SSO services to accomplish the attack, such as a Google, or Apple prompt, or Microsoft with the correct logo, input fields, and address bar, all the interface components they are accustomed to seeing. Also, when users move the mouse over the “Log in” button and the “Forgot password” link, the window can even display the correct addresses. If the user enters his/her credentials into this window, they will be redirected to the cybercriminal’s server rather than Google, Apple, or Microsoft [19].

BitB attack usually proceeds in basic steps, and the way how it is embedded on the website differs

from one attacker to another based on many factors. Figure 2 illustrates the possible scenario of a BitB attack.

The following steps show how to perform BitB attacks:

- a) The BitB attack takes advantage of the (SSO) pop-ups and creating these pop-ups is quite simple by using only HTML, CSS and JavaScript GitHub template provided by “mr.d0x”, or designing a new popup from scratch.
- b) The address bar of the fake popup spoofs the original domain to make the attack more convincing to the users.
- c) Pointing the iframe to the malicious server hosts the phishing page such as the Gophish toolkit [3]. As an example, `<iframe src=http://www.attacker.com ></iframe>` is to link the fake popup with the phishing website and receives the user’s credentials after clicking on the login button [20]. As seen in Figure 3, there are no noticeable differences between the fake and real popups of login with Facebook [3]

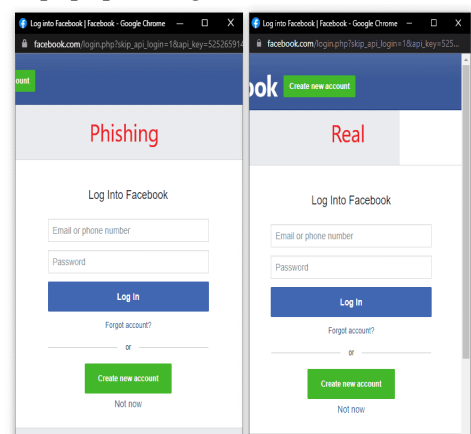


Figure 3: Legitimate SSO login vs fake SSO login [1]

Table 1: Overview of Various Browser-Based Security Attacks

	Description	Frequency	Level of exploitation attack vector	Discovery ability	Affect	Prevention
<b>Man-in-the-Middle Attack (MitM)</b> [21]	In a Man-in-the-Middle attack, someone secretly gets between two talking sides to spy or change the messages.	Broad	Hard	Hard	Normal to Harsh	<ul style="list-style-type: none"> <li>Steer clear of using WiFi undecrypted password networks.</li> <li>Heeding browser alerts that suggest a website is unsafe.</li> <li>Logging off from secure programs while not in use.</li> </ul>
<b>Man-in-the-Browser Attack</b> [17]	covertly manipulates online banking transactions by installing malware on the victims device	Broad	Hard	Normal to Hard	Harsh	<ul style="list-style-type: none"> <li>Employ Endpoint Supervision.</li> <li>Secure Browser Extensions.</li> <li>Utilize Secure Banking Utilities.</li> </ul>
<b>Browser-in-the-Middle Attack</b> [15]	Using a malicious transparent browser a browser-in-the-middle (BitM) attack places itself between the victims browser and the web server they are accessing.	Broad	Hard	Normal	Harsh	<ul style="list-style-type: none"> <li>Using a secure communication.</li> <li>Implementing network security measure.</li> <li>Using Multi-Factor authentication.</li> </ul>
<b>Picture-in-Picture Attack</b> [5]	Involves showing a fake browser window to users that appears to display a legitimate website, so the attacker can the tricks users into thinking they are on a real site when in fact they are on a fraudulent one.	Usual	Hard	Normal	Harsh	<ul style="list-style-type: none"> <li>Ensure that a link that opens an external website opens a new tab, not a new window. Attempt to drag a browser window outside of its parent window.</li> <li>Fake browser windows can't be maximized; therefore, if you find out that you can maximize the window, it might be a fake one.</li> </ul>
<b>Browser-in-the-Browser Attack</b>	An advanced type of phishing using 3rd-party single sign-on (SSO) preferences. It works by showing a spoofed pop-up window emulating the real style of third-party SSO login windows each time a user tries to log in to a breached site.	Usual	Normal	Hard	Harsh	<ul style="list-style-type: none"> <li>Check the SSL certificate of the pop-up SSO window</li> <li>Fake browser windows can't be maximized; therefore, if you find out that you can maximize the window, it might be a fake one.</li> <li>Ensure the SSO window does not contain iFrame element in its HTML code.</li> </ul>

### 3. Browser-in-the-Browser Attack

#### 3.1 Real-world BitB attack scenario and detection

Today, browser-in-the-browser attack is a significant threat to many online services. It was first described by the researcher in the Spring of 2022 when he revealed an analysis of the attack and how it works [22]. This attack aimed at government entities, including Ukraine and other such sectors [23]. Since almost all users use (SSO), this attack can affect a large variety of users [3]. One real example that is the latest happening was targeting video gamers, specifically the Steam application for playing, discussing, and creating games. Attackers started targeting victims with direct messages by inviting them to join a team to compete. The shareable link brought the targets to a phishing site for what appears to be an

organization hosting Esports “electronic sports” competitions. Then, the visitors are requested to log in via their Steam account to join a team [24]. The new login page window is a fake window created within the current page using the <iframe> tag in HTML, making it very hard to spot as a phishing attack. The landing pages define the language from the victim's browser preferences and load the correct one, it supports 27 languages. The victim is then prompted to submit the two-factor authentication code on a new form after entering their credentials. To reduce the possibility that the victim would discover the attack, the user is redirected to a legitimate URL address. The victim's login information has already been taken and delivered to the threat actors at this stage. Then attackers modified the victims' email addresses and passwords to

make it more challenging for them to regain control of their accounts [24].

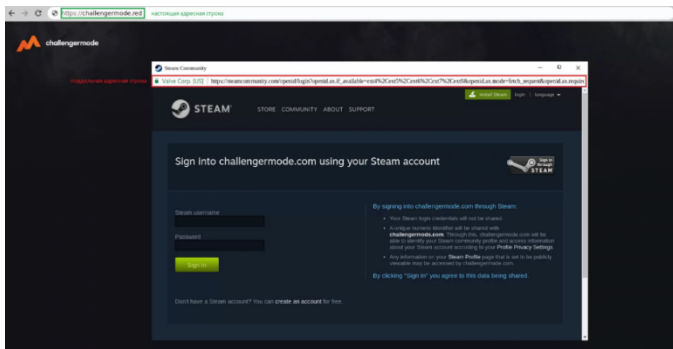


Figure 4: Phishing window created inside the phishing site [24].

There are several temporary techniques to detect BitB attacks on websites which are done manually by users. Below are listings of some indicators that exist some/all of them confirm the BitB attack:

- The (SSO) popup window cannot be dragged out of the outer window [7].
- The lock icon on the popup as seen in Figure 4 is a picture, not a valid SSL certificate.
- Cannot minimize the (SSO) popup window [7].
- Existing the iframe element in the HTML code [8].

Till now no actual prevention techniques developed yet. But there are some known procedures that can reduce the occurrence of such phishing attacks, like verifying a Site's Security and thinking before clicking, etc.

### 3.1 BitB implementation requirements

A BitB attack's success is determined by how well the SSO popup mimics a legitimate browser login popup, such as the browser header with a padlock symbol, a legitimate URL, operating system, and the use of one of the SSO service providers, such as Google, Facebook, and Steam. The SSO popup is created using HTML, CSS, and JavaScript only, so there is no limitation to the attacker's creativity. The malicious website that is controlled by the attacker can be sent using social engineering with a convincing domain name and offers an SSO option that shows a popup window to steal the user's credentials.

The popup spoofs a legitimate URL for Google login that is placed in the fake browser header with a padlock symbol to lure the user into believing there is a secure connection and uses JavaScript to mimic browser buttons such as close, minimize, and maximize. Also, the popup contains an iframe HTML tag that points to the attacker's

server hosts that mimic the SSO login for Google to be displayed to the users. The iframe phishing link is made by any available phishing tool, and in our case, we will use the PyPhisher tool on the Linux operating system. PyPhisher is a python-based tool that offers phishing links for various social platforms such as Twitter, Facebook, and others [25]. For the sake of clarity, the attack steps are the following:

1. The URL for the malicious website that is controlled by the attacker is sent to the victim via social engineering.
2. The victim enters a malicious website by clicking on the URL. This can be done using any known web browser, such as Chrome, Firefox or any others.
3. The victim then selects the SSO as a login option, which shows a login popup for Google.
4. The phishing link placed in the iframe HTML tag waits for the victim to log in to capture their credentials.
5. The victim provides his or her login information via the username and password parameters.
6. The login popup indicates that there is a login error.
7. The attacker on the background of this scenario captures the credentials from the phishing link and proceeds to the next step of the attack.

### 3.2 BitB experimental results

In this section, the main objective is to discuss the implementation of the BitB attack from the perspective of both the attacker and the victim. An examination of the steps involved in executing the attack will be conducted, as well as the tools and processes utilized by the attacker. The purpose of this section is to provide a comprehensive and informative discussion that sheds light on the mechanics of the BitB attack by carefully examining these components. Additionally, it provides insight into its potential impact on targeted systems. Overall, this section will serve as a valuable resource for individuals seeking to gain a deeper understanding of the BitB attack and its implications.

The SSO pop-up was selected for the experiment because it allows login at any website through a trusted third party that is not easily suspected by the victim, and it has a known URL link. The same experiment may be tried with any websites that offer third-party SSO services (Facebook, Microsoft, Apple, etc.). The scenario



is the one described in the “Browser-In-The-Browser (BitB) Attack” section. The testbed is set up as follows:

- Victim: The victim visits the attacker's website through social engineering techniques providing him with the website link or simply by searching the internet and reaching our website.
- Attacker’s platform: is set up on GNU/Linux distribution for its easily customizable.
- Web application target: The attacker’s website accessible through any browser, has been selected as the target. It is assumed the victim owns an active account within Google which enables them to log in through Google SSO service. Also, google SSO was selected on account of being very popular and the method here int
- produced applies exactly in the same way to any website that provides SSO service (Microsoft, Apple, etc.).

As highlighted in Figure 5, the user reaches the website that was created by the attacker through browsing the internet or receiving the link using social engineering techniques.

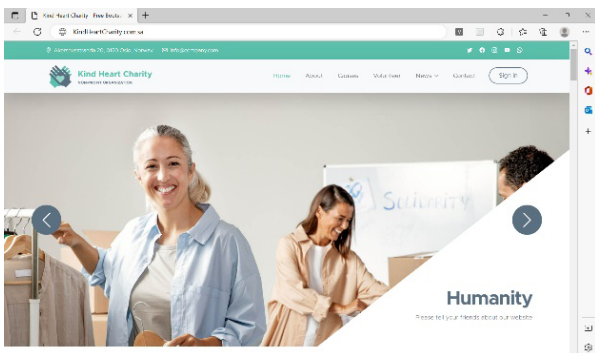


Figure 5: A website made by the attacker

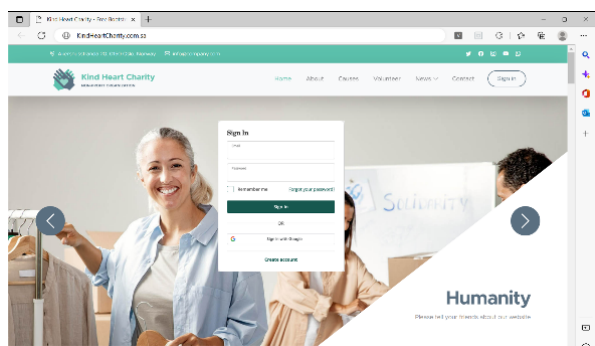


Figure 6: The user tries to sign in to the attacker’s

The user tries to log in to the website, he starts filling in the credentials if he/she already has an account on the attacker’s website or logs in through Google SSO service. Otherwise, he/she can create an account on the attacker’s website. In our case let’s assume the victim preferred to sign in through his/her google account.

After the victim clicks on "Sign in with Google" as shown in Figure 6 the fake popup within the attacker’s website will appear. The SSO popup is created using HTML, CSS, and JavaScript in a way that looks like the original popup and is hard for the victim to detect as a fake. As shown in Figure 7, the popup's URL looks legitimate and includes a padlock symbol to lure the user into believing there is a secure connection. The phishing link is placed in the iframe HTML tag, so it will appear inside the popup. As demonstrated in Figures 7 and 8, the victim will start entering his credentials by entering his e-mail and then his password. After stealing the victim's credentials, the attacker has the option to perform, depending on the attacker's scenario: either redirect the victim to the Google website or close the fake popup and so on.

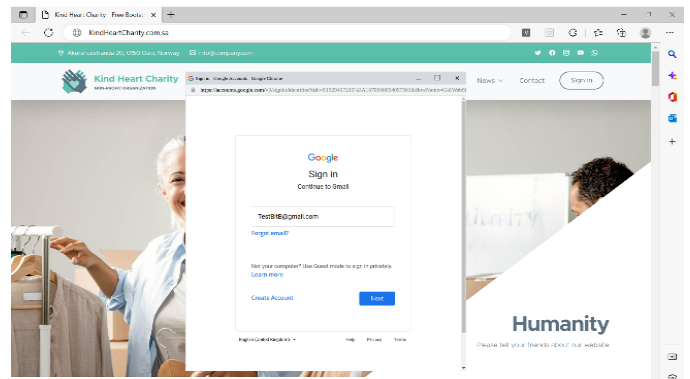


Figure 7: Attacker website provides a fake SSO

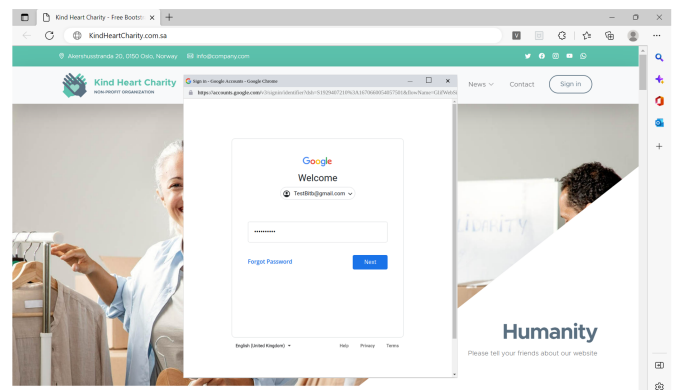


Figure 8: Attacker websites collect users’ credentials through a fake SSO (BitB attack)

On the attacker side, all google account credentials of victims will be received as shown in Figure 9. As a further step to bypass two-factor authentication, the attacker can specify a text box for filling in the authentication code which can appear after Figure 7. At this moment the attacker starts filling in these credentials on the legitimate google, and when it asked for the credentials code it will be received by the attacker server when the victim filled it in on the attacker’s website.

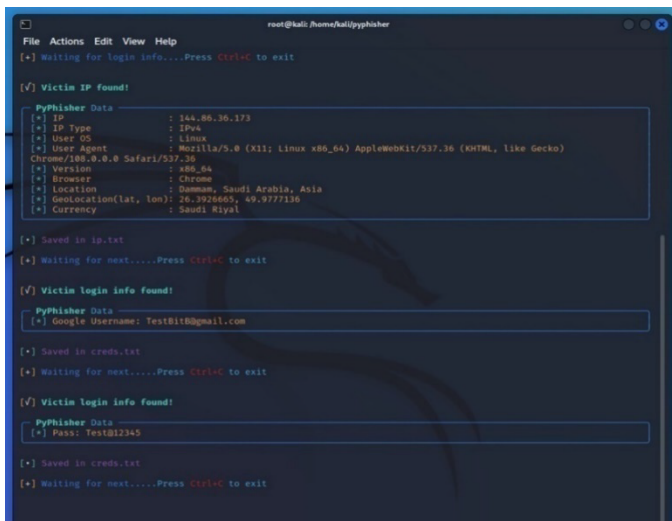


Figure 9: Attacker is capturing the Google account credentials of the victim

As the simple example here documented demonstrates, it was possible to carry on a successful attack without exploiting zero-day or any other known vulnerability at the two endpoints (the victim PC and the official SSO service, instead attacker obtains its own fake SSO) or in the communication channel. Also, the attack was entirely conducted in a remote location, simply by improper use of known technologies.

#### 4. Conclusion

The present study shows that the attack is not easy to discover, since the URL matches the legitimate address. From the user side, the best practice to avoid this kind of attack is to put extreme care into identifying the target SSO service, by trying to interact with the address bar and padlock image before filling in credentials (e.g., if BitB is the case, the address bar will be just a CSS and HTML code not interactable) and, after that, try dragging the suspect window outside the main browser window that contains it. A real browser window will behave independently, while a fake browser window will be “imprisoned” inside the real window it’s shown in.

This paper aims to be the first publication to explain and analyze the recently appeared BitB attack, which is considered a serious threat to web users, especially those who used to log into websites with SSO services. Additionally, it introduces some temporary manual countermeasures to protect against this attack, since no automated solution discovered yet. Furthermore, it shows the experimental results of the BitB attack and its significant impact on a user not sufficiently aware of the risks behind SSO services. Since it aims to steal user credentials as it is in this attack.

In future work, the authors intend to innovate an automatic solution for BitB that prevents and protects the user from such an attack. The solution will be a web extension or plugin that is used to detect BitB attacks based on a set of thoughtful indicators. This will enable the user to be warned before they fall victim to this attack.

#### Conflict of Interest

The authors declare no conflict of interest.

#### Acknowledgment

The authors acknowledge SAUDI ARAMCO Cybersecurity Chair for the support.

#### References

- [1] B. Geyik, b. Erensoy and E. Kocyigit, "Detection of Phishing Websites from URLs by using Classification Techniques on WEKA," Coimbatore, India, 2021.
- [2] S. D. Singh, "BITB (browser in the browser)Attack," InfoSec Write-ups, 14 April 2022. [Online]. Available: <https://infosecwriteups.com/bitb-browser-in-the-browser-attack-e2008c405701>
- [3] V. Lisa, "Browser-in-the-Browser Attack Makes Phishing Nearly Invisible," Threatpost [Blog], 2022.
- [4] R. M. Bian, "Alice in battlefield: an evaluation of the effectiveness of various UI phishing warnings," 2013. [Online]. Available: <https://www.cs.auckland.ac.nz/compsci725s2c/archive/termpapers/725mbian13.pdf>. [Accessed 19 September 2022].
- [5] C. Jackson, D. Simon, D. Tan and A. Barth, "An evaluation of extended validation and picture-in-picture phishing attacks," in International Conference on Financial Cryptography and Data Security, 2007.
- [6] "Novel Phishing Technique Browser-in-the-Browser Attack Targets Government Websites," June 2022. [Online]. Available: <https://cloudsek.com/>. [Accessed 9 October 2022].
- [7] L. Grustniy, "Browser-in-the-browser attack: a new phishing technique," Kaspersky, 25 April 2022. [Online]. Available: <https://www.kaspersky.com/>. [Accessed 16 September 2022].
- [8] Lebedev and D. Eroshev, "Hackers use the browser-in-the-browser technique to steal Steam accounts," 13 September 2022. [Online]. Available: <https://blog.group-ib.com/steam>. [Accessed 21 September 2022].
- [9] K. Jain and B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," Enterprise Information Systems, vol. 16, no. 4, pp. 527-565, 2022.
- [10] A.-P. W. Group, "Phishing Activity Trends Report, 1st Quarter 2022," 2022.
- [11] N. Chandru, "A Review on Phishing Attacks and Anti-Phishing Browser Plugins," International Journal of Computer Science & Engineering Technology (IJCSSET), vol. 9, no. 5, pp. 51-58, 2018.
- [12] S. M. Mohamed, N. Abdelbaki and A. F. Shosha, "Digital forensic analysis of web-browser based attacks," in The Steering Committee of The World Congress in Computer Science,

- Computer Engineering and Applied Computing (WorldComp), USA, 2016.
- [13] J. Andress, "Chapter 3 - Authorization and Access Control," in *The Basics of Information Security (Second Edition)*, Syngress, 2014, pp. 39-56.
- [14] G. F. He, T. Zhang, Y. Y. Ma and J. X. Fei, "Protecting User's Privacy from Browser-Based Attacks," in *Applied Mechanics and Materials*, 2014, pp. 941-945.
- [15] F. Tommasi, C. Catalano and I. Taurino, "Browser-in-the-Middle (BitM) attack," *International Journal of Information Security*, vol. 21, no. Springer, pp. 179-189, 2022.
- [16] M. Conti, N. Dragoni and V. Lesyk, "A survey of man in the middle attacks," *IEEE communications surveys*, vol. 18, no. 3, pp. 2027-2051, 2016.
- [17] P. J. Kumar, W. Hu, X. Li and K. Lal, "Mobile Banking Adeptness on Man-In-The-Middle and Man-In-The-Browser Attacks," *IOSR Journal of Mobile Computing \& Application*, vol. 4, pp. 13-19, 2017.
- [18] Y. Sun, S. Zhu, Y. Zhao and P. Sun, "Let Your Camera See for You: A Novel Two-Factor Authentication Method against Real-Time Phishing Attacks," *arXiv preprint arXiv:2109.00132*, 2021.
- [19] D. DAS, "What Is a Browser-in-the-Browser Attack and How Can You Protect Yourself?," *makeuseof*, 24 June 2022. [Online]. Available: <https://www.makeuseof.com/what-is-browser-in-the-browser-attack/>. [Accessed 2022].
- [20] M. G. Alkhozai and O. . A. Batarfi, "Phishing websites detection based on phishing characteristics in the webpage source code," *International Journal of Information and Communication Technology Research*, vol. 1, no. 6, pp. 283-291, 2011.
- [21] E. A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *International Journal of data and Network Science*, vol. 2, no. 2, pp. 109-134, 2018.
- [22] Mr.d0x, "Browser In The Browser (BITB) Attack," 15 March 2022. [Online]. Available: <https://mrd0x.com/browser-in-the-browser-phishing-attack/>. [Accessed 20 September 2022].
- [23] "Browser in the Browser" attacks: A devastating new phishing technique arises," 1 April 2022. [Online]. Available: <https://www.techrepublic.com/>. [Accessed 19 9 2022].
- [24] B. Toulas, "Hackers steal Steam accounts in new Browser-in-the-Browser attacks," 12 September 2022. [Online]. Available: <https://www.bleepingcomputer.com/news/security/hackers-steal-steam-accounts-in-new-browser-in-the-browser-attacks/>. [Accessed 20 9 2022].
- [25] M. Shariq, "Pyphisher - simple python tool for phishing," *GeeksforGeeks*, 21 April 2022. [Online]. Available: <https://www.geeksforgeeks.org/pyphisher-simple-python-tool-for-phishing/>. [Accessed 10 December 2022].

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

# Analyzing the Impact of Optical Wireless Communication Technologies on 5G/6G and IoT Solutions: Prospects, Developments, and Challenges

Ramsha Khalid<sup>1,2</sup>, Muhammad Naqi Raza<sup>1</sup>

<sup>1</sup> Department of Electrical Engineering Technology, University of Sialkot, Sialkot, 51310, Pakistan

<sup>2</sup> Department of Electrical Engineering, University of Lahore, Lahore, 53720, Pakistan

\*Corresponding author: Ramsha Khalid, University of Sialkot, Sialkot, Pakistan Email: [ramshakhalid2404@gmail.com](mailto:ramshakhalid2404@gmail.com)

**ABSTRACT:** The imminent 5G and 6G communication systems are projected to exhibit substantial advancements in comparison to the current 4G communication system. Several critical and prevalent concerns pertaining to the service quality of 5G and 6G communication systems encompass elevated capacity, extensive connectivity, minimal latency, robust security measures, energy efficiency, superior quality of user experience, and dependable connectivity. Undoubtedly, 6G communication is expected to offer markedly improved performance across these domains compared to 5G communication. The integration of the Internet of Things (IoT) within the framework of the tactile internet is anticipated to be a fundamental component of advanced communication systems, encompassing both 5G and beyond (5GB), such as 5G and 6G. Consequently, 5GB wireless networks will encounter various challenges in accommodating diverse types of heterogeneous traffic and meeting the specified parameters related to service quality. Optical wireless communication (OWC), alongside various other wireless technologies, emerges as a promising candidate to fulfill the requisites of 5G communication systems. This comprehensive review articulates the efficacy of OWC technologies, including Visible Light Communication (VLC), Light Fidelity (LiFi), Optical Camera Communication (OCC), and Free Space Optics (FSO) Communication, as a viable solution for the successful deployment of 5G/6G and IoT systems.

**KEYWORDS:** 5G, 6G, internet of things, heterogeneous traffics, wireless technologies, communication systems, Optical Wireless Communication

## 1. Introduction

In recent times, OWC technologies have garnered significant research attention owing to their notable features [1–5]. OWC designates wireless connectivity utilizing the optical spectrum. OWC has positioned itself as a favored complementary technology to Radio Frequency (RF)-based wireless technologies, particularly in the context of future communication networks, encompassing the 5G and 6G communication systems. OWC technologies exhibit several notable features, including broad spectrum coverage, high data rates, minimal latency, robust security, cost-effectiveness, and energy efficiency. These attributes effectively cater to the demanding specifications of 5GB communications, exemplified by 5G and 6G technologies. In addition to this, the IoT network is gaining significant importance, with a proliferation of end-user devices or sensors being

interconnected within IoT. Furthermore, the integration of tactile internet will emerge as a pivotal aspect of future IoT, facilitating real-time communication systems across various societal, industrial, and commercial applications. In visualizing the concept of IoT, there is an exponential surge in the quantity of physical devices connected to the internet [6]. Hence, the IoT generates a substantial volume of data. OWC technologies assume a crucial role in sensing, monitoring, and facilitating resource sharing within the extensive device connectivity of IoT networks [2,6]. Additionally, OWC can effectively fulfill the low-power consumption and stringent security requisites of IoT.

The specifications for the 5G communication system have been finalized, and it is anticipated that 5G will be fully implemented by 2020 [7]. The forthcoming 5G communication infrastructure will introduce novel services characterized by exceptionally high Quality of

Service (QoS). Key attributes of 5G communication services will encompass unparalleled system capacity, minimal latency, enhanced security measures, extensive device connectivity, minimal energy consumption, and exceptional Quality of Experience (QoE) [7–11]. The introduction of the 6G communication system is projected to occur within the timeframe spanning 2027 to 2030. While the precise specifications for 6G have yet to be defined, numerous researchers are actively engaged in its development [12–16]. Research challenges encompassing capacity enhancement, augmented connectivities, latency reduction, heightened security, improved energy efficiency, elevated user QoE, and enhanced reliability are focal points addressed by both the 5G and prospective 6G communication systems. The forthcoming 6G communication infrastructure is anticipated to serve as a global communication cornerstone, offering service levels significantly superior to those of 5G.

RF currently serves as a prevalent choice for diverse wireless connectivity needs. However, RF-based wireless communication encounters significant hurdles, including spectrum limitations, susceptibility to interference, and stringent regulatory constraints. Sole reliance on RF technologies proves inadequate in meeting the demands of 5G and IoT networks. Consequently, researchers are diligently exploring alternative spectrums to address the escalating requirements. One particularly promising avenue involves leveraging a significantly expansive optical band. This strategic shift toward OWC holds considerable potential for advancing 5G and IoT networks, offering distinct advantages over conventional RF-based networks. These advantages encompass heightened data rates, diminished latency, enhanced security, and improved energy efficiency [1–3], [6]. Effective communication spans distances ranging from a few nanometers to over 10,000 kilometers, facilitated by the implementation of various OWC systems [2]. Key technologies integral to OWC networks comprise VLC [6][17–19], LiFi [20–22], OCC [23–27], and FSO [28–30]. A subsequent section provides a concise exploration of the distinctions and commonalities inherent in these technologies. Each of these technologies possesses unique strengths alongside certain limitations. Diverse OWC technologies present a spectrum of services catering to indoor, outdoor, and space communications. Consequently, OWC technologies assume a crucial role in realizing the objectives of 5G and IoT systems.

Our prior review paper concerning OWC [2] extensively examines and compares various optical wireless technologies, offering a comprehensive understanding of their distinctions. However, the primary objective of the current review paper diverges from providing a detailed explanation of OWC technologies. Instead, its focus is on illustrating how

OWC technologies can serve as an effective solution for the seamless deployment of 5G/6G and IoT systems. Within this study, we delineate potential detailed solutions for 5G/6G and IoT utilizing diverse OWC networks. This paper's contributions can be succinctly outlined as follows:

1. Comprehensive examination of the key characteristics of 5G and IoT networks, with a brief presentation of potential 6G requirements.
2. Concise discussion of various OWC technologies within the context of 5G/6G and IoT systems.
3. Detailed exploration of the scope of OWC technologies in meeting the specific requirements of 5G/6G and IoT deployments.
4. Thorough survey of recent advancements in OWC technologies pertaining to 5G and IoT solutions, accompanied by a discussion on emerging research trends.
5. In-depth consideration of challenging issues associated with the deployment of OWC for 5G/6G and IoT solutions.

The subsequent sections of the paper are structured as follows: Section 2 furnishes a concise overview of the requirements associated with 5G, 6G, and IoT. Section 3 provides an in-depth description of various OWC technologies. In Section 4, the potential of OWC technologies to address the demands of 5G, 6G, and IoT systems is elucidated. Section 5 delves into several key challenging issues inherent in OWC-based 5G/6G and IoT solutions. Finally, Section 6 encapsulates the conclusion of this paper.

## 2. Concise Examination of the Requirements for 5G, 6G, and IoT

5G is anticipated to deliver a significant enhancement in key attributes compared to 4G, enabling efficient support for the burgeoning array of heterogeneous multimedia applications with varying requirements [11]. The specifications for 5G requirements have been delineated, with full deployment of the 5G system anticipated by 2020. The essential requirements of 5G can be succinctly summarized as follows:

- *High Traffic Volume:* The mobile data volume per unit area is projected to increase by a factor of 1000 in comparison to 4G wireless networks, accompanied by a surge in the number of connected wireless devices, which is expected to be 100 times higher.
- *Massive Connectivity:* 5G is designed to facilitate massive connectivity, with the capability to connect ten to 100 times more devices than the 4G communication system [11].

- *High User Data Rate Link:* The 5G networks are mandated to support exceptionally high user data rates, enabling users to achieve up to 10 Gbps, representing a ten to 100-fold increase compared to 4G.
- *Low-Energy Consumption:* Significantly reduced energy consumption is a pivotal requirement in the 5G communication system, aiming to achieve more than a 90% reduction, i.e., 10 times lower compared to 4G networks [11].
- *Extremely Low Latency:* Ensuring extremely low latency, with end-to-end latency levels ranging from sub-millisecond to a few milliseconds, is a critical objective for 5G networks [11].

Researchers are currently engaged in the standardization of requirements for 6G networks [12–16,31–34]. A pivotal requirement for 6G is anticipated to be ultra-high bit rates per device, ranging from tens of gigabits per second to terabits per second [12,31]. Furthermore, 6G is projected to exhibit 1000 times higher simultaneous wireless connectivity compared to 5G. Envisaged characteristics for 6G encompass ultra-long-range communication coupled with ultra-low-power consumption, ensuring user experiences with latency of less than 1 millisecond [13]. Other key anticipated features of 6G include spatial multiplexing, higher spectral efficiency at 100 bits per second per Hertz, ultra-high wireless security, exceptional reliability, ultra-low-power consumption, and the integration of massively connected complex networks.

The networks will possess distinct characteristics designed to accommodate the demands of 5G wireless communication systems. The essential features of future 5G and 6G networks can be encapsulated as follows:

- *Ultra-High-Density Network:* To ensure consistent QoE, accommodate massive connectivity, and meet high capacity demands, 5G networks are anticipated to exhibit significantly higher density, characterized by ultra-dense heterogeneous networks, compared to their 4G counterparts.
- *Small-Cell Networks:* The establishment of high-density small-cell networks is identified as a fundamental characteristic in the design of 5G communication systems.
- *Higher Spectral Efficiency:* 5G systems are poised to optimize frequency spectrum utilization through the incorporation of multiple-input and multiple-output techniques, advanced coding and modulation schemes, and innovative waveform design. The targeted spectral efficiency for 5G is set to be at least three times higher than that of 4G networks.

- *Low Cost:* A key objective for 5G systems is to achieve a 100-fold increase in efficiency compared to 4G systems, delivering a hundred times more data traffic using the same energy across the network. This necessitates the adoption of low-cost network equipment, reduced deployment expenses, and enhanced power-saving functionalities on both network and user equipment sides [35].
- *Offloading Heavy Traffic to Indoors:* Recognizing that nearly 80% of mobile traffic is generated indoors, a strategic characteristic of 5G and 6G networks involves offloading this substantial data volume to indoor small cells. This approach aims to alleviate the strain on macrocells, preserving valuable resources and enhancing overall network efficiency [36].

### 3. Brief Overview of OWC Technologies

The four primary OWC technologies, namely VLC, LiFi, OCC, and FSO, are regarded as promising solutions to address the requirements of 5G/6G and IoT networks due to their unique features. Figure 1 provides a concise depiction of the architectures of these technologies [37]. In terms of infrastructure, these technologies exhibit variations in transmitter types, receiver configurations, and communication media. VLC utilizes light-emitting diodes (LEDs) or laser diodes (LDs) as transmitters and photodetectors (PDs) as receivers, utilizing only visible light (VL) as the communication medium. LiFi, akin to Wireless Fidelity (WiFi) technology, offers high-speed wireless connectivity alongside illumination, employing LEDs or diffuse LDs as transmitters and PDs as receivers. While VL serves as the forward path medium, LiFi employs infrared (IR) for the return path communication, although VL can also be utilized for the return path. However, the uplink communication performance in both VLC and LiFi may be constrained as receiver devices in most user equipment, such as smartphones, are not equipped with high-power LEDs [38–40]. Furthermore, they exhibit limitations in return path performance when the uplink involves diffused light, facing significant interference from the downlink lights. OCC employs an LED array or light as a transmitter, with a camera or image sensor serving as the receiver. The inclusion of built-in complementary metal-oxide semiconductor cameras enhances the capability to capture photos and videos [41]. The camera can be of either global shutter or rolling shutter type [42]. OCC typically utilizes VL or IR as the communication medium, although the ultraviolet (UV) spectrum can also be employed. FSO technology commonly employs a LD and PD as the transmitter and receiver, respectively. However, heterodyne optical detection receivers are also utilized in FSO communication. Typically, it operates using IR as the communication medium but can also utilize VL and UV. Table 1 outlines a comparison of performance metrics

across various OWC technologies [37]. These technologies exhibit distinct differences, with each offering specific characteristics. Notably, VLC distinguishes itself by employing visible light as its communication medium. A LiFi system is required to support seamless mobility, bidirectional communication, point-to-multipoint, and multipoint-to-point communications. Among all OWC technologies, only the OCC system utilizes a camera or image sensor as a receiver. Leveraging the narrow beams of focused light from a LD transmitter, FSO systems can establish both long-distance and high-data-rate communication links. For further insight into the variances among OWC technologies, refer to our previous work [2].

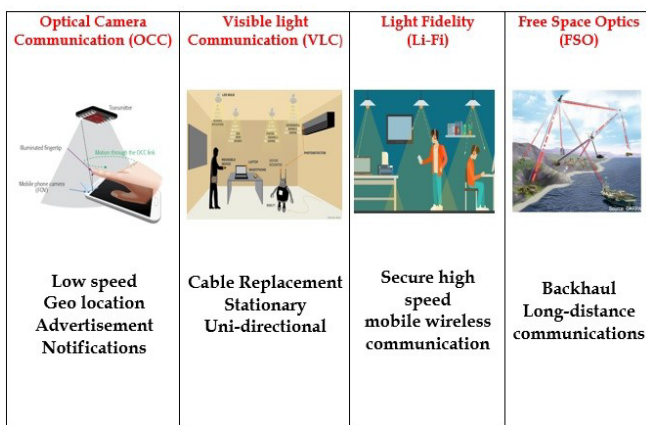


Figure 1: Taxonomies of OWC for 5G, 6G, and Internet of Underwater Things Communications.

## 4. OWC Technologies for the 5G, 6G, and IoT Solutions

### 4.1. Advantages of Opting for OWC Technologies

The RF band spans from 3 kHz to 300 GHz within the electromagnetic spectrum [2]. However, the range of 3 kHz to 10 GHz is predominantly utilized by existing wireless technologies due to its favorable communication properties. This spectrum is nearing exhaustion and falls short in meeting the high demands of 5G/6G and IoT networks. Additionally, it is subject to stringent regulations imposed by local and international authorities.

OWC emerges as a compelling alternative, offering outstanding features to address these stringent requirements. OWC finds application across a diverse range of scenarios, including machine-to-machine, device-to-device, chip-to-chip, vehicle-to-vehicle, vehicle-to-infrastructure, infrastructure-to-vehicle, point-to-point, and point-to-multipoint communications [2,6,29]. The inherent properties of light enable connectivity across a wide range, spanning from nanometers to over 10,000 km. This facilitates various communication scenarios, such as ultra-short-range inter-chip interconnects using FSO systems and in-body networks employing VLC, OCC, or LiFi systems. Other applications encompass short-range LiFi, vehicle-to-everything (V2X) communications, indoor positioning, medium-range inter-building networks, long-range inter-city backhaul connectivity, and extended-range satellite-to-satellite communications.

Furthermore, OWC technologies offer the capability to establish high-data-rate communication links. Key features of OWC encompass a wide unregulated bandwidth, enhanced security measures, low power consumption, cost-effectiveness in infrastructure and device deployment, absence of interference with RF devices and networks, high Signal-to-Noise Ratio (SNR), and seamless integration into existing lighting infrastructures. However, a notable limitation of OWC systems is the susceptibility to transmission blockage by obstacles.

The coexistence of RF and OWC networks presents an effective strategy for mitigating the limitations inherent in individual RF-based and optical wireless communication systems. Figure 2 showcases several notable 5G/6G and IoT platforms leveraging OWC technologies [37]. OWC networks have the capacity to support a myriad of applications across various aspects of daily life, including V2X communications, underwater communications, cellular connectivity support, space communication, smart shopping, eHealth, and smart home systems. This section elucidates how OWC networks can deliver effective solutions for the deployment of 5G, 6G, and IoT networks.

Table 1: Performance Metric Comparison Across Different Optical Wireless Communication Technologies [2,18,20,24,28,43]

Problem	Parameter	VLC	Lifi	OCC	FSO
Topology of communication	Direction	Uni or Bi-direction	Bi-direction	Uni-direction	Uni or Bidirection
Area of Communication	Distance	20m	10m	60m	10,000km
Deployment	support for mobility	Not- compulsory	compulsory	Not- Compulsory	No
Effect on environment	Indoor/ Outdoor	No/Yes	No/Yes	No	Yes
Obstruction	Level of Interference	Low	Lows	Zero	Low
Speed of communication	Data rate	100Gbps using LD and 10Gbps using LED	100Gbps using LD and 10Gbps using LED	55Mbps	40Gbps
Network Performance	Security (related to data encryption and protection measures)	High	High	High	High

4.2. Achieving Service Quality Characteristics

**Substantial Capacity Enhancement:** Achieving thousand-fold capacity improvements in 5G networks necessitates a significantly broader bandwidth, a requirement readily met by the optical spectrum. Table 2 provides a comparison of RF and optical frequencies within the electromagnetic spectrum [44]. The RF band occupies merely 300 GHz of this vast spectrum, while the optical band (ranging from 300 GHz to 30 PHz) offers considerably greater potential. Currently, only a fraction of the optical spectrum, encompassing parts of visible light, near-infrared, and middle ultraviolet, is actively utilized. However, ongoing research aims to expand utilization across the optical spectrum and enhance its efficiency. Notably, the terahertz band (0.3–3 THz) within the infrared region is anticipated to play a crucial role in future high-data-rate cellular communications [31]. Leveraging the expansive optical spectrum through various OWC technologies presents an opportunity to accommodate the substantial data capacity requirements. Additionally, high-speed network connectivity is imperative to support the extensive connectivity demands of massive IoT deployments. Thus, the optical spectrum holds promise in handling the substantial data traffic generated by high-data-rate heterogeneous multimedia applications in 5G, 6G, and IoT networks.

rate of 100 Gbps [18,45]. FSO technology also excels in supporting high-data-rate services both indoors and outdoors, facilitating outdoor remote high-speed connectivity. Additionally, OWC utilizing the UV band extends its capabilities to offer high-data-rate, non-line-of-sight communications [4]. Ongoing research initiatives aim to further elevate data rates within OWC technologies. Consequently, OWC technologies emerge as valuable complementary solutions for enabling high-data-rate connectivity in 5G, 6G, and advanced communication systems. As illustrated in Figure 3, a diverse array of OWC technologies facilitates high-speed connectivity scenarios for both indoor and outdoor users, as well as in V2X communications, offering promising prospects for supporting advanced communication systems beyond 5G and 6G [44].

Table 2: Comparison of RF and optical spectra [2–6,21,29]

Property	RF Spectrum	Optical Spectrum
Frequency Range	Limited (3 kHz to 300 GHz)	Extensive (300 GHz to 30 PHz)
Bandwidth	Restricted	Broad
Utilized Spectrum	Primarily below 300 GHz	A small portion (Visible light, near-infrared, middle ultraviolet) actively used
Future Research	Limited expansion potential	Ongoing research to explore and expand utilization
Emerging Band	Terahertz band (0.3–3 THz) within infrared	Potential for high-data-rate cellular communications in terahertz range [31]
Communication Medium	Radio waves	Light waves
Interference Potential	Susceptible to interference due to crowded spectrum	Lower interference potential as optical spectrum is underutilized
Capacity Potential	Limited capacity due to spectrum congestion	High capacity potential due to broad spectrum availability

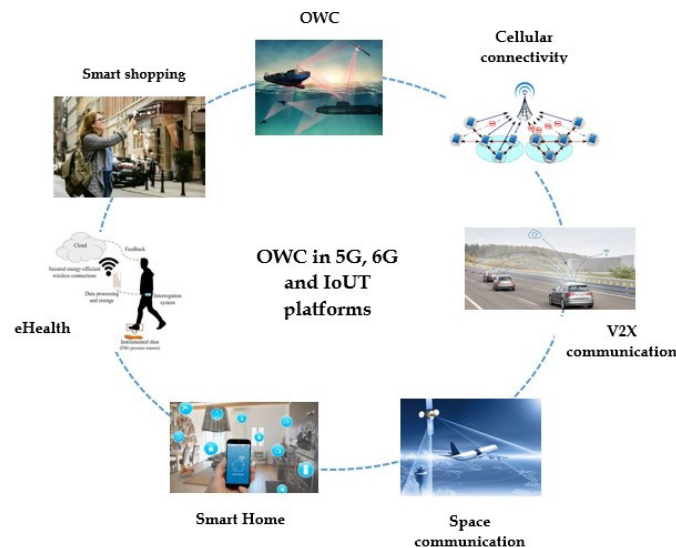


Figure 2: OWC networks for the 5G/6G and IoT platforms.

**Ultra-High User Data Rate:** The anticipated transmission rates for 5G mobile communication systems are projected to average around 1 Gbps, with a peak rate of 10 Gbps [8]. Subsequently, 6G is expected to support even higher bit rates ranging from tens of Gbps to Tbps per device. Notably, VLC and LiFi technologies demonstrate the capability to deliver exceptionally high-data-rate services at the user level. LiFi, in particular, offers comprehensive network support, encompassing point-to-multipoint, multipoint-to-point, and bidirectional communications akin to WiFi. VLC has already achieved a confirmed data

**Ultra-low latency:** Achieving low latency is a critical requirement for communication systems, especially in the context of 5G and beyond. OWC systems typically operate along line-of-sight (LOS) paths, resulting in minimal communication distance and no signal loss due to obstructions. In contrast, RF-based communications utilize both LOS and non-line-of-sight (NLOS) paths, encountering significant signal loss in NLOS scenarios and increased communication distances. Despite both optical and RF signals propagating at the speed of light, optical communication systems demonstrate faster communication due to rapid propagation. Furthermore, optical systems exhibit short processing times, enabling the provision of communication services with a fraction



of millisecond end-to-end delays. Consequently, OWC technologies emerge as a promising solution for 5G communication systems, delivering services with negligible latency.

*Ultra-low-energy consumption:* Energy efficiency stands out as a paramount requirement in the design of 5G, 6G, and IoT systems. OWC systems, predominantly structured around LEDs, align with this imperative. Currently deployed LEDs exhibit minimal power consumption, and ongoing global research endeavors are focused on further reducing their energy usage. Notably, LEDs serve a dual purpose by functioning as both illumination sources and communication transmitters, eliminating additional energy consumption when utilized for illumination. In comparison to RF sensors, LED sensors demonstrate significantly lower energy consumption. Consequently, OWC technologies present a compelling solution, offering communication systems with markedly low power consumption. This aligns seamlessly with the critical demand for energy-efficient communication systems in the deployment of 5G and IoT technologies.

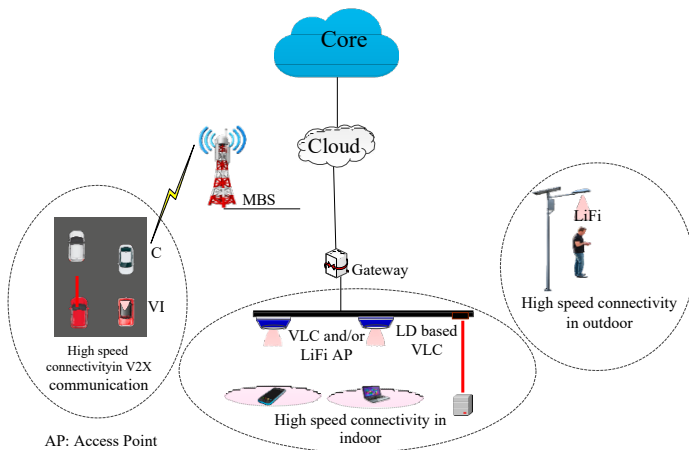


Figure 3: Achieving high-speed connectivity through various OWC technologies.

*Reliable connectivity:* Ensuring dependable connectivity stands as a pivotal criterion for any communication system. OWC systems offer a notably elevated SNR, particularly beneficial for indoor users. In outdoor scenarios, OCC ensures interference-free communication and a robust SNR, maintaining stable performance even with increased communication distances. FSO also exhibits commendable SNR levels for long-distance outdoor communication. Furthermore, OWC networks present an additional tier for indoor users, contributing to heightened communication system reliability. Consequently, OWC systems play a crucial role in enhancing connectivity reliability for users within the realms of 5G/6G and IoT networks.

*Ultra-high security:* OWC technologies, essential for the robust communication demanded by 5G, 6G, and IoT networks, ensure a high level of security. Due to the inability of OWC signals to penetrate obstacles, external

entities are prevented from unauthorized access to sensitive information. The impervious nature of OWC technology prevents external network hacking devices from intercepting internal optical signals. This unparalleled security feature makes OWC systems particularly well-suited for the exchange of information in highly sensitive domains, such as healthcare. Consequently, OWC systems provide an elevated level of security for 5G/6G and IoT networks.

#### 4.3. Fulfilling the Network and Infrastructure Characteristics

*Network densification using highly dense heterogeneous networks:* Network capacity enhancement can be achieved through three primary methods: network densification, spectrum efficiency optimization, and utilization of additional frequency spectra. Network densification involves the strategic addition of more cell sites to augment capacity, encompassing the deployment of small cells and the optimization of frequency utilization. This approach strategically places cell sites in capacity-constrained areas to augment overall capacity and alleviate traffic congestion on surrounding sites. Network densification is particularly relevant in densely populated areas with significant traffic volumes. The 5G/6G communication systems, characterized by high system capacity and per-user data rates, necessitate the densification of access networks and the deployment of supplementary network infrastructures. Increasing the number of small cells can boost traffic volume, while reducing the access network-to-user distance enhances achievable data rates. Consequently, network densification, specifically through the deployment of small cells, becomes imperative to fulfill the demands of 5G/6G paradigms. In dense deployments, a combination of macrocells, wide-area networks, and various indoor and outdoor optical or RF small cells is employed. Each indoor environment may host multiple optical small cells (e.g., VLC, LiFi, and OCC networks) alongside RF small cells. Outdoor applications, such as vehicular networks and street lighting, also utilize numerous optical small cells for communication. The dense deployment of OWC networks aligns with the network densification criterion, ensuring a high-capacity FSO backhaul connectivity. Figure 4 illustrates that the OWC-based small-cell networks, in conjunction with RF small cells, contribute to a highly dense network deployment.

*Multi-tier architecture and convergence of heterogeneous networks:* To address the evolving requirements of future communication, networks will leverage a multi-tier architecture comprising broader coverage satellite and/or macrocell networks supporting smaller cells housing RF small cells alongside optical VLC, LiFi, and OCC networks. In this architecture, VLC and LiFi technologies form a sub-tier below RF small cells. Illustrated in Figure 4 is an exemplary depiction of this multi-tier architecture

featuring macrocells, RF small cells, and optical small cells. The integration of optical small cells, including VLC and LiFi, presents an opportunity to augment high-capacity capabilities within multi-tier wireless heterogeneous networks. Consequently, the burden on costly satellite or macrocell networks can be alleviated through load offloading to small-cell networks. Indoor OWC systems can efficiently serve a significant number of users, enhancing the overall service quality provided by outdoor macrocell and satellite networks, which are often constrained by capacity limitations. Furthermore, the incorporation of OWC technologies within multi-tier heterogeneous networks addresses the limitations inherent in RF-based wireless communication systems. Optical and RF signals operate independently, mitigating interference effects within the multi-tier network infrastructure. In essence, OWC technologies will assume a pivotal role in the advancement of multi-tier heterogeneous networks, spanning across 5G, 6G, and future generations of communication systems.

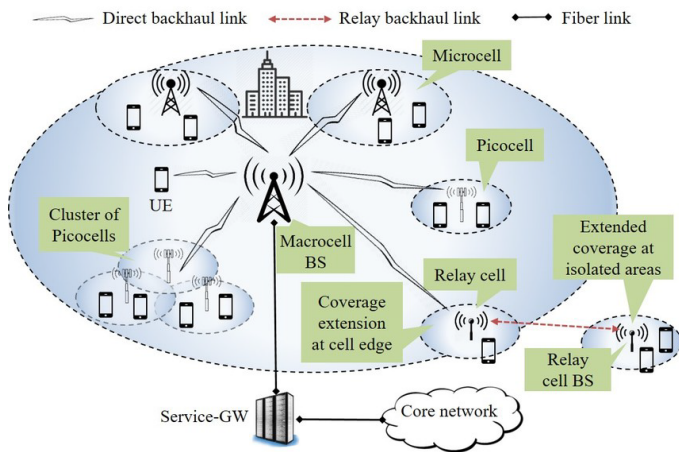


Figure 4: Scenario of heterogeneous multi-tier networks containing an RF microcell, many RF smallcells, and a large number of optical small cells.

*Provision of hybrid network connectivity:* Each of the distinct RF and optical wireless technologies possesses inherent limitations and advantages. The integration of heterogeneous networks, characterized by the coexistence of both RF and OWC technologies, offers an effective solution to overcome these limitations. The concurrent operation of two systems enhances link reliability and facilitates load balancing, thereby optimizing network performance. In outdoor applications, the hybrid system proves particularly advantageous in mitigating atmospheric effects. Figure 5 provides Performance Analysis of Hybrid Radio Frequency and Free Space Optical Communication Networks with Cooperative Spectrum Sharing. Collaboration between RF and optical links is leveraged to establish direct or relay-based connectivity from a source to a destination. The relay system incorporates optical links, connecting either from source-to-relay or relay-to-destination within the hybrid framework. Additionally, the simultaneous utilization of optical and RF links is possible in either or both of these

connection scenarios. The configuration of forward and return communication links may vary based on application scenarios and the specific hybrid architecture. This can involve separate forward and return paths or the sharing of paths, where optical links handle the forward path, and RF links manage the return path. Consequently, OWC technologies assume a pivotal role in the strategic design of hybrid systems, effectively mitigating limitations and providing viable solutions within the context of 5G/6G networks.

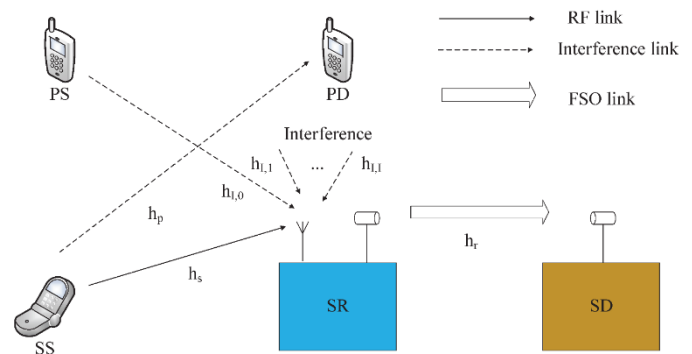


Figure 5: Performance Analysis of Hybrid Radio Frequency and Free Space Optical Communication Networks with Cooperative Spectrum Sharing

*Massive device connectivity:* Robust connectivity on a large scale stands as a pivotal attribute in the landscape of future communication systems. In the 5G era, the IoT is anticipated to interconnect a diverse array of up to 50 billion heterogeneous devices. This connectivity extends beyond mobile phones, encompassing applications in vehicles, household electronics, and medical equipment, contributing to the realization of a smart society [46]. The IoT, facilitated by massive connectivity, enables the integration of various sensors and physical devices, allowing them to communicate and interact autonomously, free from human intervention [47]. Projections for the 6G paradigm indicate an even broader scope, connecting a greater number of intelligent devices. OWC emerges as a pivotal enabler for achieving massive connectivity. The escalating use of LEDs is noteworthy due to their cost-effectiveness, low energy consumption, and extended lifespan. OCC, in particular, garners significant interest within the realm of IoT. Leveraging existing or minimally modified infrastructures, OCC presents economically viable solutions for a diverse range of IoT applications. Thus, OWC technology, employing low-power LEDs, has the potential to establish an extensive network of connections, aligning with the objectives of 5G/6G and IoT networks. Figure 6 illustrates various examples of widespread connectivity across different environments through diverse OWC technologies, supporting applications in homes, healthcare, transportation systems, remote connectivity, and smart grid systems [44]. In the context of smart grids, which integrate operational and energy-measuring devices like smart meters, appliances, renewable energy resources, and energy-efficient

technologies, OWC technologies facilitate extensive connectivity. Through these interconnected elements, smart grids serve as foundational components for effective energy management within a sustainable environment [47].

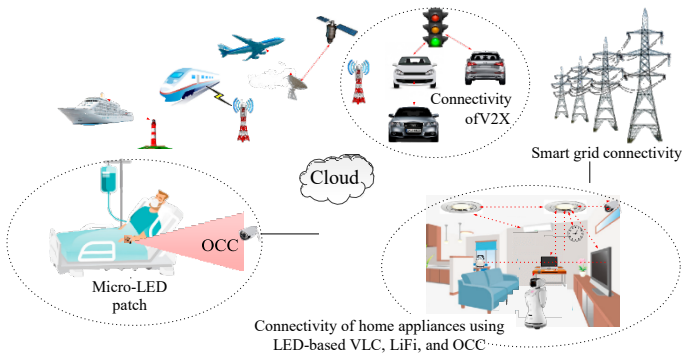


Figure 6: Several instances exemplify extensive connectivity facilitated by OWC technologies.

The IoT networks are characterized by several crucial requirements, including low device cost, low power consumption, economical deployment, heightened energy efficiency, robust security and privacy measures, and the ability to accommodate a large number of devices. LED-based OWC systems encompass all the essential features necessary to support the diverse needs of the IoT. Presently, key technologies employed for IoT connectivity include Zigbee, Bluetooth Low Energy (BLE), and WiFi. Zigbee, recognized for its cost-effectiveness and low-power attributes, serves as a prevalent wireless mesh network standard for IoT applications [48]. However, Zigbee faces limitations in terms of transmission rates and security levels, with interference emerging as a concern in densely populated Zigbee networks. BLE, designed as a low-energy variant of Bluetooth for short-range communication, operates in a single-hop topology (piconet) where one master device communicates with several slave nodes, alongside a broadcast group topology featuring an advertiser node broadcasting to multiple scanners [48]. On the other hand, WiFi lacks guaranteed QoS and is susceptible to interference due to shared unlicensed bands with Zigbee, Bluetooth, and various other devices in the Industrial, Scientific, and Medical (ISM) band. In contrast, OWC technologies exhibit superior capabilities in meeting the specific requirements of IoT networks compared to existing wireless technologies. The inherent advantages of OWC systems position them as a robust solution for addressing the multifaceted demands of IoT applications.

**Small-cell networks:** A highly effective approach for enhancing area spectral efficiency involves reducing the cell size in instances where a limited number of users are served by each cell [49]. In the evolution of communication systems, the third-generation system exclusively featured microcellular networks to support cellular connectivity. The 4G system introduced small-cell and microcell deployments alongside macrocellular networks, while the upcoming 5G system is anticipated to

incorporate ultra-dense small-cells in addition to macro cellular networks [50]. The reduction in cell size presents an opportunity to allocate more spectra to each user. The integration of indoor small-cells or femtocells has significantly expanded possibilities in this regard. An indoor small-cell typically has a cell radius of around 10 meters, catering to five to six users [51]. This deployment strategy proves cost-effective and energy-efficient, meeting coverage and capacity requirements [52]. With the anticipated peak user data rates reaching 10 Gbps for 5G and 1 Tbps for 6G communication systems, the management of heavy data traffic, particularly generated indoors, becomes crucial. Consequently, the deployment of highly dense small-cell networks emerges as a key characteristic of 5G communication systems. Indoor VLC and LiFi technologies contribute to the creation of highly dense small cells. Each network formed under a single light source is considered a small cell, and in large indoor spaces, hundreds of VLC/LiFi-based small cells can be established. Therefore, OWC networks align with the criteria essential for the development and success of 5G/6G networks.

**Seamless movement:** Seamless mobility is a pivotal requirement for the incorporation of any technology into the 5G networks. The LiFi system stands out by providing comprehensive support for mobility, addressing the demands of both 5G and anticipated 6G communication systems. High-capacity backhaul networks play a crucial role in connecting the access network to the core network. Presently, backhaul networks predominantly utilize dedicated fiber, copper, microwave, mm Wave, and occasionally satellite links [8,53]. Satellite links for backhaul connectivity are contingent on alternative options. In the context of 5G systems, a high-capacity backhaul network is indispensable for facilitating the exchange of substantial data traffic between the access and core networks. Without a robust high-capacity backhaul network, even if the access networks support Gbps communication links to user equipment, the communication system remains incomplete, with a low-capacity backhaul network posing a potential bottleneck. To address this challenge, optical wireless networks, such as FSO systems, alongside wired optical fiber networks, present effective solutions. FSO systems exhibit remarkable features for establishing high-capacity, long-range outdoor backhaul links. Figure 7 illustrates Establishment of high-capacity backhaul connectivity for a ship connectivity, space communications, cellular BS & remote connectivity. FSO technology can also establish high-quality connectivity with Macrocellular Base Stations (MBSs), offering an alternative to existing backhaul network technologies. A comparative analysis in Table 3 highlights the achieved data rates and latencies of key backhaul technologies. While optical fiber currently boasts the highest throughput, FSO systems

demonstrate comparable throughput. Given their similar transmitter and receiver architecture, FSO systems have the potential to achieve throughput levels similar to optical fiber systems in the near future. Latency, calculated for transmission during backhaul connectivity, underscores the FSO network's potential as a valuable complementary solution to wired, microwave, and mmWave systems, supporting high-data-rate communications in 5G and 6G networks.

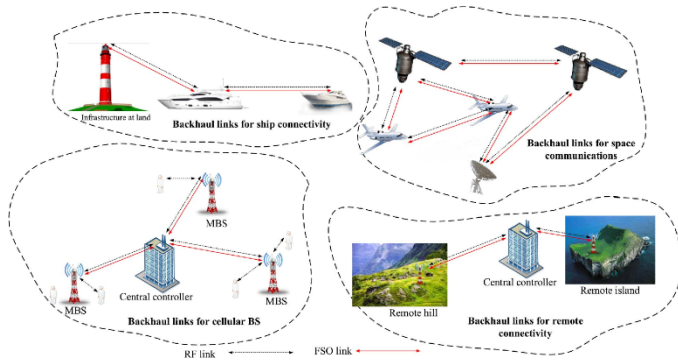


Figure 7: Establishing high-capacity backhaul connectivity for a ship connectivity, space communications, cellular BS & remote connectivity.

Table 4: Comparison of the achieved data rates and latencies in the existing important backhaul technologies [2,9,54]

Backhaul Technology	Achieved Data Rates	Latency
Optical Fiber	Highest throughput	Low
Copper	Moderate	Moderate
Microwave	Moderate	Moderate
mm Wave	Moderate	Moderate
Satellite	Varies	High

**Green Communication:** The realization of green communication in future 5G/6G and IoT networks relies on various factors, including energy-conscious network deployment, the selection of communication devices, and the design of communication network protocols. Achieving environmental sustainability necessitates energy-efficient communication methods, a goal that can be effectively met through the increased utilization of LED-based OWC technologies. OWC technologies are poised to handle a substantial portion of the overall wireless data volume, leading to significant energy savings when employed for indoor communication. By leveraging LEDs, which serve dual purposes as both communication devices and illumination sources, OWC networks have the potential to contribute significantly to energy efficiency. Furthermore, OWC systems can play a role in energy harvesting (EH), as demonstrated by integrating solar cells into VLC links. This integration allows solar cells to function not only as energy harvesters but also as optical receivers [55]. Consequently, OWC systems play a pivotal role in establishing environmentally conscious communication systems, a

key characteristic integral to the development of 5G/6G and IoT networks.

**Tactile internet support:** The International Telecommunication Union characterizes the Tactile Internet as the forthcoming internet infrastructure merging ultra-low latency with exceptionally high levels of availability, reliability, and security. Representing the next phase of evolution for the IoT, the Tactile Internet will extend its scope to include interactions between humans and machines, as well as machine-to-machine interactions [56–59]. OWC technologies possess the capability to underpin the Tactile Internet. In a prior study [60], we introduced Human Bond Communication (HBC) as a concept facilitating continuous bidirectional communication among multiple users.

**Intelligent transportation:** Vehicular communication stands as a pivotal component of the modern era, promising pervasive connectivity with ultra-reliable and low-latency features [61]. V2X communications play a vital role in enhancing road safety, optimizing traffic efficiency, and ensuring the availability of infotainment services [62]. The Dedicated Short-Range Communication (DSRC) technology, operating in the 5.9 GHz band, is extensively utilized for supporting V2X communications, particularly in applications focused on vehicular safety [63]. In addition to DSRC, millimeter-wave (mm Wave) bands have gained prominence in V2X communications due to their ability to deliver Gigabits per second data rates, surpassing the capabilities of DSRC [63]. Furthermore, OWC technologies emerge as a promising option for ensuring reliable connectivity in LOS conditions. Specifically, VLC and LiFi can facilitate short-distance inter-vehicle communications, while OCC extends support for communication over a distance of 60 meters [64]. FSO communication, utilizing laser-based technology, offers the potential for even longer-distance communication in vehicular scenarios.

#### 4.4. Surveys of OWC-Based 5G/6G and IoT Systems

Numerous researchers globally are actively engaged in exploring OWC for the development of future communication networks. An innovative approach introduced in [60] focuses on HBC utilizing head-mounted displays (HMDs). This method employs the camera of an HMD as a receiver and incorporates an IR light source as a transmitter, demonstrating the feasibility of HMDs for communication purposes. This HBC system enables efficient communication between users or devices using their respective HMDs. In [65], researchers propose an optical V2V communication system based on LED transmitters and camera receivers. This technology has the potential to emerge as a significant development for the Internet of Vehicles, where the LED transmitter in one vehicle communicates various data to camera receivers in

other vehicles using an optical communication image sensor. The LiFi/WiFi-integrated architecture presented in [66] is designed to meet the requirements of the 5G system, showcasing a comprehensive integration of LiFi and WiFi. A universal traffic management system detailed in [67] provides expressway and road information to vehicles. This system utilizes LED headlights as transmitters for the uplink and multiple PDs with lenses as receivers on the roadside. For the downlink, signals are transmitted from an LED on a roadside unit and received using an optical communication image sensor on the vehicle. Motivating factors for VLC usage in supporting highly dense users are discussed in [68]. The study explores VLC integration with RF technologies, emphasizing the importance of selecting suitable operating conditions for optimal outcomes in both RF and VLC solutions. Additionally, [69] introduces a relay-assisted VLC system where an amplify-and-forward relay is employed to forward signals while simultaneously transmitting its own signals. The relay terminal assists the source terminal in forwarding signals to the destination terminal, with signal allocation to even and odd subcarriers for source and relay terminals, respectively.

The integration of 5G New Radio (NR) with VLC downlink architecture is elucidated by the authors in [70], showcasing the synergistic potential of these emerging wireless technologies. Specifically, the transmission of 5G NR frames over VLC is meticulously implemented, marking a significant stride in bridging these complementary technologies. Furthermore, in the context of a three-dimensional hybrid RF/VLC indoor IoT system described in [71], a homogeneous Poisson point process is employed to model terminal distribution. This study incorporates a light energy harvesting (EH) model alongside a LOS propagation model for VLC, enabling efficient energy utilization. Notably, the harvested energy from PDs at each device within the room is leveraged for transmissions over the RF uplink. The paper underscores pivotal advancements in OWC technologies, addressing future demands posed by 5G, 6G, and IoT systems, an aspect largely unexplored in existing review literature. By comprehensively examining various OWC technologies, the article delineates their potential contributions towards realizing the objectives of next-generation wireless systems.

## 5. Challenges of the OWC in the 5G/6G and IoT Solutions

Successfully deploying OWC technologies for 5G/6G and IoT solutions necessitates adeptly tackling a range of formidable challenges. Several critical challenges are succinctly examined below:

*Frequent handover:* Prospective communication systems will be characterized by heterogeneous small dense

networks, leading to frequent handovers. These handovers will occur both within optical networks and between optical and RF networks. Given the diminutive size of optical cells, the likelihood of numerous superfluous handovers exists, necessitating the mitigation of unnecessary handovers and the associated ping-pong effect. Additionally, the distinctive properties of the physical and data-link layers in optical and RF-based wireless networks pose a significant challenge for ensuring effective mobility support in RF/optical hybrid systems.

*Inter-cell interference:* Effectively addressing the management of inter-cell optical interference emerges as a critical concern during the deployment of optical VLC and LiFi networks. The dense deployment of LEDs in OWC technologies has the potential to induce substantial interference within 5G/6G and IoT networks. Consequently, the mitigation of inter-cell optical interference stands out as a formidable challenge in this context.

*Atmospheric loss:* The efficacy of OWC technologies is susceptible to various atmospheric factors such as scattering, refraction, air absorption, free space loss, and scintillation. Outdoor settings introduce additional challenges, as fog and dust impede the transmission of optical signals from the transmitter to the receiver. Unfavorable atmospheric conditions contribute to degradation in the communication link quality for FSO. Consequently, mitigating atmospheric losses poses a considerable challenge, particularly in outdoor environments, in striving to achieve the objectives of 5G networks.

*Limited uplink communication using OWC technologies:* Many user equipment designs incorporate low-power LEDs to minimize power consumption. However, this presents challenges for VLC and LiFi systems in uplink communication. The use of low-power LEDs results in diffused, low-intensity light, making them susceptible to interference from downlink high-power lights and thereby constraining uplink communication performance. Additionally, the vulnerability of the uplink communication link is heightened by the slightest deflection or movement of the user equipment's receiver. Addressing these issues is crucial for the future enhancement of VLC and LiFi systems to efficiently support uplink communication.

*Low data rate of the OCC system:* A significant limitation of the current OCC system is its constrained data rate, primarily attributed to the low-frame rate cameras employed. Achieving a high data rate is challenging within this framework, as evidenced by the most recent recorded data rate of only 55 Mbps [27]. There is a pressing need to augment this data rate to meet the

burgeoning service requirements in the context of 5G/6G and IoT networks.

*Flickering avoidance:* Flickering refers to variations in the luminance of light perceivable by humans, posing a significant concern in OWC systems. Various modulation schemes employed in OWC systems may induce flickering, which can adversely impact human health. Effectively addressing this challenge involves modulating LEDs in a manner that mitigates flickering, adding a layer of complexity to the task.

*Data rate improvement of the FSO backhaul system:* The backhaul infrastructure within 5G/6G systems is tasked with managing a substantial volume of data traffic to facilitate high-data-rate services for end-users. Failure to address this efficiently may lead to bottleneck issues. Consequently, the challenging endeavor involves enhancing FSO backhaul capacity in response to the escalating traffic volumes.

*Machine learning for OWC:* The future landscape of 6G communication networks necessitates the incorporation of learning-based networking systems as a key requirement. Given the escalating complexity of network structures and diverse requirements, artificial control and decision-making become imperative in challenging environments. Supervised learning finds application in various OWC-based scenarios such as smart healthcare [72], smart home lighting [73], and OWC data mining. Unsupervised machine learning methods prove efficient for OWC data-based analysis, encompassing tasks such as correlation, ranking, spatial and temporal analysis, and flow prediction. Furthermore, reinforcement learning emerges as a valuable tool for optimizing data rates, implementing network switching, and managing traffic within ultra-dense OWC networks designed for 6G [14]. The integration of machine learning into 6G OWC networks facilitates intelligent network assignment, automated error correction, efficient decision-making, and network reassignment, among other functionalities. Notably, the application of the machine learning approach is integral in the context of indoor mobile robot-based dense OWC small networks, enabling swift and efficient task execution.

## 6. Conclusion

The introduction of 5G communication is anticipated to occur by 2020, followed by the projected launch of 6G communication between 2027 and 2030. Realizing the objectives of 5G/6G and the IoT through the tactile internet poses several challenges. Key among these challenges are the provision of high capacity, massive connectivity, low latency, high security, low-energy consumption, high QoE, and highly reliable connectivity for 5G communication systems. Solely relying on RF-

based systems proves insufficient to meet the substantial demands of future 5G/6G and IoT networks. OWC technologies, including VLC, LiFi, OCC, and FSO communication, emerge as ideal complementary solutions to RF networks. The concurrent operation of RF and optical wireless systems holds the potential to achieve the ambitious goals set for these networks. This study provides a comprehensive examination of how OWC technologies contribute to the successful deployment of future 5G/6G and IoT networks. The characteristics of 5G, 6G, and IoT systems, as well as the features of OWC technologies such as VLC, LiFi, OCC, and FSO, are succinctly outlined. Each specification of 5G, 6G, and IoT is individually expounded upon, highlighting how OWC systems facilitate the realization of these features. Additionally, the paper offers a summary of existing OWC-related studies pertaining to 5G and IoT, making it a valuable resource for comprehending research contributions across various optical wireless systems in the context of future network deployment.

## Conflict of Interest

The authors declare no conflict of interest.

## References

- [1] Z. Ghassemlooy, S. Arnon, M. Uysal, Z. Xu, J. Cheng, "Emerging optical wireless communications—advances and challenges," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, 1738–1749, 2015, doi:10.1109/JSAC.2015.2430821.
- [2] M.Z. Chowdhury, M.T. Hossan, A. Islam, Y.M. Jang, "A comparative survey of optical wireless technologies: Architectures and applications," *IEEE Access*, vol. 6, 9819–10220, 2018, doi:10.1109/ACCESS.2018.2799852.
- [3] M. Uysal, H. Nouri, "Optical wireless communications—An emerging technology," in *Proceedings of the International Conference on Transparent Optical Networks*, 2014, doi:10.1109/ICTON.2014.6876505.
- [4] Z. Xu, R.B.M. Sadler, "Ultraviolet communications: Potential and state-of-the-art," *IEEE Communications Magazine*, vol. 46, no. 7, 67–73, 2008, doi:10.1109/MCOM.2008.4569743.
- [5] J.B. Carruthers, *Wireless Infrared Communications*, Wiley Encyclopedia of Telecommunications, 2003.
- [6] P.H. Pathak, X. Feng, P. Hu, P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, 2047–2077, 2015, doi:10.1109/COMST.2015.2444095.
- [7] M. Shafi, A.F. Molisch, P.J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, 1201–1221, 2017, doi:10.1109/JSAC.2017.2695280.
- [8] M. Jaber, M.A. Imran, R. Tafazolli, A. Tukmanov, "5G backhaul challenges and emerging research directions: A survey," *IEEE*

- Access, vol. 4, 1143–1166, 2016, doi:10.1109/ACCESS.2016.2546541.
- [9] J.G. Andrews, S. Buzzi, W. Choi, S. V Hanly, A. Lozano, A.C. Soong, J.C. Zhang, “What will 5G be?” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, 1065–1082, 2014, doi:10.1109/JSAC.2014.2328098.
- [10] W.A. Hassan, H.-S. Jo, T.A. Rahman, “The feasibility of coexistence between 5G and existing services in the IMT-2020 candidate bands in Malaysia,” *IEEE Access*, vol. 5, 14867–14888, 2017, doi:10.1109/ACCESS.2017.2710159.
- [11] A. Ijaz, L. Zhang, M. Grau, A. Mohamed, S. Vural, A.U. Quddus, M.A. Imran, C.H. Foh, R. Tafazolli, “Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations,” *IEEE Access*, vol. 4, 3322–3339, 2016, doi:10.1109/ACCESS.2016.2546541.
- [12] K. David, H. Berndt, “6G vision and requirements: Is there any need for beyond 5G?” *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, 72–80, 2018, doi:10.1109/MVT.2018.2816618.
- [13] F. Tariq, M. Khandaker, K.K. Wong, M. Imran, M. Bennis, M. Debbah, “A speculative study on 6G,” *ArXiv Preprint*, 2019.
- [14] S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman, “Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future,” *IEEE Access*, vol. 7, 46317–46350, 2019, doi:10.1109/ACCESS.2019.2900597.
- [15] R.A. Stoica, G.T.F. Abreu, “6G: The wireless communications network for collaborative and AI applications,” *ArXiv Preprint ArXiv:1904.03413*, 2019.
- [16] W. Saad, M. Bennis, M. Chen, “A vision of 6G wireless systems: Applications, trends, technologies, and open research problems,” *ArXiv Preprint ArXiv:1902.10265*, 2019.
- [17] T. Nguyen, M.Z. Chowdhury, Y.M. Jang, “A novel link switching scheme using pre-scanning and RSS prediction in visible light communication networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, 1–17, 2013, doi:10.1186/1687-1499-2013-1.
- [18] D. Tsonev, S. Videv, H. Haas, “Towards a 100 Gb/s visible light wireless access network,” *Optics Express*, vol. 23, no. 2, 1627–1637, 2015, doi:10.1364/OE.23.001627.
- [19] M.Z. Chowdhury, M.T. Hossan, M.K. Hasan, Y.M. Jang, “Integrated RF/optical wireless networks for improving QoS in indoor and transportation applications,” *Wireless Personal Communications*, vol. 107, no. 3, 1401–1430, 2018, doi:10.1007/s11277-018-5482-8.
- [20] H. Haas, L. Yin, Y. Wang, C. Chen, “What is LiFi?” *Journal of Lightwave Technology*, vol. 34, no. 6, 1533–1544, 2016, doi:10.1109/JLT.2016.2525829.
- [21] S. Dimitrov, H. Haas, *Principles of LED Light Communications: Towards Networked Li-Fi*, Cambridge University Press, 2015.
- [22] H.H. Lu, C.Y. Li, H.W. Chen, C.M. Ho, M.T. Cheng, Z.Y. Yang, C.K. Lu, “A 56 Gb/s PAM4 VCSEL-based LiFi transmission with two-stage injection-locked technique,” *IEEE Photonics Journal*, vol. 9, 1–8, 2017, doi:10.1109/JPHOT.2017.2696500.
- [23] M.K. Hasan, M.Z. Chowdhury, M. Shahjalal, Y.M. Jang, “Fuzzy based network assignment and link-switching analysis in hybrid OCC/LiFi system,” *Wireless Communications and Mobile Computing*, 2018, doi:10.1155/2018/5703580.
- [24] M. Hossan, M.Z. Chowdhury, M. Hasan, M. Shahjalal, T. Nguyen, N.T. Le, Y.M. Jang, “A new vehicle localization scheme based on combined optical camera communication and photogrammetry,” *Mobile Information Systems*, 2018, doi:10.1155/2018/4609192.
- [25] M. Shahjalal, M. Hossan, M. Hasan, M.Z. Chowdhury, N.T. Le, Y.M. Jang, “An implementation approach and performance analysis of image sensor based multilateral indoor localization and navigation system,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018, doi:10.1155/2018/5703580.
- [26] Z. Ghassemlooy, P. Luo, S. Zvanovec, *Optical camera communications*, Springer: 547–568, 2016, doi:10.1007/978-3-319-48872-5\_20.
- [27] Y. Goto, I. Takai, T. Yamazato, H. Okada, T. Fujii, S. Kawahito, S. Arai, T. Yendo, K. Kamakura, “A new automotive VLC system using optical communication image sensor,” *IEEE Photonics Journal*, vol. 8, 1–17, 2016, doi:10.1109/JPHOT.2016.2593718.
- [28] A. Malik, P. Singh, “Free space optics: Current applications and future challenges,” *International Journal of Optics*, vol. 2015, 2015, doi:10.1155/2015/146591.
- [29] M.A. Khalighi, M. Uysal, “Survey on free space optical communication: A communication theory perspective,” *IEEE Communications Surveys & Tutorials*, vol. 16, 2231–2258, 2014, doi:10.1109/SURV.2014.012214.00189.
- [30] H. Kaushal, G. Kaddoum, “Optical communication in space: Challenges and mitigation techniques,” *IEEE Communications Surveys & Tutorials*, vol. 19, 57–97, 2017, doi:10.1109/COMST.2016.2618498.
- [31] S. Mumtaz, J.M. Jornet, J. Aulin, W.H. Gerstacker, X. Dong, B. Ai, “Terahertz communication for vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 66, 5617–5625, 2017, doi:10.1109/TVT.2016.2639738.
- [32] L. Lovén, T. Leppänen, E. Peltonen, J. Partala, E. Harjula, P. Poromaa, M. Ylianttila, J. Riekkii, “Edge AI: A vision for distributed, edge-native artificial intelligence in future 6G networks,” in *Proceedings of the 6G Wireless Summit*, Levi, Finland, 2019.
- [33] F. Clazzer, A. Munari, G. Liva, F. Lazaro, C. Stefanovic, P. Popovski, “From 5G to 6G: Has the time for modern random access come?” *ArXiv Preprint ArXiv:1903.03063*, 2019.
- [34] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, M. Zorzi, “Towards 6G networks: Use cases and technologies,” *ArXiv Preprint ArXiv:1903.12216*, 2019.
- [35] 5G Requirements.
- [36] *Light Communications for Wireless Local Area Networking*.
- [37] D. Menaka, C.T. Sabitha Gauni, Manimegalai, K. Kalimuthu, “Vision of IoUT: advances and future trends in optical wireless communication,” *Journal of Optics*, vol. 50, 439–452, 2021.
- [38] P. Hu, P.H. Pathak, A.K. Das, Z. Yang, P. Mohapatra, “PLiFi: Hybrid WiFi-VLC networking using power lines,” in *Proceedings of the Workshop on Visible Light Communication Systems*, New York, NY, USA, 2016.
- [39] Z. Du, C. Wang, Y. Sun, G. Wu, “Context-aware indoor VLC/RF heterogeneous network selection: Reinforcement learning with knowledge transfer,” *IEEE Access*, vol. 6, 33275–33284, 2018, doi:10.1109/ACCESS.2018.2847723.
- [40] T. Koonen, “Indoor optical wireless systems: Technology, trends, and applications,” *Journal of Lightwave Technology*, vol. 36, no. 7, 1459–1467, 2018, doi:10.1109/JLT.2018.2791740.

- [41] C. Danakis, M. Afgani, G. Povey, I. Underwood, H. Haas, "Using a CMOS camera sensor for visible light communication," in Proceedings of the IEEE Globecom Workshops, Anaheim, CA, USA, 2012.
- [42] H.M. Tsai, H.M. Lin, H.Y. Lee, "Demo: Rollinglight-universal camera communications for single LED," in Proceedings of the International Conference on Mobile Computing and Networking, Maui, HI, USA, 2014.
- [43] L.Y. Wei, C.W. Chow, G.H. Chen, Y. Liu, C.H. Yeh, C.W. Hsu, "Tricolor visible-light laser diodes based visible light communication operated at 40.665 Gbit/s and 2 m free-space transmission," *Optics Express*, vol. 27, no. 18, 25072–25077, 2019, doi:10.1364/OE.27.025072.
- [44] M.Z. Chowdhury, M. Shahjalal, M.K. Hasan, Y.M. Jang, "The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges," *Applied Sciences*, vol. 9, 2019.
- [45] C. Chang, "A 100-Gb/s multiple-input multiple-output visible laser light communication system," *Journal of Lightwave Technology*, vol. 32, no. 22, 4723–4729, 2014, doi:10.1109/JLT.2014.2361215.
- [46] D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez, T. Sato, "One integrated energy efficiency proposal for 5G IoT communications," *IEEE Internet of Things Journal*, vol. 3, 1346–1354, 2016, doi:10.1109/JIOT.2016.2593778.
- [47] Z. Yan, O. Zhang, A. V Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, 120–134, 2014, doi:10.1016/j.jnca.2014.01.012.
- [48] M.R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, 510–527, 2016, doi:10.1109/JSAC.2016.2525478.
- [49] X. Ge, J. Yang, H. Gharavi, Y. Sun, "Energy efficiency challenges of 5G small cell networks," *IEEE Communications Magazine*, vol. 55, no. 1, 184–191, 2017, doi:10.1109/MCOM.2017.1600493.
- [50] Y. Hao, M. Chen, L. Hu, J. Song, M. Volk, I. Humar, "Wireless fractal ultra-dense cellular networks," *Sensors*, vol. 17, no. 4, 841, 2017, doi:10.3390/s17040841.
- [51] M.Z. Chowdhury, Y.M. Jang, Z.J. Haas, "Cost-effective frequency planning for capacity enhancement of femtocellular networks," *Wireless Personal Communications*, vol. 60, no. 1, 83–104, 2011, doi:10.1007/s11277-010-9987-2.
- [52] H.A.U. Mustafa, M.A. Imran, M.Z. Shakir, A. Imran, R. Tafazolli, "Separation framework: An enabler for cooperative and D2D communication for future 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 18, 419–445, 2016, doi:10.1109/ACCESS.2018.2847723.
- [53] X. Artiga, A. Perez-Neira, J. Baranda, E. Lagunas, S. Chatzinotas, R. Zetik, P. Gorski, K. Ntougias, D. Perez, G. Ziaragkas, "Shared access satellite-terrestrial reconfigurable backhaul network enabled by smart antennas at mmWave band," *IEEE Network*, vol. 32, no. 5, 46–53, 2018, doi:10.1109/MNET.2018.1700241.
- [54] F. Knobloch, "Delay analysis for optical wireless multihop networks," in Proceedings of the International Conference on Transparent Optical Networks (ICTON), Trento, Italy, 2016.
- [55] S. Zhang, D. Tsonev, S. Videv, S. Ghosh, G.A. Turnbull, I.D.W. Samuel, H. Haas, "Organic solar cells as high-speed data detectors for visible light communication," *Optica*, vol. 2, no. 7, 607–610, 2015, doi:10.1364/OPTICA.2.000607.
- [56] What is The Tactile Internet? Available online: <https://5g.co.uk/guides/what-is-the-tactile-internet> (accessed on 15 August 2019).
- [57] G. Fettweis, "The tactile internet: Applications and challenges," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, 64–70, 2014, doi:10.1109/MVT.2013.2293016.
- [58] A. Aijaz, M. Dohler, A.H. Aghvami, V. Friderikos, M. Frodigh, "Realizing the tactile internet: Haptic communications over next generation 5G cellular networks," *IEEE Wireless Communications*, vol. 24, no. 1, 82–89, 2017, doi:10.1109/MWC.2017.1600493.
- [59] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, G. Fettweis, "5G-enabled tactile internet," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, 460–473, 2016, doi:10.1109/JSAC.2016.2525478.
- [60] M.T. Hossan, M.Z. Chowdhury, M. Shahjalal, Y.M. Jang, "Human bond communication with head-mounted displays: Scope, challenges, solutions, and applications," *IEEE Communications Magazine*, vol. 57, no. 2, 26–32, 2019, doi:10.1109/MCOM.2019.1800421.
- [61] S.A.A. Shah, E. Ahmed, M. Imran, S. Zeadally, "5G for vehicular communications," *IEEE Communications Magazine*, vol. 56, no. 11, 111–117, 2018, doi:10.1109/MCOM.2018.1700241.
- [62] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, L. Zhao, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Communications Standards Magazine*, vol. 1, no. 1, 70–76, 2017, doi:10.1109/MCOMSTD.2017.1700015.
- [63] T.S. Rappaport, Y. Xing, G.R. MacCartney, A.F. Molisch, E. Mellios, J. Zhang, "Overview of millimeter wave communications for fifth generation (5G) wireless networks— with a focus on propagation models," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, 6213–6230, 2017, doi:10.1109/TAP.2017.2734243.
- [64] P. Luo, M. Zhang, Z. Ghassemlooy, H. Le Minh, H.M. Tsai, X. Tang, L.C. Png, D. Han, "Experimental demonstration of RGB LED-based optical camera communications," *IEEE Photonics Journal*, vol. 7, –12, 2015, doi:10.1109/JPHOT.2015.2457321.
- [65] I. Takai, T. Harada, M. Andoh, K. Yasutomi, K. Kagawa, S. Kawahito, "Optical vehicle-to-vehicle communication system using LED transmitter and camera receiver," *IEEE Photonics Journal*, vol. 6, 1–14, 2014, doi:10.1109/JPHOT.2014.2361215.
- [66] M. Ayyash, H. Elgala, A. Khreishah, V. Jungnickel, T. Little, S. Shao, M. Rahaim, D. Schulz, J. Hilt, R. Freund, "Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges," *IEEE Communications Magazine*, vol. 54, no. 2, 64–71, 2016, doi:10.1109/MCOM.2016.7432165.
- [67] T. Yamazato, N. Kawagita, H. Okada, T. Fujii, T. Yendo, S. Arai, K. Kamakura, "The uplink visible light communication beacon system for universal traffic management," *IEEE Access*, vol. 5, 22282–22290, 2017, doi:10.1109/ACCESS.2017.2766759.
- [68] M.B. Rahaim, T.D.C. Little, "Toward practical integration of dual-use VLC within 5G networks," *IEEE Wireless Communications*, vol. 22, 97–103, 2015, doi:10.1109/MWC.2015.7124872.
- [69] Z. Na, Y. Wang, M. Xiong, X. Liu, J. Xia, "Modeling and throughput analysis of an ADO-OFDM based relay-assisted



- VLC system for 5G networks," IEEE Access, vol. 6, 17586–17594, 2018, doi:10.1109/ACCESS.2018.2808258.
- [70] L. Shi, W. Li, X. Zhang, Y. Zhang, G. Chen, A. Vladimirescu, "Experimental 5G new radio integration with VLC," in Proceedings of the IEEE International Conference on Electronics, Circuits and Systems (ICECS), 1–4, 2018, doi:10.1109/ICECS.2018.8611640.
- [71] G. Pan, H. Lei, Z. Ding, Q. Ni, "3-D Hybrid VLC-RF indoor IoT systems with light energy harvesting," IEEE Transactions on Green Communications and Networking, vol. 3, 853–865, 2019, doi:10.1109/TGCN.2019.2908839.
- [72] M.K. Hasan, M. Shahjalal, M.Z. Chowdhury, Y.M. Jang, "Real-time healthcare data transmission for remote patient monitoring in patch-based hybrid OCC/BLE networks," Sensors, vol. 19, 1208, 2019, doi:10.3390/s19051208.
- [73] K.P. Pujapanda, "LiFi Integrated to power-lines for smart illumination cum communication," in Proceedings of the International Conference on Communication Systems and Network Technologies, 1–4, 2013.

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).



**RAMSHA KHALID** has done her bachelor's degree from Lahore College for Women University, Lahore in 2018. She has done her master's degree from University of Lahore, Lahore in 2022. Her area of interest includes Computer & Communication Networks,

Machine Learning, Artificial Intelligence, Cyber Security, Control Systems and Renewable Energy Systems. Recently she has published a conference paper in IEEE INMIC'23 held in University of Central Punjab, Lahore as a first author.



**M. NAQI RAZA** has done his bachelor's degree from University of Gujrat, Gujrat in 2018. Currently, he is doing his master's degree from University of Sialkot, Sialkot.

His area of interest includes Power Generation (Conventional and Renewable), Wind Power Generation and Utilization, Optimization of Wind Energy, Solar Energy, Solar Power Applications, Electric Vehicles (PHEVs).