Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network

Yuliia Kostiuk[1,†], Pavlo Skladannyi[1,2,*,†], Nataliia Korshun[1,†], Bohdan Bebeshko[1,†] and Karyna Khorolska[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*
[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680 Kyiv, Ukraine*

Abstract

This paper presents an integrated approach to enhancing the security of adaptive video streams transmitted over Bluetooth wireless networks with increased data transfer rates using adaptive modulation and a three-zone buffer. The study addresses key security challenges such as confidentiality, integrity, and availability, proposing a comprehensive strategy that combines adaptive encryption, dynamic modulation, traffic multiplexing, and buffer management. The adaptive encryption mechanism allows for real-time adjustments to encryption levels based on network conditions, ensuring both security and transmission efficiency. A three-zone buffer policy is introduced, prioritizing the transmission of video data packets (I-frames, P-frames, and B-frames) according to buffer occupancy and data importance. The use of traffic multiplexing across multiple transmission paths enhances the availability of video streams, mitigating the effects of network congestion and packet loss. The paper also explores future directions for video stream security, including the potential of quantum encryption for unbreakable security and AI-driven techniques for real-time threat detection and dynamic security adaptation. The relevance of lightweight encryption methods and edge computing solutions in securing video streams within the Internet of Things (IoT) environments is also discussed. Overall, the proposed approach balances security and performance, making it suitable for modern multimedia applications. This research contributes to advancing video stream protection strategies in wireless networks, ensuring continuous, secure, and high-quality video transmission.

Keywords

adaptive video streaming, Bluetooth wireless networks, video stream security, artificial intelligence, IoT security, multimedia applications, real-time video transmission

1. Introduction

Video transmission in wireless networks is a key component for many modern multimedia applications, such as monitoring systems, video telephony, and personalized television. Streaming video, using compression and buffering technologies, enables real-time transmission over local networks and the Internet. This requires high bandwidth, minimal delays, and acceptable data loss [1–15]. However, the Internet does not always guarantee the required quality of service due to the heterogeneity of network structures and video systems. Developing effective standards for video compression, conversion, and transmission methods is a significant challenge in information technology [4–6, 14–33].

Improving Bluetooth video streaming with adaptive modulation and a three-zone buffer addresses both data transmission efficiency and security concerns. Ensuring the confidentiality, integrity, and availability of video data is critical when using open communication channels [5, 6, 17, 18, 26–29, 34–36]. Confidentiality limits access to authorized users, and the growing risks of unauthorized access in the globalized Internet heighten the need for robust security solutions [1–6, 15–18, 37].

2. Analysis of recent studies and publications

In video streaming over Bluetooth networks with increased data rates using adaptive modulation and a three-zone buffer, protecting confidentiality, integrity, and availability

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
y.kostiuk@kubg.edu.ua (Y. Kostiuk);
p.skladannyi@kubg.edu.ua (P. Skladannyi);
n.korshun@kubg.edu.ua (N. Korshun);
b.bebeshko@kubg.edu.ua (B. Bebeshko);
karynakhorolska@gmail.com (K. Khorolska)

0000-0001-5423-0985 (Y. Kostiuk);
0000-0002-7775-6039 (P. Skladannyi);
0000-0003-2908-970X (N. Korshun);
0000-0001-6599-0808 (B. Bebeshko);
0000-0003-3270-4494 (K. Khorolska)
© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3826/paper12.pdf

is critical [38–43]. Video data encryption is a promising method, but due to the limitations of some encryption algorithms, adaptive encryption and visual cryptography are needed to ensure both security and efficiency for large data volumes [7–11, 15, 27, 34–36].

Integrity and availability are equally important. While methods like redundancy and mirroring protect data at the physical level, they do not ensure availability during transmission. Cryptographic methods may secure integrity but are not always available [2, 20–24, 28–31]. Therefore, combining visual cryptography and traffic multiplexing to secure both confidentiality and availability is essential.

As Bluetooth networks evolve, confidentiality and availability protection methods are increasingly vital [31, 32, 44, 45]. Specialized encryption algorithms help secure video streams but may lack sufficient cryptographic strength. Alternatives like data hiding or digital signatures address integrity but not availability. Load balancing and redundancy improve availability at lower network layers but do not address the content level, reducing their effectiveness in Bluetooth networks.

3. The purpose of the study

The purpose of this study is to develop and evaluate an integrated security framework for adaptive video streaming over Bluetooth wireless networks with enhanced data transfer rates. The framework aims to address critical security concerns—confidentiality, integrity, and availability—while maintaining high transmission efficiency. By incorporating adaptive encryption, dynamic modulation, traffic multiplexing, and a novel three-zone buffer management strategy, the research seeks to ensure the secure, reliable, and uninterrupted transmission of multimedia content in resource-constrained environments. The study also explores future trends, such as quantum encryption and AI-driven security adaptations, to further strengthen video stream protection in wireless networks.

4. Methods and Models

To address emerging challenges in protecting digital video, specialized methods must be developed, focusing on ensuring confidentiality and availability without relying solely on encryption algorithms. This can be achieved through analytical transformation of the data sequence and route-hiding techniques during exchange, enhancing resilience against unauthorized access using existing physical security measures.

A key approach involves traffic multiplexing systems that distribute data fragments across multiple physical channels, increasing the difficulty of reconstructing the original data based on specific needs [8, 17]. This method aligns with modern encryption techniques, including quantum cryptography and AI algorithms, applied at various network transmission layers. These systems include intermediate nodes and specialized devices that process and protect data, implementing advanced security measures across the network [1, 2, 5, 7, 8, 28–32, 44, 45]. The traffic multiplexing model uses sophisticated cryptographic protection integrated with advanced data processing techniques. The classical method of sending equal-sized projections to each participant has become outdated. Modern technologies now use compression and advanced encoding to optimize data sizes, reduce traffic, and address bandwidth limitations, enhancing video stream security over Bluetooth networks [5, 7–9, 21–27, 34, 35].

A more advanced approach uses a data segmentation algorithm, dividing image points into non-overlapping classes and distributing video data across multiple channels without adding redundancy, minimizing transmitted data volume [2–6, 18, 26, 27, 34]. However, if projections are intercepted, partial information could be exposed, so segmentation methods must reduce the value of intercepted data.

To ensure availability, a method is needed that allows recipients to restore the image even if some projections are blocked or altered by an attacker. Balancing security and availability is crucial for protecting video transmissions over wireless networks [5, 7–10, 13, 14, 17, 19–25].

A study of video confidentiality methods over Bluetooth networks with increased data transfer rates, using adaptive modulation and a three-zone buffer, proposed a segmentation method based on pixel brightness values. Projections would include pixels from a specific brightness range, with the number of participants determining the class division. For example, in a two-participant scenario, pixels would be divided into corresponding brightness-based classes:

$$P_0 = \{(x,y) | f(x,y) < \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y)\},$$
$$P_0 = \{(x,y) | f(x,y) \geq \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y)\}. \quad (1)$$

For a scenario with an arbitrary number of participants where $n = 2^k (k > 1)$, the definition of classes is recursive:

$$P_i = \{(x,y) | f(x,y) < \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y) \in \underline{P_j}} f(x,y)\},$$
$$P_{i+1} = \{(x,y) | f(x,y) \geq \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y) \in \underline{P_j}} f(x,y)\}. \quad (2)$$

where $\underline{P_j}$ is the class obtained for the scheme with 2 participants, for the scheme with 2^{k-1}, i.e $j \in [0; 2^{k-1} - 1]$, a $i = 2j$.

At the same time, to ensure maximum availability of transmitted video information, a method of uniform image segmentation was proposed. Suppose the digital image P with dimensions $M_1 \times M_2$ corresponds to the following matrix:

$$\begin{bmatrix} f(0,0) & f(1,0) & \cdots & f(M_1-1,0) \\ f(0,1) & f(1,1) & \cdots & f(M_1-1,1) \\ \vdots & \vdots & & \vdots \\ f(0,M_2-1) & f(1,M_2-1) & \cdots & f(M_1-1,M_2-1) \end{bmatrix} \quad (3)$$

It is necessary to divide it into nnn projections so that a minimal number of projections is required for restoring the original image [10–12, 15, 16]. To achieve this, it is evident that each projection should contain points evenly distributed across the entire frame, meaning the projection will represent a grid with equidistant nodes, and $n = 2^k$, $k \geq 1$:

$$\begin{bmatrix} f(0,0) & 0 & \cdots & f(\sqrt{n},0) & 0 & \cdots \\ 0 & 0 & & & & \\ \vdots & & \ddots & & & \\ f(0,\sqrt{n}) & & & f(\sqrt{n},\sqrt{n}) & & \\ 0 & & & & 0 & \\ \vdots & & & & & \ddots \end{bmatrix} \quad (4)$$

In securing video streams over Bluetooth networks with increased data rates using adaptive modulation and a three-zone buffer, restoring the original image from incomplete projections is crucial for maintaining integrity and confidentiality [1, 5, 7–9]. This is achieved by constructing interpolation functions for known points to estimate unknown ones. The more projections received, the more accurate the reconstruction, enhancing data protection [2–6, 10–13, 15–17, 19–22].

Security risks arise if attackers access a single physical channel, enabling them to analyze or modify data. Since each channel carries only part of the frame, an attacker could reconstruct the original frame from an intercepted projection, compromising the stream's confidentiality [1, 3, 7, 8, 17, 18]. Blocking or altering a projection could further affect integrity and availability, raising concerns about system robustness against attacks.

The study examined various methods for restoring frames from projections, focusing on Bluetooth streaming security with adaptive modulation and a three-zone buffer [11–16, 19, 20, 46].

To evaluate the effectiveness of image restoration methods and, consequently, video stream protection methods over a Bluetooth wireless network with increased data transfer rates using adaptive modulation with a three-zone buffer, the following criteria were identified [19–24]. One of these criteria is the minimum square mean error of the restored image. This criterion measures the accuracy of image reproduction after the restoration procedure. It assesses the deviation between the original image and its restored version. The smaller the value of this criterion, the better the image restoration, and therefore, the more effective the video stream protection against possible attacks or distortions.

$$\varepsilon^2 = \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} (h(x,y) - f(x,y))^2 \longrightarrow min, \quad (5)$$

The psychovisual criterion for image reproduction quality is essential when evaluating image restoration methods for securing video streams over Bluetooth networks with adaptive modulation and a three-zone buffer [7–11, 17]. Several methods were analyzed, including bilinear interpolation, bicubic spline interpolation, and linear extrapolation. Bicubic spline interpolation proved most effective in minimizing restoration error for uniformly segmented projections. A clear link was found between increased gap size and higher relative error. While gap extrapolation worked in some cases, it was ineffective for brightness-based segmentation [27, 28, 30–32, 34, 35, 44, 45]. These results align with the psychovisual quality criterion, though expert evaluation is advised for specific cases.

Furthermore, the conclusion was formulated that justifies the advantages of the brightness segmentation method over other methods in the context of ensuring video stream security over a Bluetooth wireless network with increased data transfer rates using adaptive modulation with a three-zone buffer. Since brightness segmentation maximizes the difference between values of $\underline{f_i}$ the value of the expression $(\underline{f} - \underline{f_i})$ in this case will also be maximized. Let the initial image $f(x,y)$ be segmented into n projections $f_1(x,y), \dots, f_n(x,y)$ using the brightness segmentation method. Then the mean square error ε_i, of the restored image $h_i(x,y)$ based on an arbitrary projection $f_i(x,y)$ using interpolation methods has the following lower bound:

$$\varepsilon_i{}^2 \geq (\bar{f} - \bar{f}_i)^2 \quad (6)$$

where $\underline{f_i}$ is the mean value of $f(x,y)$ for projection i, and $\underline{f}$ is the mean value of $f(x,y)$ for the initial image. The proof of this theorem is conducted by applying the method of mathematical induction and transitioning from $h_i(x,y)\ to f_i(x,y)$.

The implementation of methods for ensuring confidentiality and availability in digital video transmission over distributed networks was achieved using advanced video processing technologies [1–6, 8–11, 15, 17]. Microsoft DirectShow was employed to create components that transform the original video stream into projections. Confidentiality protection relies on modern image segmentation, while the availability filter applies uniform segmentation [1–6, 8–11, 15, 17]. These filters process the stream and generate projections with predefined parameters.

These filters were integrated into a filter graph for secure transmission over Bluetooth networks with adaptive modulation and a three-zone buffer. The video source can be any capture device or file, and the Infinite Pin Tee Filter generates the necessary stream copies based on the number of participants [7, 22–24, 26, 27, 34]. Each copy is segmented according to the participant's class number, and streams are transmitted via the ASF Writer filter. The final recipient combines these streams, ensuring data security and integrity [19–25, 27, 28, 35, 36].

The system was tested in a high-speed Bluetooth network with transmission rates up to 1 Gbps, in a large organization's network, meeting modern Bluetooth standards [1–7, 9–19, 46]. Intel Core i9 workstations (4.5 GHz) were used to assess system performance. The main objectives were to determine the optimal number of system participants based on video stream frame size and evaluate the efficiency of protection methods. Processing large volumes of video data in the traffic multiplexing system could limit overall efficiency.

Radio Channel Resource Allocation Algorithms for Adaptive Video Streaming:

The radio channel resource management algorithms for securing video streams over Bluetooth networks with increased data rates, using adaptive modulation and a three-zone buffer, are designed to ensure reliable transmission while meeting security requirements. These algorithms adjust to network changes such as signal fluctuations and congestion, optimizing transmission quality [14, 15, 19–22, 28, 35, 36]. Key features include adaptive modulation and traffic management, with machine learning methods used to predict and optimize transmission, enhancing security and reliability.

In parallel, systems for storing and transmitting video over HTTP have grown in popularity due to increased mobile device usage, social media integration, and the demand for distance learning. Video transmission is a telecommunications priority, utilizing two main HTTP-based technologies: non-adaptive (HTTP Progressive Download) and adaptive (HTTP Adaptive Streaming), defined by the DASH standard. As user mobility and reliance on wireless networks grow, these networks face strain, leading to issues like buffering and playback interruptions [14, 15, 19–22, 28, 35, 36].

The performance of centralized wireless networks is significantly impacted by how frequency-time resources are allocated among users. Scheduling algorithms at the base station handle this resource allocation, but since these algorithms vary by manufacturer, they directly affect overall system performance [9–16, 19, 20, 37, 46]. Research into efficient scheduling algorithms is essential for maintaining high performance and ensuring optimal Quality of Experience (QoE) during video transmission via the HTTP protocol.

Key aspects of HTTP-based video transmission include analyzing technologies and assessing user QoE, which is vital for evaluating playback satisfaction. Models and criteria for evaluating video quality perception are developed based on this analysis. A common QoE evaluation method is the Mean Opinion Score (MOS), which rates user satisfaction on a 1–5 scale, depending on video playback statistics and whether the transmission is adaptive or non-adaptive [5–8, 11, 17, 18].

In the analysis of MOS functions and their approximations, two key factors affecting video quality perception were identified: buffering during playback, which influences both adaptive and non-adaptive technologies, and the average bitrate, which plays a crucial role in adaptive technologies. These factors directly impact user satisfaction and overall video transmission quality.

User satisfaction with viewing and, consequently, the performance of the telecommunications system is inversely proportional to the value of the buffering factor and directly proportional to the average bitrate of the stream. Two QoE criteria characterize the buffering factor for a specific user i:

The normalized ratio of buffering and viewing durations:

$$g_i = \lim_{T\to\infty} \frac{b_i^T}{\omega_i^T + b_i^T} \quad (7)$$

where b_i^T is the total buffering duration of user i during time T; ω_i^T is the total video viewing duration by user i during time T.

The ratio of buffering and viewing durations:

$$q_i = \lim_{T\to\infty} \frac{b_i^T}{\omega_i^T}, \quad (8)$$

In studying wireless systems for video stream security over Bluetooth networks with increased data transfer rates, using adaptive modulation and a three-zone buffer, differences were noted between adaptive and non-adaptive transmission technologies [22–26, 28–31, 36]. While many studies focus on wireless communication performance, there remains a gap in data for certain QoE aspects. This research evaluates video quality using both technologies in a centralized wireless HTTP transmission model, where subscribers connect via radio channels. The model includes local components such as a video server, buffering, and playback processes, accounting for data transfer speeds and clip selection [15, 34–37].

For Bluetooth video streaming with adaptive modulation and a three-zone buffer, the system operates in equal-duration periods (slots), optimizing the allocation of frequency-time resources. A wireless channel model and resource scheduler at the base station play critical roles in resource allocation, directly influencing data transfer speeds and user satisfaction [15, 20–24, 28, 35, 36]. A software-hardware setup, including a video player that sequentially downloads segments from the server, is also key to securing video streams (Fig. 1). Below are the main assumptions used in these models.

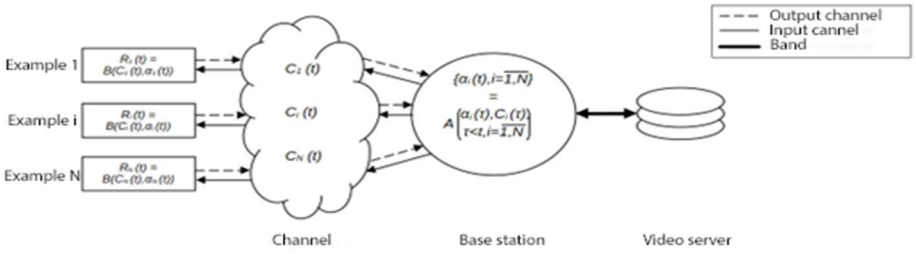

Figure 1: Video Data Transmission Model in a Wireless Network
Source: Developed by the author in the LibreOffice environment

Each video data segment j is presented in a continuous range of bit rates:

$$R_{i,j} \in [R_{min}, R_{max}], i = \overline{1,N}, \quad (9)$$

The user behavior model is characterized by the user video stream sparsity coefficient i—which is the ratio of the total durations of viewing and pauses to the viewing duration of user i over a given time interval $T \longrightarrow \infty$:

$$\gamma_i = \lim_{T\to\infty} \frac{\omega_i^T + b_i^T}{\omega_i^T} \quad (10)$$

The user is considered active at time t if they are downloading at that moment; otherwise, the user is considered inactive.

In the wireless communication channel, signal attenuation during propagation occurs uniformly across the entire bandwidth for a specific user at a particular time. Let us introduce the variable $C_i(T)$, which equals the data transmission speed through the wireless channel if all available resources were allocated to the user i at time t.

This is called the maximum achievable channel speed. The assumptions used for the wireless channel model are:

During the transmission of one packet k from segment j by user i in the downlink, the maximum achievable wireless channel speed is constant:

$$C_i(T) = C_{i,j,k}, t_{i,j,k} \le t \le t_{i,j,k} + \Delta t_{i,j,k}, \quad (11)$$

where $t_{i,j,k}$ is the moment when user j, $\Delta t_{i,j,k}$ is the duration of downloading packet k by user i from segment j, $C_{i,j,k}$ is being the maximum achievable channel speed during the packet download.

The sequence of random variables:

$$C_{i,1}^{-1}, C_{i,2}^{-1}, \dots, i = \overline{1,N}, \quad (12)$$

where $C_{i,1}^{-1} = \frac{1}{P_{i,j}} \sum_{k=1}^{P_{i,j}} \frac{1}{C_{i,j,k}}$, forms an ergodic random process with finite mathematical expectations $E[C_i^{-1}]$ and variation coefficients ν_i^C.

At each moment t, the scheduling algorithm distributes portions of the channel resources $\alpha_i(t)$ for all users:

$$A(t) = \{\alpha_i(t), \quad i = \overline{1,N}\} \quad (13)$$

An evident constraint on the operation of the scheduling algorithm is the finite volume of available resources:

$$\forall t: \sum_{i=1}^{N} \alpha_i(t) \le 1 \quad (14)$$

To optimize resource allocation in a Bluetooth wireless network with increased data transfer rates using adaptive modulation with a three-zone buffer, the scheduler has access to prior data, including portions of allocated channel resources, maximum achievable channel speeds, and the volume of transmitted data for each individual user:

$$A(t) = \mathcal{A}(\alpha_i(\tau),\ C_i(\tau); \tau < t,\ \ i = \overline{1,N}), \quad (15)$$

where $A(\cdot)$ is represents the scheduling algorithm.

To ensure the security of video streams over a Bluetooth wireless network with increased data transfer rates using adaptive modulation with a three-zone buffer, the following assumptions are considered for the scheduling algorithm [10, 17, 46]:

The scheduler allocates all available channel resources at every moment.

The scheduler does not allocate resources to inactive users.

Each active user is guaranteed a minimum portion of the channel resources.

When a new video data segment is requested by the video player, the problem of choosing the bit rate for the requested segment is solved by the following expression:

$$R_{i,j} = \mathcal{B}(R_{i,k},\ C_i(\tau), \alpha_i(\tau); k < j, \tau\ < t_{i,j}), \quad (16)$$

where $B(\cdot)$ is represents the algorithm for calculating the bit rate of segment j for user i, $R_{i,j}$ is the bit rate of segment j for user i, $t_{i,j}$ is the time when user i requests segment j.

The frequency of switching bit rates is limited:

$$\forall i: \frac{\sigma[R_i]}{E[R_i]} \le \nu_i^R, \quad (17)$$

where $E[R_i] = lim_{j\to\infty} E[R_{i,j}], \sigma[R_i] = lim_{j\to\infty} E[R_{i,j}]$.

The sequences $R_{i,1}, R_{i,2}, \dots,\ i = \underline{1,N}$ form ergodic random processes with finite mathematical expectations $E[R_i]$ and variation coefficients that do not exceed the values of ν_i^R respectively.

The presented analytical model describes the key components and parameters of a real video data transmission system over the HTTP protocol.

For all possible scheduling and video adaptation algorithms that meet the assumptions, the following inequality holds:

$$\sum_{i=1}^{N} (1 - \nu_i^R \nu_i^C) \frac{E[R_i]\, E[C_i^{-1}]}{q_i + \gamma_i} \le 1, \quad (18)$$

The relationship between all parameters of the video data transmission network is reproduced by dependencies on the features of the user behavior model (γ_i, q_i) video stream properties $(E[R_i])$ and the operation of the wireless channel $(E[C_i^{-1}])$ for each network participant.

The radio channel resource allocation algorithms for adaptive video streams, which are expressed by the ratio of buffering duration to viewing duration q_i, while considering the average bit rate of the viewed stream, are of great importance. It is worth noting that due to the presence of video stream adaptation to wireless channel conditions, the scheduling and video adaptation algorithms, denoted as A and B, respectively, influence the buffering factor. According to the research on quality criteria conducted in the first section, it is proposed to evaluate system performance using two criteria. The average value of the ratio of buffering duration to viewing duration:

$$\bar{q}(A,B) = \frac{1}{N} \left(\sum_{i=1}^{N} q_i(A,B)\right), \quad (19)$$

The average bitrate of the viewed video stream, which is a key parameter:

$$\bar{R}(A,B) = \frac{1}{N} \left(\sum_{i=1}^{N} E\ [R_i(A,B)]\right), \quad (20)$$

The primary goal is to determine the lower bound for all possible scheduling and video adaptation algorithms that meet the conditions introduced in the second section for the average ratio of buffering duration to viewing duration for all users in the system, provided that the average bitrate of the viewed stream for all users is not less than the given value $R_{a\vartheta g}$.

$$Q = \inf_{A,B:\bar{R}(A,B)\ge R_{a\vartheta g}, A\in\mathcal{A}, B\in\mathcal{B}} \bar{q}(A,B) \quad (21)$$

The task of finding the lower bound of the quality of experience (QoE) criterion Q is formulated as an optimization problem aimed at minimizing this criterion under certain constraints and conditions. The objective is to minimize $Q = \frac{1}{N} \sum_{i=1}^{N} q_i$ subject to:

$$\begin{cases} \sum_{i=1}^{N} \left(1 - \nu_i^R \nu_i^C\right) \frac{\bar{R}_i \overline{C_i^{-1}}}{q_i + \gamma_i} - 1 \le 0, \\ -\frac{1}{N} \sum_{i=1}^{N} \widetilde{R}_i + R_{a\vartheta g} \le 0 \\ \widetilde{R}_i \in [R_{min}, R_{min}], i = \overline{1,N} \\ -q_i \le 0, i = \overline{1,N} \end{cases} \quad (22)$$

$$\widetilde{R}_i = E\ [R_i] \text{ та } \widetilde{C_i^{-1}} = E[C_i^{-1}], \quad (23)$$

In this context, the optimization problem is non-linear with general constraints, making it a non-convex problem with no standard solutions [9–12, 15, 16, 21–27, 34, 35]. To solve this, a two-stage optimization approach is proposed.

First, an intermediate optimization problem is introduced, where a solution algorithm is already known. Then, the relationship between the main optimization problem and the intermediate one is established, followed by a relaxation of constraints to solve the original problem.

This approach involves solving the intermediate problem first, and then formulating the final problem with relaxed constraints. A new algorithm is proposed to solve this, comparing the performance of existing heuristic algorithms for wireless channel resource allocation based on the QoE criterion QQQ. The lower bound for adaptive video streams is derived and compared with heuristics for non-adaptive streams. Simulation modeling of heuristic scheduling algorithms for adaptive video transmission was performed with a fixed number of users per cell, while non-adaptive video transmission was simulated assuming the video stream bit rate viewed by all users equals $R_{a\vartheta g}$.

In summary, the challenges of securing video streams over a Bluetooth wireless network with increased data rates using adaptive modulation and a three-zone buffer were addressed [7–10, 17, 18]. A two-stage optimization approach was proposed: first, an intermediate optimization problem with a known solution was introduced, followed by establishing its relationship to the main problem. Finally, an optimization problem with relaxed constraints was formulated and solved [3, 7, 24–27, 34, 35].

An algorithm was developed to solve this optimization problem, and its performance was compared with existing wireless channel resource allocation heuristics. The study derived a bound for adaptive video streams and compared it with non-adaptive heuristics. Simulation modeling of heuristic scheduling algorithms for both adaptive and non-adaptive video was conducted, assuming a fixed number of users per cell. For non-adaptive video, the modeling assumed all users viewed video streams at the average bitrate $R_{a\vartheta g}$.

The study tackled the challenges of securing video streaming over Bluetooth networks using adaptive modulation with a three-zone buffer. A nonlinear optimization problem was formulated and solved using a two-stage approach [12–17, 19]. The proposed algorithm effectively enhanced video stream security. A comparative analysis of resource allocation methods demonstrated the benefits of adaptive modulation over non-adaptive approaches. As a result, the developed radio channel resource allocation algorithms proved effective in ensuring both security and efficiency for video streaming over Bluetooth networks with increased data rates.

Integrated Priority and Information Protection Strategy for Multi-Level Interaction Among Users:

The integrated strategy for managing priorities and information protection in Bluetooth wireless networks combines advanced traffic management and security technologies. It includes a multi-level interaction model that dynamically adjusts bandwidth and priorities based on data type and importance, ensuring secure transmission through priority buffering policies that consider transmission context and confidentiality [20–23].

Recent innovations, such as AI integration, enable real-time traffic analysis and adaptive decision-making. Machine learning optimizes transmission priorities and bandwidth, ensuring stable video streams even in challenging conditions [3, 7, 8, 12, 15, 16]. This approach enhances both security and efficiency, meeting modern demands for Bluetooth video streaming.

In the transmission buffer, Bluetooth packets are prioritized and transmitted using one of two modulation schemes based on their priority. Low-priority packets are sent at 3 Mbps to reduce errors. The Bluetooth ARQ (Automatic Repeat Request) mechanism, with adjustable flush timeouts, prevents packet delays that could lead to frame skips. The flush timeout is set at 1250 microseconds, equivalent to two Bluetooth timeslots, after which handshake packets stop [19–21]. Non-flushable settings protect against data loss in other streams [14, 19, 26, 27, 34, 46].

As technologies evolve, secure transmission and data confidentiality are increasingly vital. Modeling methods, such as the Gilbert-Elliott ergodic chain and Gilbert's Markov chains, improve understanding of wireless channel errors and support effective protection strategies [30–32]. Adaptive methods like adaptive frequency hopping (AFH) in Bluetooth ensure stable transmissions by avoiding interference.

End-to-end encryption (E2EE) is also becoming more common, offering robust protection against unauthorized access throughout the transmission process [20–25, 27, 31].

Currently, the modeling of the AWGN (Additive White Gaussian Noise) channel with a bit error rate (BER) of 10^{-5} at higher data transfer rates of 3 Mbps and an E_b/N_0(energy per bit to noise power spectral density ratio of 16 dB is widely used. This method allows for analyzing the response of various protection schemes to different channel conditions. The Gilbert-Elliott ergodic chain with two states in discrete time and Gilbert's Markov chain are applied to model the error characteristics of a wireless channel. Even with the use of modern technologies such as adaptive frequency hopping (AFH) in Bluetooth version 5.2, the Gilbert-Elliott model remains an effective tool for channel analysis, considering its limitations and impact on audio/video applications. Studying the average durations of good and bad channel states T_g and T_b, helps to understand the system's behavior in real-world operating conditions, while setting the timeout at the appropriate level allows for effective data flow management to ensure the security and reliability of information transmission. The average duration of a good state in seconds, and the duration of a bad state is $T_b = 0{,}25\ seconds$. In Bluetooth time slot units, where each time slot lasts 625 microseconds, $T_g = 3200$, and $T_b = 400$. Consequently, if the current state is good (g), the probability that the next state will also be good (g), (Pgg) is 0,9996875, while the probability that the next state will be bad (b), (Pbb) given the current state is 0.9975.

$$T_g = \frac{1}{1 - Pgg}, \quad T_b = \frac{1}{1 - Pbb} \tag{24}$$

At a speed of 3 Mbps, the bit error rate (BER) in the good state is 10^{-5}, and in the bad state, it is—10^{-4}. The two SNR states of 16.00 and 14.70 dB correspond to varying transmission conditions. The first SNR value is ideal for comparison with a single-stationary model, while the second is optimal for 2 Mbps transmission speeds. As SNR worsens below 10 dB, only basic rate-protected packets

remain viable. Adaptive User Priority (UP) schemes are effective for Enhanced Data Rate (EDR) modes, which build on earlier concepts like IBM's BlueHoc and Blueware, with specifications covering baseband, L2CAP, and multi-slot packet transmission [28–33, 44, 45]. Clock drift is considered in timing and scheduling, although real-world implementations may experience slower EDR mode switching.

Changes in priority buffering policies align with advanced traffic management and video security measures. Adaptive buffers improve data prioritization by considering factors like data importance, confidentiality, quality of service, and security requirements. Critical data, such as confidential information, is given higher priority to ensure faster and more secure transmission [20, 23, 28, 29, 31, 32, 44, 45].

The integration of adaptive modulation with a three-zone buffer allows dynamic adjustments to signal changes and transmission quality, optimizing bandwidth and reducing the risk of buffer overflow as data volumes and noise levels fluctuate. Modern priority buffering policies have become essential for securing video streams over Bluetooth networks, balancing transmission efficiency, data protection, and user satisfaction.

These policies prioritize data based on buffer fill levels. In zone 1, where the buffer is less full, protection strategies like random number generation are used [8–10]. In zone 3, when the buffer is nearly full, urgent data is transmitted immediately, with reduced protection to maintain speed. This approach optimizes security while managing data flow and resource use [1–6, 11, 17, 18]. Given the rise of cyber threats, such policies are crucial for ensuring strong data protection in dynamic network environments.

In zone 1 of the buffer, all Bluetooth packets of type I- or P-frames are automatically protected by sending them at a lower data transmission rate. B-frame packets are only protected in zone 1 if they pass the following test. A comparison is made between a uniformly distributed random number generated in the interval [0,1] and the fraction f, which determines the buffer's occupancy with packets relative to the zone's bandwidth (Fig. 2). If the random number is greater than f, the B-frame packet is also transmitted at a reduced transmission speed, indicating its protection. This test is implemented so that the number of protected B-frame packets increases linearly with the buffer's fill level in zone 1.

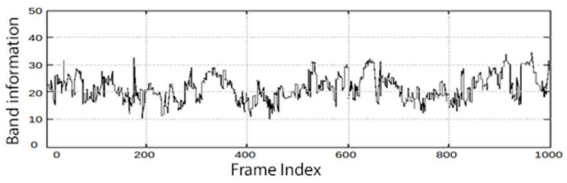

Figure 2: Temporal Change of Spatial Information
Source: Aggregated from sources [8–13, 15, 16, 22–27, 34, 35]

As the buffer fills and packets enter zone 2, a distinct priority policy applies for P-frames. In this zone, I-frames remain protected, while B-frames lose their protection. P-frames are partially protected based on the ratio of internally encoded macroblocks, with protection levels dynamically adjusted as data and buffer usage change. The boundary between protected and unprotected P-frames shifts according to historical encoding ratios, adapting in real-time.

In zone 3, when the buffer is full, B-frames and P-frames lose protection, but I-frames retain it, like in zone 1, using random number generation and fraction comparison. The UP policy is linear in zones 1 and 3 but remains nonlinear for P-frames, balancing content importance with buffer fill levels. This ensures that P-frame output adjusts toward a linear mode, compensating for buffer saturation.

As security and efficiency demands in video transmission grow, improving buffer priority policies become crucial [12, 22–24, 32, 37, 44–46]. Modern methods safeguard data while ensuring quality transmission. Adaptive buffers, combined with modulation technology, allow dynamic responses to network conditions, enhancing security and performance in wireless communication.

Dynamic frame content regulation for enhancing video stream protection efficiency:

Dynamic frame content regulation is a key approach for optimizing cybersecurity and information protection in video sequences by managing frame sizes based on parameters like brightness, motion, and texture [23–27, 30–32, 34, 35, 44, 45]. Real-time adjustments, such as resolution changes or compression, are made to ensure efficient video transmission.

Modern systems analyze brightness, motion, texture, and context, allowing quick responses to video stream alterations. Advanced algorithms adapt transmission parameters, reducing resolution or applying compression during high motion to decrease data volume while maintaining essential details. This improves network efficiency and prevents unauthorized access [13].

Dynamic regulation is especially important in Bluetooth wireless networks using adaptive modulation and a three-zone buffer, optimizing bandwidth and reducing data leakage during intense video changes to balance protection and efficiency [2, 7, 9]. Adjusting the ratio between buffer zones enhances system resilience. Spatial content affects I-frame size and transmission speed, while temporal content impacts B- and P-frame processing, crucial for confidentiality. Research [36] evaluates spatial and temporal information using brightness filtering and the Sobel algorithm to strengthen video data protection (Fig. 3).

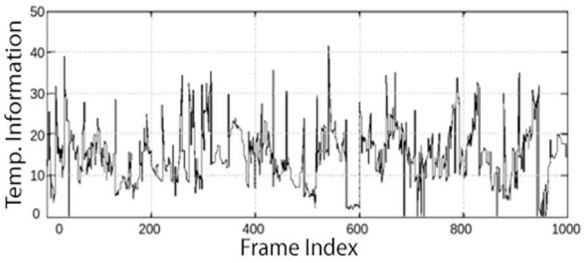

Figure 3: Temporal information changes over time for the same sequence
Source: Aggregated from sources [11, 15, 16, 22–27, 34, 35]

The analysis of the temporal dimension of video data involves calculating brightness differences between frames

and computing frame-by-frame standard deviation (SD), which helps assess changes in spatial and temporal information. This highlights the need for dynamic buffer zone adjustments to ensure efficient data storage and processing, particularly for cybersecurity and data protection.

Dynamic frame regulation is crucial for optimizing data transmission and security over Bluetooth connections. Bluetooth frames made up of asynchronous connectionless (ACL) packets, occupy multiple time slots, and their size impacts payload. Continuous monitoring of content characteristics such as brightness, motion, and texture allows for dynamic adjustments in frame sizes, improving transmission efficiency and security [7, 8, 14, 18, 25, 46].

Packet size quantization often increases Bluetooth packet sizes, reducing bandwidth efficiency. Dynamic adjustments ensure that when packet sizes don't match content, smaller transmission schemes (e.g., switching from 3DH5 to 3DH3 or 3DH1) can improve efficiency [3–5, 18, 28, 34–36]. A key challenge is managing partially filled packets, which wastes bandwidth. Research suggests forming filled Bluetooth packets to enhance performance, though this could affect noise immunity [1, 2, 26, 28].

The CQDDR model adjusts packet types based on channel quality but overlooks content and network congestion. An improved scheme using a three-zone buffer effectively prioritizes data transmission by considering these factors [20, 25, 34]. Additionally, Hamming code error correction (DAEC and SEC) enhances transmission reliability by correcting errors, improving both bandwidth utilization and data protection.

5. Conclusions

Ensuring secure video streaming over Bluetooth networks with enhanced data rates requires adaptive modulation and a three-zone buffer. To meet confidentiality, integrity, and availability requirements, strategies combining data protection and adaptive resource allocation are essential. Buffer priority policies adjust protection based on buffer fill levels, safeguarding I-frames in critical zones and optimizing resource use.

As Bluetooth traffic increases, adaptive buffers, and modulation maintain video quality. Adjustments based on frame brightness and buffer size improve stream management, while Hamming codes enhance reliability. A two-stage optimization, using cryptography and data analysis, ensures secure and efficient streaming, meeting modern cybersecurity standards.

Overall, secure video streaming over Bluetooth networks demands an integrated approach that combines encryption, authentication, and quality management to ensure data protection.

References

[1] W. Wang, et al., Mobile Node Design of Indoor Positioning System based on Bluetooth and LoRa Network, Journal of Physics: Conference Series, 1738(1) (2021).

[2] R. Razavi, M. Fleury, M. Ghanbari, Low-Delay Video Control in a Personal Area Network for Augmented Reality, 4th Visual Information Engineering (2007) 1245–1300.

[3] W. Wilkowska, et al., Analyzing Technology Acceptance and Perception of Privacy in Ambient Assisted Living for using Sensor-based Technologies, PLoS ONE, 17(7) (2022).

[4] S. Ye, R. S. Blum, L. J. Cimini Jr., Adaptive Modulation for Variable-Rate OFDM Systems with Imperfect Channel Information, in: 55th IEEE Vehicular Technology Conference, 2 (2002) 767–771.

[5] M. J. Haenssgen, After Access: Inclusion, Development, and a More Mobile Internet, Journal of Human Development and Capabilities, 18(1) (2017).

[6] S. W. Campbell, From Frontier to Field: Old and New Theoretical Directions in Mobile Communication Studies, Communication Theory, 29(1) (2019) 46–65. doi: 10.1093/ct/qty021.

[7] A. Iyer, U. B. Desai, A Comparative Study of Video Transfer over Bluetooth and 802.11 Wireless MAC, IEEE Wireless Communications and Networking Conference, 3 (2003) 2053–2057.

[8] R. Prasad, Book Review: After Access: Inclusion, Development and a More Mobile Internet, Communication and the Public, 2(1) (2017).

[9] C. H. Chia, M. S. Beg, Realizing MPEG-4 Video Transmission over Wireless Bluetooth Link via HCI, IEEE Transactions on Consumer Electronics, 49(4) (2003) 1028–1034.

[10] O. Kryvoruchko, Y. Kostiuk, A. Desiatko, Systematization of Signs of Unauthorized Access to Corporate Information based on Application of Cryptographic Protection Methods, Ukrainian Scientific Journal of Information Security, 30(1) (2024) 140–149.

[11] K. A. Pearce, Rice Ronald. Digital Divides. From Access to Activities: Comparing Mobile and Personal Computer Internet Users, J. Commun. 63(4) (2013) 721–744. doi: 10.1111/jcom.12045.

[12] R. Razavi, M. Fleury, M. Ghanbari. Power-Constrained Fuzzy Logic Control of Video Streaming over a Wireless Interconnect, EURASIP Journal on Advances in Signal Processing (2008). doi: 10.1155/2008/560749.

[13] C. Scheiter, et al., A System for QOS-enabled MPEG-4 Video Transmission over Bluetooth for Mobile Applications, International Conference on Multimedia and Expo (ICME'03), 1 (2003) 789–792. doi: 10.1109/ICME.2003.1221036.

[14] S. Tahir, et al., Hybrid Congestion Sharing and Route Repairing Protocol for Bluetooth Networks, Wseas Transactions On Computers 20 (2021) 49–55. doi: 10.37394/23205.2021.20.6.

[15] G. R. Reddy, et al., An Efficient Algorithm for Scheduling in Bluetooth Piconets and Scatternets, Wireless Networks, 16(7) (2009) 1799–1816. doi: 10.1007/s11276-009-0229-3.

[16] T. Dave, U. Pandya, Simultaneous Monitoring of Motion ECG of Two Subjects using Bluetooth Piconet and Baseline Drift, Biomedical Engineering Letters, 8(4) (2018) 365–371. doi: 10.1007/s13534-018-0081-4.

[17] Core Specification of the Bluetooth System, Version 2.1+EDR (2007). URL: http://www.Bluetooth.com

[18] Q. Li, M. van der Schaar, Providing adaptive QoS to layered video over wireless local area networks through realtime retry limit adaptation, IEEE Transactions on Multimedia, 6(2) (2004) 278–290.

[19] Z.-K. Chen, An Adaptive FEC to Protect RoHC and UDP-Lite H.264 Video Critical Data, Journal of Zhejiang University—Science A, 7(5) (2006). doi: 10.1631/jzus.2006.A0910

[20] C.-H. Yang, S.-J. Lee, Virtual Scatternet Formation for Supporting Multicast in Bluetooth Networks, Int. J. New Technol. Res. (2022).

[21] L.-J. Chen, et al., Audio Streaming over Bluetooth: an Adaptive ARQ Timeout Approach, in: 24th International Conference on Distributed Computing Systems, 24 (2004) 196–201.

[22] C. Ru, et al., A New UEP Scheme for Robust Video Transmission in MIMO System, China Communications, 4(5) (2006) 102–108.

[23] S. Li, Y. Lou, B. Liu, Bluetooth Aided Mobile Phone Localization, ACM Transactions on Embedded Computing Systems (TECS), 13(4) (2014) 1–15. doi: 10.1145/2560018.

[24] L.-J. Chen, H.-H. Hung, A Two-State Markov-Based Wireless Error Model for Bluetooth Networks, Wireless Personal Communications, 58(4) (2009) 657–668. doi: 10.1007/s11277-009-9899-5.

[25] R. Razavi, M. Fleury, M. Ghanbari, Deadline-Aware Video Delivery in a Disrupted Bluetooth Network, IEEE Sarnoff Symposium (2007). doi: 10.1109/SARNOF.2007.4567352.

[26] Y. Kostiuk, Y. Konstantinov, Improved Security Methods in 4G Networks to Provide Effective Protection Against Data Transmission Attacks, (Series "Pedagogy", Series "Law", Series "Economics", Series "Physical and Mathematical Sciences", Series "Technology"): Journal, 6(34) (2024).

[27] S. Tahir, A Self-organizing Location and Mobility-Aware Route Optimization Protocol for Bluetooth Wireless, Int. J. Adv. Comput. Sci. Appl. (2016). doi: 10.14569/IJACSA.2016.070631.

[28] C.-M. Chen, C.-W. Lin, Y.-C. Chen, Packet Scheduling for Video Streaming over Wireless with Content-Aware Packet Retry Limit, in: 8th IEEE Workshop on Multimedia Signal Processing (MMSP'06) (2006) 409–414.

[29] N. Golmie, N. Chevrollier, O. Rebala, Bluetooth and WLAN Coexistence: Challenges and Solutions, IEEE Wireless Communications, 10(6) (2003) 22–29. doi: 10.1109/MWC.2003.1265849

[30] R. Razavi, et al., An Efficient Packetization Scheme for Bluetooth Video Transmission, Electronic Letters, 42(20) (2006) 1143–1145.

[31] J. H. Yoon, S.-B. Lee, S.-C. Park, Packet and Modulation Type Selection Scheme based on Channel Quality Estimation for Bluetooth Evolution Systems, IEEE Wireless Communications and Networking Conference (WCNC '04), 2 (2004) 1014–1017.

[32] A. E. Khalil, et al., Efficient Speaker Identification from Speech Transmitted over Bluetooth Networks, Int. J. Speech Technol. 17(4) (2014).

[33] V. Lakhno, et al., Methodology for Placing Components of a Video Surveillance System for Smart City Based on a Composite Cost Optimization Model, Software Engineering Perspectives in Systems, 501 (2022). doi: 10.1007/978-3-031-09070-7_2.

[34] A. B. Nahas, et al., BlueFlood: Concurrent Transmissions for Multi-Hop Bluetooth 5—Modeling and Evaluation, Comput. Res. Repository, 2(4(22)) (2021) 1–30. doi: 10.1145/346275.

[35] T. Chi, M. Chen, A Frequency Hopping Method for Spatial RFID/WiFi/Bluetooth Scheduling in Agricultural IoT, Wireless Networks, 25(2) (2017) 805–817. doi: 10.1007/s11276-017-1593-z.

[36] K. P. Rajesh, Fuzzy Logic Controller for Wireless Video Transmission, J. Comput. Sci. 7(7) (2011) 1119–1127. doi: 10.3844/jcssp.2011.1119.1127.

[37] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[38] V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421.

[39] V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.

[40] V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.

[41] V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.

[42] V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.

[43] V. Sokolov, P. Skladannyi, A. Platonenko, Video Channel Suppression Method of Unmanned Aerial Vehicles, in: IEEE 41st International Conference on Electronics and Nanotechnology (2022) 473–477. doi: 10.1109/ELNANO54667.2022.9927105.

[44] S. K. Mohsin, M. A. Mohammed, H. M. Yassien, Developing of Bluetooth Mesh Flooding between Source-Destination Linking of Nodes in Wireless Sensor Networks, Eastern-European Journal of Enterprise Technologies 6(9(114)) (2021). : 10.15587/1729-4061.2021.248978.

[45] R. Razavi, M. Fleury, M. Ghanbari, Detecting Congestion within a Bluetooth Piconet: Video Streaming Response, London Communications Symposium (2006) 181–184.
[46] S. Rzaieva, et al., Methods of Modeling Database System Security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 384–390.