International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)

Koffka Khan[1], Wayne Goodridge[1]
[1]Department of Computing and Information Technology, Faculty of Science and Agriculture, The University of the West Indies, St. Augustine Campus, TRINIDAD AND TOBAGO.
Email address: koffka.khan@gmail.com

Abstract**—** *In the face of natural and man-made disasters, the need for efficient and resilient communication networks is paramount. Video streaming plays a critical role in disaster response by facilitating real-time information exchange, situational awareness, and decision-making. To comprehensively address the multifaceted challenges of video streaming in disaster scenarios, we present the Disaster-Resilient Video Streaming Taxonomy (DR-ViST). DR-ViST provides a structured framework for categorizing and understanding the intricate components of video streaming within resilient communication networks during disaster response efforts. The taxonomy encompasses various dimensions, including network infrastructure, streaming protocols, video compression, resilience strategies, disaster scenarios, edge and fog computing, quality monitoring, user devices, security, content delivery, resource management, and practical case studies. By employing DR-ViST, researchers, practitioners, and disaster response professionals can navigate the complexities of video streaming in disaster situations. This taxonomy serves as a valuable guide for designing, optimizing, and deploying video streaming solutions that ensure effective communication, situational awareness, and response coordination when it matters most. DR-ViST is a versatile tool that fosters a deeper understanding of the critical role video streaming plays in disaster response and helps pave the way for innovative solutions to enhance resilience in communication networks during times of crisis.*

Keywords**—** *Disaster: Resilient: Video Streaming.*

I. INTRODUCTION

In an era marked by increasing instances of natural disasters and unforeseen calamities, the ability to establish and maintain resilient communication networks is an imperative for disaster response and recovery efforts. Among the array of communication tools at our disposal, video streaming emerges as a pivotal asset in these critical scenarios, facilitating real-time information dissemination, remote collaboration, and situational awareness. To navigate the complexities and challenges of integrating video streaming into disaster response, we introduce the Disaster-Resilient Video Streaming Taxonomy (DR-ViST).

The rapid evolution of technology has given rise to diverse communication networks, video streaming protocols, and innovative content delivery strategies. In the realm of disaster response, these technologies must not only meet the demands of high-quality video transmission but also exhibit robustness and adaptability in the face of disrupted infrastructure and dynamic operational conditions [7]. DR-ViST addresses this multifaceted landscape by providing a structured taxonomy that organizes and categorizes the key components and considerations necessary for effective video streaming during disaster response.

This taxonomy encompasses a wide spectrum of dimensions, each playing a vital role in the successful deployment of video streaming solutions. It delves into the intricacies of network infrastructure, streaming protocols, video compression techniques, resilience and redundancy strategies, the spectrum of disaster scenarios, the role of edge and fog computing, quality monitoring, user device considerations, security and privacy, content delivery mechanisms, resource allocation, and management strategies. Furthermore, DR-ViST incorporates practical case studies to illustrate real-world deployments, challenges, and lessons learned in the field.

As disaster response professionals, researchers, and practitioners strive to harness the potential of video streaming to enhance their operations, DR-ViST serves as a guiding compass. It empowers them to navigate the labyrinth of choices, trade-offs, and technological nuances to develop video streaming solutions that are not just functional but resilient, ensuring effective communication and coordination in the most adverse and unpredictable conditions.

We delve into the depths of DR-ViST, illuminating the critical elements and principles that underpin the successful integration of video streaming in disaster response. By embracing this taxonomy, we aim to foster a profound understanding of the pivotal role that video streaming plays in safeguarding lives, facilitating response efforts, and ultimately contributing to the resilience of communication networks when disaster strikes.

In Section II we outline the DR-ViST taxonomy. In Section III we give a discussion of the taxonomy. The conclusion is given Section IV.

II. TAXONOMY

The DR-ViST taxonomy is as follows:

1. Disaster Response Network Infrastructure [16]:

Wired Infrastructure:

Fiber-optic cables: Fiber-optic cables are high-capacity, long-distance transmission mediums that use light signals to carry data. They offer exceptional bandwidth, low latency, and resistance to environmental factors, making them ideal for disaster-resilient communication networks. These cables can withstand physical damage better than traditional copper wires.

Koffka Khan and Wayne Goodridge, "A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 4, pp. 84-91, 2023.

Ethernet connections: Ethernet is a widely used wired networking technology that enables high-speed data transmission over copper or fiber-optic cables. Ethernet connections are essential for connecting devices in local area networks (LANs) and can be a foundational component in disaster response network infrastructure.
Wireless Infrastructure:
Cellular networks (e.g., 4G, 5G): Cellular networks provide wireless communication services through a network of cell towers. 4G and 5G networks offer high-speed data connectivity and are vital for mobile devices used in disaster response. They provide both voice and data services and can be rapidly deployed.
Satellite communication: Satellite communication systems use geostationary or low-earth orbit satellites to relay signals between ground stations. These systems are critical when terrestrial infrastructure is compromised during disasters. They offer wide coverage but can have latency issues due to the long distances involved.
Mesh networks: Mesh networks are decentralized wireless networks where each node can relay data for others. They are highly resilient because they can self-organize and route traffic dynamically. Mesh networks can be crucial in disaster scenarios where traditional infrastructure is damaged, as they allow for the creation of ad-hoc communication networks.
Ad Hoc Networks:
Mobile ad hoc networks (MANETs): MANETs are self-configuring, infrastructure-less networks formed by mobile devices that communicate directly with each other. They are adaptable and can be set up quickly in disaster-stricken areas where traditional infrastructure may be unavailable or unreliable. MANETs enable peer-to-peer communication.
Delay-tolerant networks (DTNs): DTNs are designed to operate in challenging environments where network connectivity is intermittent or unpredictable. They store and forward data between nodes when connectivity is available. DTNs are well-suited for disaster response in remote or austere environments where network links are unreliable or disrupted.

Each of these components within the Disaster Response Network Infrastructure category serves a unique purpose in establishing resilient communication networks during disaster response efforts. The choice of infrastructure elements will depend on the specific disaster scenario, available resources, and the need for rapid deployment and adaptability to ensure effective communication and coordination among responders and affected communities.
2. Video Streaming Protocols [11], [14], [15]:
Real-Time Protocols:

RTP (Real-Time Transport Protocol): RTP is a network protocol used for delivering audio and video over IP networks. It provides mechanisms for time-stamping and sequencing packets, allowing real-time synchronization of multimedia streams. RTP is often used in conjunction with RTCP (RTP Control Protocol) for monitoring and control.
RTSP (Real-Time Streaming Protocol): RTSP is a network control protocol used for initiating and controlling streaming media sessions. It allows clients to request and control the delivery of multimedia content from servers. RTSP is commonly used for live video streaming and video-on-demand services.
WebRTC (Web Real-Time Communication): WebRTC is a collection of open-source technologies that enable real-time communication, including audio and video streaming, directly within web browsers and mobile applications. It uses secure peer-to-peer connections for efficient and low-latency communication.
HTTP-Based Protocols:
HTTP Live Streaming (HLS): HLS is an adaptive streaming protocol developed by Apple. It breaks multimedia content into small chunks and dynamically adjusts the quality of each chunk based on the viewer's network conditions. HLS is widely used for delivering video content over the internet, including live events.

Dynamic Adaptive Streaming over HTTP (DASH): DASH [12] is an industry-standard adaptive streaming protocol. It enables dynamic switching between different quality levels of video based on available bandwidth and device capabilities [13]. DASH is codec-agnostic and widely adopted for delivering streaming video over HTTP.
Smooth Streaming: Smooth Streaming is a proprietary adaptive streaming protocol developed by Microsoft. It delivers multimedia content in chunks, adjusting quality based on the viewer's bandwidth. It is commonly used in Microsoft's ecosystem and was part of the Microsoft Silverlight technology.
P2P Streaming:
BitTorrent-based streaming: BitTorrent-based streaming leverages the peer-to-peer BitTorrent protocol to distribute video content. It allows users to stream content while simultaneously sharing it with others, reducing the load on central servers. This approach can be useful for cost-effective and scalable streaming.
WebTorrent: WebTorrent is a JavaScript library that enables peer-to-peer streaming directly in web browsers. It combines BitTorrent and WebRTC technologies to create efficient and decentralized streaming solutions for web applications.
P2P video conferencing protocols: These protocols are designed for real-time video conferencing and collaboration. They often employ peer-to-peer communication to reduce latency and improve scalability, making them suitable for applications like remote meetings and disaster response coordination.

Each of these video streaming protocols serves specific purposes and has distinct characteristics. The choice of protocol depends on factors such as the nature of the content, target audience, network conditions, and the desired level of control and security. In disaster response scenarios, the selection of an appropriate protocol can significantly impact the effectiveness of video streaming for communication and situational awareness.
3. Video Compression and Quality [9]:
Compression Standards:
H.264/AVC (Advanced Video Coding): H.264 is a widely adopted video compression standard known for its efficient compression algorithms. It is used for video streaming, video

Koffka Khan and Wayne Goodridge, "A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 4, pp. 84-91, 2023.

conferencing, and video storage. H.264 achieves high-quality video at lower bitrates, making it suitable for bandwidth-constrained scenarios.

H.265/HEVC (High-Efficiency Video Coding): H.265, also known as HEVC, is the successor to H.264. It offers significantly improved compression efficiency, allowing for the delivery of high-quality video at lower bitrates. HEVC is essential for delivering 4K and UHD video content over networks with limited bandwidth.

VP9: VP9 is an open-source video compression format developed by Google. It competes with H.265 by offering high compression efficiency, making it suitable for streaming high-definition video on the internet. VP9 is widely used in platforms like YouTube and WebRTC.

Quality Adaptation:

Adaptive Bitrate Streaming: Adaptive bitrate streaming (ABR) is a technique that adjusts the quality of video streams in real time based on the viewer's available bandwidth and device capabilities. ABR protocols, like HLS and DASH, deliver video content in multiple quality levels, allowing seamless switching to prevent buffering and provide the best possible viewing experience.

Quality of Service (QoS) Mechanisms: QoS mechanisms encompass various techniques and strategies for monitoring and ensuring the quality of video streams. This includes minimizing packet loss, optimizing network routing, and prioritizing video traffic to maintain a smooth viewing experience.

Video Transcoding for Adaptive Streaming: Video transcoding involves converting video content from one codec or format to another. In the context of adaptive streaming, transcoding is used to create multiple versions of video content at different quality levels. Transcoding can be performed in real time to adapt to changing network conditions and viewer preferences.

Effective video compression and quality adaptation are crucial for disaster response scenarios. Bandwidth constraints, variable network conditions, and diverse user devices necessitate efficient video compression to ensure that critical information can be transmitted reliably. Quality adaptation mechanisms are equally vital, as they allow video streams to adjust dynamically to deliver the best possible viewing experience, even when network conditions are suboptimal.

By incorporating the appropriate compression standards and quality adaptation techniques, disaster response teams can optimize video streaming to provide situational awareness, coordinate response efforts, and communicate effectively with stakeholders, all while ensuring that bandwidth and network resources are used efficiently.

4. Resilience and Redundancy [18]:

Network Resilience:

Network Redundancy: Network redundancy involves the creation of duplicate network infrastructure components to ensure that communication remains available in case of component failure. This can include redundant links, routers, and switches. In disaster response scenarios, network redundancy is crucial for maintaining connectivity even when network elements are damaged or disrupted.

Load Balancing: Load balancing techniques distribute network traffic across multiple servers or paths to ensure that no single server or path is overwhelmed. Load balancers monitor the health of network resources and make real-time routing decisions to optimize resource usage and maintain network stability during high traffic loads.

Failover Mechanisms: Failover mechanisms are designed to automatically switch network traffic to a backup path or resource when the primary path or resource fails. This ensures continuous communication and minimizes downtime in the event of network failures. Failover mechanisms are particularly important for critical disaster response operations.

Content Resilience:

Content Replication: Content replication involves creating multiple copies of data or video streams and distributing them across geographically diverse locations or servers. This redundancy ensures that content remains available even if one server or location becomes inaccessible or experiences issues.

Distributed Content Caching: Distributed content caching systems store frequently accessed content at the edge of the network, closer to end-users. Caches reduce the load on central servers and improve content delivery speed. In disaster response scenarios, distributed caching can mitigate the impact of network congestion.

Error Correction Codes: Error correction codes (ECC) are mathematical algorithms that add redundant data to transmitted information, allowing receivers to detect and correct errors. ECC is essential for maintaining data integrity in unreliable or lossy network environments. It is particularly valuable for video streaming to ensure that received frames or packets are error-free.

Resilience and redundancy are foundational principles for disaster response communication networks. These strategies ensure that critical communication can continue even in the face of network disruptions, equipment failures, or increased demand. By incorporating network redundancy, load balancing, failover mechanisms, content replication, distributed caching, and error correction codes, disaster response teams can enhance the reliability and availability of video streaming services, facilitating better situational awareness and response coordination. These techniques are instrumental in ensuring that communication networks remain operational and responsive when they are needed most.

5. Disaster Scenarios [8]:

Natural Disasters:

Earthquakes: Earthquakes are sudden shaking or trembling of the Earth's surface caused by tectonic plate movements. They can disrupt communication networks through physical damage to infrastructure, including fiber optic cables, cell towers, and power lines. Additionally, they may trigger aftershocks, posing further risks to network stability.

Hurricanes: Hurricanes are powerful tropical storms with high winds and heavy rainfall. They can damage communication infrastructure through strong winds, flooding, and storm surges. Post-hurricane recovery efforts often require resilient communication networks to coordinate response and aid distribution.

Koffka Khan and Wayne Goodridge, "A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 4, pp. 84-91, 2023.

Floods: Floods result from excessive rainfall, storm surges, or dam failures. They can inundate critical infrastructure such as data centers, cell towers, and network facilities. Floods disrupt communication networks by causing equipment damage and power outages.
Wildfires: Wildfires are uncontrolled fires that spread rapidly through vegetation. They can damage communication infrastructure through direct flames, smoke, and ash. Smoke can impair visibility and disrupt wireless communication signals.
Man-Made Disasters:
Terrorism: Acts of terrorism can intentionally target critical infrastructure, including communication networks. Explosions, cyberattacks, and physical damage to network components can result in communication breakdowns during and after terrorist incidents.
Cyberattacks: Cyberattacks, including Distributed Denial of Service (DDoS) attacks and ransomware, can disrupt communication networks by overwhelming servers, encrypting data, or compromising network security. Cyberattacks can be orchestrated by malicious actors to disrupt critical services.
Infrastructure Failures: Infrastructure failures, such as bridge collapses, power outages, or transportation accidents, can indirectly impact communication networks by damaging fiber optic cables, utility poles, or data centers. These failures can disrupt network connectivity in affected areas.

Each disaster scenario presents unique challenges to communication networks, and the resilience of these networks is vital for effective disaster response. Understanding the specific risks and vulnerabilities associated with each disaster type allows for the development of tailored strategies and technologies to ensure that video streaming and communication capabilities remain available during and after these events. Disaster response teams must prepare for a range of scenarios to ensure that communication infrastructure remains operational in the face of adversity.
6. Edge Computing and Fog Computing [4]:
Edge Servers:

Deploying video servers at the network edge: Edge servers are positioned closer to the end-users or devices, reducing the latency for video streaming. They cache and deliver video content locally, minimizing the need for data to travel to centralized data centers. In disaster response scenarios, deploying edge servers can significantly improve the responsiveness and availability of video streams, even in remote or disaster-affected areas.

Edge analytics for video processing: Edge servers can host video analytics applications that process video data at or near the source. This enables real-time analysis, object detection, facial recognition, and other video processing tasks without relying on central data centers. Edge analytics enhance situational awareness and can trigger alerts or actions based on video content, improving disaster response decision-making.
Fog Nodes:

Fog computing for real-time video analysis: Fog computing extends edge computing capabilities by distributing computing resources throughout the network. Fog nodes, strategically placed within the network, can perform real-time video analysis tasks such as image recognition, anomaly detection, and event identification. This is especially valuable in disaster response for identifying critical situations or hazards.

Fog-based video transcoding: Video transcoding at fog nodes allows for on-the-fly conversion of video streams to different formats or bitrates based on network conditions and viewer devices. This dynamic transcoding improves the adaptability and quality of video streams, ensuring that responders and stakeholders receive the best possible video experience during disaster response efforts.

Edge computing and fog computing are pivotal in disaster response scenarios where timely and efficient video processing is essential. By bringing compute resources closer to the data source and the end-users, these approaches minimize latency, reduce dependence on centralized data centers, and enhance the resilience of video streaming in challenging environments. Edge and fog computing enable real-time video analysis, content optimization, and responsive decision-making, making them integral components of the DR-ViST taxonomy for disaster response communication networks.
7. QoS and QoE Monitoring [3], [5]:
Quality of Service (QoS):
Network Latency: Network latency refers to the delay or time it takes for data packets to travel from the source to the destination. Low latency is essential for real-time video streaming to ensure minimal delay between sending and receiving video frames. Monitoring and managing network latency help maintain smooth video playback and responsiveness.
Bandwidth Availability: Bandwidth availability represents the amount of data that can be transmitted over a network connection in a given time frame. In video streaming, sufficient bandwidth is crucial for delivering high-quality video without buffering or degradation in resolution. QoS mechanisms ensure that adequate bandwidth is allocated to video streams during disaster response operations.
Jitter and Packet Loss: Jitter refers to the variation in packet arrival times in a network. Packet loss occurs when data packets are lost or dropped during transmission. Both jitter and packet loss can negatively impact video quality and user experience. QoS mechanisms address these issues by minimizing jitter and mitigating packet loss through error correction or redundancy.
Quality of Experience (QoE):
User Experience Metrics: QoE metrics include various user-centric measurements such as video start time, buffering events, and rebuffering ratio. These metrics assess the overall quality of the video streaming experience from the viewer's perspective. Monitoring QoE metrics helps identify and address issues that may impact user satisfaction.
Viewer Feedback and Satisfaction: Gathering viewer feedback through surveys or user ratings provides valuable insights into the quality of video streaming services. Viewer satisfaction levels, feedback on video quality, and user-reported issues

Koffka Khan and Wayne Goodridge, "A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 4, pp. 84-91, 2023.

contribute to improving disaster response communication networks and video streaming solutions.

Video Playback Smoothness: Smooth video playback is critical for maintaining viewer engagement and comprehending critical information. Video playback smoothness is affected by factors like buffering events, frame rate, and bitrate adaptation. Monitoring and optimizing these factors ensure that video content is delivered seamlessly, especially in bandwidth-constrained or unreliable network conditions.

Effective QoS and QoE monitoring are essential for delivering a satisfactory video streaming experience during disaster response operations. By continuously assessing and managing network latency, bandwidth, jitter, packet loss, user experience metrics, viewer feedback, and video playback smoothness, disaster response teams can ensure that video communication remains reliable and responsive. QoS and QoE monitoring tools and practices are indispensable for maintaining situational awareness, coordinating efforts, and providing essential information to decision-makers and responders in disaster scenarios.

8. User Devices and Endpoints [2]:

Smartphones and Tablets:

Mobile Streaming Apps: Smartphones and tablets are commonly used for video streaming during disaster response. Mobile streaming apps provide a convenient way for users to access live video feeds, receive alerts, and collaborate with other responders. These apps often support adaptive streaming to deliver the best quality based on the device and network conditions.

Responsive Design: Responsive design ensures that streaming apps and websites adapt to various screen sizes and orientations. This is crucial for ensuring that video content is accessible and user-friendly on different smartphones and tablets, regardless of the device's form factor.

Computers and Laptops:

Web-Based Streaming: Computers and laptops can access video streams through web-based platforms. This approach allows users to view live video feeds and participate in video conferencing sessions directly from web browsers without the need for additional software installations.

Dedicated Video Conferencing Software: Dedicated video conferencing software applications, such as Zoom, Microsoft Teams, and Cisco Webex, are often used on computers and laptops for video communication and collaboration. These platforms offer features like screen sharing, chat, and document sharing, enhancing remote coordination during disaster response efforts.

IoT Devices:

Surveillance Cameras: IoT surveillance cameras, including fixed and PTZ (pan-tilt-zoom) cameras, are deployed for real-time video capture and monitoring in disaster-affected areas. These cameras can stream video feeds to command centers and mobile devices, providing critical situational awareness.

Wearable Cameras: Wearable cameras, such as body-worn cameras or helmet-mounted cameras, are used by first responders to capture and stream live video from their point of view. These devices provide real-time insights into on-the-ground conditions, allowing remote teams to make informed decisions.

Drones for Aerial Video Capture: Drones equipped with cameras are deployed for aerial video capture in disaster response scenarios. They can provide aerial views of affected areas, identify hazards, and assess damage. Live video feeds from drones enable remote teams to plan and respond effectively.

User devices and endpoints play a pivotal role in accessing and contributing to video streaming during disaster response. The diversity of devices, from smartphones and tablets to computers, laptops, IoT surveillance cameras, wearable cameras, and drones, ensures that responders have a range of tools at their disposal for capturing, transmitting, and viewing live video. These devices enable remote coordination, situational awareness, and decision-making, enhancing the effectiveness of disaster response operations.

9. Security and Privacy [17]:

Encryption and Authentication:

Secure Transmission: Secure transmission involves the use of encryption protocols to protect video data during transit. Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) are common encryption mechanisms used to ensure that video streams are transmitted securely over the network. Encryption prevents eavesdropping and data tampering during transmission.

User Authentication: User authentication mechanisms ensure that only authorized individuals or devices have access to video streams. This can include password-based authentication, multi-factor authentication (MFA), or biometric authentication. Proper authentication controls help prevent unauthorized access to sensitive video content.

Privacy Concerns:

Protecting Sensitive Video Data: Disaster response video streams may capture sensitive or confidential information, such as personal identification, medical details, or sensitive locations. Implementing access controls, encryption, and data masking techniques helps protect this sensitive data from unauthorized access or exposure.

Compliance with Privacy Regulations: Video streaming systems must adhere to relevant privacy regulations and compliance standards, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). Compliance ensures that video content is handled in a manner that respects privacy rights and data protection laws.

Security and privacy considerations are paramount in disaster response video streaming. Ensuring the confidentiality, integrity, and availability of video content is crucial for maintaining trust and compliance with privacy regulations. Encryption and authentication mechanisms safeguard video transmission, while privacy controls protect sensitive data and ensure that video streaming practices align with legal and ethical standards. Effective security and privacy measures bolster the resilience of communication networks during disaster response efforts.

10. Content Delivery Strategies [10]:

Content Distribution Networks (CDNs):

CDN Selection and Optimization: Content Distribution Networks (CDNs) consist of distributed servers strategically placed across various geographical locations. CDNs are responsible for caching and delivering content to end-users efficiently. Disaster response teams must select appropriate CDNs based on factors like geographic coverage, performance, and reliability. Optimization involves configuring CDNs to ensure the best possible content delivery performance.

Edge Caching for Faster Delivery: CDNs employ edge caching, where content is cached at servers located at the network's edge, closer to end-users. This reduces latency and improves content delivery speed. Disaster response video streams benefit from edge caching, ensuring that critical information reaches users quickly, even in areas with limited infrastructure.

Peer-to-Peer (P2P) Distribution:

Leveraging P2P Networks for Distribution: Peer-to-Peer (P2P) distribution harnesses the collective resources of end-users to share and distribute video content. P2P networks can significantly reduce the load on central servers and improve scalability. Disaster response teams can leverage P2P distribution to ensure that video streaming remains responsive, even in situations with limited network bandwidth or infrastructure.

P2P Content Discovery Mechanisms: P2P content discovery mechanisms are essential for locating and accessing video streams within a P2P network. These mechanisms include distributed indexes, trackers, and discovery protocols that help users find and join relevant P2P video streams. Efficient content discovery ensures that responders and stakeholders can access the information they need in real-time.

Effective content delivery strategies are critical in disaster response scenarios where timely access to video streams can be a matter of life and death. CDNs and edge caching reduce latency and improve content delivery speed, while P2P distribution optimizes resource utilization and ensures responsiveness, even in challenging network conditions. Disaster response teams should carefully consider and implement these strategies to enhance the availability and reliability of video streaming for coordination and situational awareness.

11. Resource Allocation and Management [6]:

Resource Allocation Policies:

Prioritizing Video Traffic: Disaster response scenarios require the prioritization of video traffic to ensure that critical information reaches its destination without delay. Network policies can be established to prioritize video streaming traffic over other less time-sensitive data. This ensures that video streams maintain their quality and responsiveness even during peak network loads.

Resource Reservation for Disaster Response: Resource reservation involves allocating specific network resources, such as bandwidth and processing power, to support disaster response operations. This proactive approach ensures that sufficient resources are available for video streaming, data analysis, and communication, regardless of competing demands on the network.

Network Monitoring and Control:

Network Traffic Analysis: Network traffic analysis involves continuously monitoring the flow of data across the network. This helps in identifying patterns, bottlenecks, and potential issues that may affect video streaming quality and network performance. Real-time monitoring enables rapid responses to network anomalies.

Automated Resource Provisioning: Automated resource provisioning involves the use of intelligent systems to allocate and manage resources dynamically based on real-time network conditions and demands. Automated provisioning ensures that resources are allocated efficiently, maximizing the quality and availability of video streams during disaster response.

Resource allocation and management are essential components of disaster response video streaming. Prioritizing video traffic and reserving resources ensure that critical communication remains responsive and reliable, even in challenging network conditions. Network monitoring and automated resource provisioning enable adaptive responses to changing circumstances, guaranteeing that disaster response teams have the resources needed to maintain situational awareness and coordination.

12. Case Studies and Use Cases [1]:

Real-World Deployments:

Examples of Video Streaming in Disaster Response Scenarios: Real-world deployments provide specific examples of how video streaming technologies and strategies have been used in disaster response situations. These case studies showcase the practical application of video streaming in scenarios like natural disasters, public safety emergencies, and humanitarian crises. They may include details on the types of video equipment used, network infrastructure, and communication protocols employed.

Lessons Learned and Best Practice: Lessons learned from past deployments offer valuable insights into what worked well and what challenges were faced during disaster response. These lessons can inform best practices and guide the development of a framework for Resilient Communication Networks for Disaster Response (RCN-DRF). Documentation of best practices can help shape future disaster response strategies and technologies.

Real-world case studies and use cases are essential for understanding the practical applications of video streaming in disaster response. They provide tangible examples of how video streaming has been employed to enhance communication, coordination, and situational awareness in critical scenarios. Moreover, the lessons learned from these deployments can inform the ongoing development and improvement of a framework (RCN-DRF), ensuring that it remains adaptive and responsive to the evolving needs of disaster response teams and communities.

III. Discussion

The Disaster-Resilient Video Streaming Taxonomy (DR-ViST) introduced in this framework serves as a comprehensive guide for understanding the intricacies of video streaming in the context of disaster response. It is a tool designed to empower disaster response professionals,

Koffka Khan and Wayne Goodridge, "A Disaster-Resilient Video Streaming Taxonomy (DR-ViST)," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 6, Issue 4, pp. 84-91, 2023.

researchers, and technology developers to navigate the complex landscape of video streaming and leverage it effectively during critical times.

1. Holistic Approach to Disaster Response: DR-ViST recognizes the fundamental role that video streaming plays in modern disaster response efforts. It acknowledges that real-time video transmission is not merely a convenience but a necessity for ensuring timely decision-making, resource allocation, and coordination. By categorizing the various components of video streaming, from network infrastructure to security measures, DR-ViST enables a holistic approach to disaster response, where each element contributes to the overall resilience of the communication network.

2. Resilience as a Core Principle: One of the standout features of DR-ViST is its emphasis on resilience. In disaster scenarios, communication networks are often subjected to disruptions, making the ability to adapt and recover quickly a critical factor. Resilience strategies, including network redundancy, edge computing, and content replication, are integral components within the taxonomy. These strategies ensure that video streaming can continue to function even in challenging conditions, thereby enhancing the overall effectiveness of disaster response operations.

3. Technology Flexibility: The taxonomy recognizes the diverse range of technologies available for video streaming, from traditional wired networks to emerging wireless and peer-to-peer solutions. This flexibility allows disaster response teams to choose the most appropriate technology based on the specific context of the disaster. For example, satellite communication may be preferred in remote areas with limited infrastructure, while 4G or 5G networks may be more suitable in urban environments.

4. Quality and Security Considerations: DR-ViST highlights the importance of both quality of service (QoS) and security in disaster response video streaming. Ensuring high-quality video delivery, with adaptive bitrate streaming and quality monitoring, enhances the user experience and situational awareness. Simultaneously, robust security measures, including encryption and authentication, protect sensitive video data and prevent unauthorized access, particularly in scenarios where privacy and confidentiality are paramount.

5. Resource Management: Efficient resource allocation and management are crucial in disaster response. DR-ViST explores resource allocation policies and network monitoring mechanisms to ensure that video streaming does not strain already limited resources. Effective resource management helps maintain network stability and ensures that critical communication channels remain available for essential functions.

6. Real-World Insights: The inclusion of practical case studies within DR-ViST provides valuable insights into the challenges and successes of implementing video streaming in disaster response. These real-world examples illustrate how the taxonomy can be applied in different scenarios and serve as a source of inspiration for future deployments.

In conclusion, the Disaster-Resilient Video Streaming Taxonomy (DR-ViST) is a versatile and comprehensive framework that addresses the multifaceted challenges of video streaming in disaster response. By promoting a holistic, resilient, and flexible approach to video streaming, DR-ViST equips disaster response professionals with the tools and knowledge needed to harness the full potential of video communication in safeguarding lives and optimizing response efforts during times of crisis. As technology continues to evolve, DR-ViST will adapt and expand, ensuring that it remains a relevant and invaluable resource in the ever-changing landscape of disaster response.

IV. Conclusion

The Disaster-Resilient Video Streaming Taxonomy (DR-ViST) introduced in this framework is more than just a classification system; it is a roadmap to harnessing the power of video streaming in the most challenging and critical of circumstances—disaster response. In times of crisis, when communication is a lifeline, DR-ViST emerges as an invaluable tool that illuminates the path towards resilient, effective, and adaptable video streaming solutions. DR-ViST encapsulates the essence of disaster response by recognizing that video streaming is more than just a medium for transmitting data—it is a lifeline, a source of critical information, a bridge to remote collaboration, and a beacon of hope in the darkest hours. By dissecting the ecosystem of video streaming, DR-ViST offers clarity and structure to an otherwise complex landscape.

This taxonomy's emphasis on resilience stands as a testament to the need for adaptive systems capable of withstanding the harshest of conditions. Disaster scenarios bring unpredictability, but DR-ViST ensures that video streaming remains a reliable thread connecting responders, decision-makers, and communities. As the world evolves, so too will DR-ViST. Emerging technologies, innovative protocols, and evolving disaster response strategies will continue to shape the landscape of video streaming in disaster scenarios. DR-ViST is not a static framework but a living document, ready to adapt to new challenges and opportunities.

In essence, DR-ViST is a tribute to human ingenuity, resilience, and adaptability. It is a testament to the unyielding commitment of disaster response professionals, researchers, and technology developers to harness the power of video streaming for the greater good. As we navigate the complexities of disaster response in an ever-changing world, DR-ViST will remain a guiding light—a source of knowledge, inspiration, and innovation. It is a reminder that even in the face of adversity, we can leverage technology to connect, communicate, and ultimately, to save lives. In the spirit of resilience, innovation, and collaboration, let DR-ViST serve as a beacon of hope—a symbol of our unwavering commitment to building a safer, more connected world, one video stream at a time.

References

[1] Aggarwal, S., Kumar, N. and Tanwar, S., 2020. Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions. IEEE Internet of Things Journal, 8(7), pp.5416-5441.

[2] Al Qundus, J., Dabbour, K., Gupta, S., Meissonier, R. and Paschke, A., 2020. Wireless sensor network for AI-based flood disaster detection. Annals of Operations Research, pp.1-23.

[3] Alipour, M., Moghaddam, M.T., Vaidhyanathan, K., Kristensen, T. and Krogager Asmussen, N., 2023, July. Emotional Internet of Behaviors: A QoE-QoS Adjustment Mechanism. In International Conference on Human-Computer Interaction (pp. 3-22). Cham: Springer Nature Switzerland.

[4] Al-Khafajiy, M., Baker, T., Hussien, A. and Cotgrave, A., 2020. UAV and fog computing for IoE-based systems: A case study on environment disasters prediction and recovery plans. Unmanned Aerial Vehicles in Smart Cities, pp.133-152.

[5] Apostolakis, Konstantinos C., George Margetis, Constantine Stephanidis, Jean-Michel Duquerrois, Laurent Drouglazet, Arthur Lallet, Serge Delmas et al. "Cloud-native 5g infrastructure and network applications (netapps) for public protection and disaster relief: The 5g-epicentre project." In 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), pp. 235-240. IEEE, 2021.

[6] Chaudhuri, N. and Bose, I., 2020. Exploring the role of deep neural networks for post-disaster decision support. Decision Support Systems, 130, p.113234.

[7] Chou, S.F., Yu, C.Y. and Sou, S.I., 2023, April. Efficient Multi-UAV-Aided Communication Service Deployment in Disaster-Resilient Wireless Networks. In 2023 IEEE Vehicular Networking Conference (VNC) (pp. 1-8). IEEE.

[8] Ejaz, W., Azam, M.A., Saadat, S., Iqbal, F. and Hanan, A., 2019. Unmanned aerial vehicles enabled IoT platform for disaster management. Energies, 12(14), p.2706.

[9] Fleury, M., Kanellopoulos, D. and Qadri, N.N., 2019. Video streaming over MANETs: An overview of techniques. Multimedia Tools and Applications, 78, pp.23749-23782.

[10] Jiang, D., Wang, F., Lv, Z., Mumtaz, S., Al-Rubaye, S., Tsourdos, A. and Dobre, O., 2021. QoE-aware efficient content distribution scheme for satellite-terrestrial networks. IEEE Transactions on Mobile Computing, 22(1), pp.443-458.

[11] Khan, K. and Goodridge, W., 2017. SAND and Cloud-based Strategies for Adaptive Video Streaming. International Journal of Advanced Networking and Applications, 9(3), pp.3400-3410.

[12] Khan, K. and Goodridge, W., 2018. Future DASH applications: A survey. International Journal of Advanced Networking and Applications, 10(2), pp.3758-3764.

[13] Khan, K. and Goodridge, W., 2020. QoE evaluation of dynamic adaptive streaming over HTTP (DASH) with promising transport layer protocols: Transport layer protocol performance over HTTP/2 DASH. CCF Transactions on Networking, 3(3-4), pp.245-260.

[14] Khan, K. and Goodridge, W., Markov Decision Processes for bitrate harmony in adaptive video streaming. In 2017 Future Technologies Conference (FTC), Vancouver, Canada, unpublished..

[15] Koffka, K. and Wayne, G., 2018. A DASH Survey: the ON-OFF Traffic Problem and Contemporary Solutions. Computer Sciences and Telecommunications, (1), pp.3-20.

[16] Pi, Y., Nath, N.D. and Behzadan, A.H., 2020. Convolutional neural networks for object detection in aerial imagery for disaster response and recovery. Advanced Engineering Informatics, 43, p.101009.

[17] Rizi, M.H.P. and Seno, S.A.H., 2022. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, p.100584.

[18] Wu, Y. and Chen, S., 2023. Resilience modeling and pre-hazard mitigation planning of transportation network to support post-earthquake emergency medical response. Reliability Engineering & System Safety, 230, p.108918.