Mobile and Wireless Networks

Visible Light Communication Protocol Security

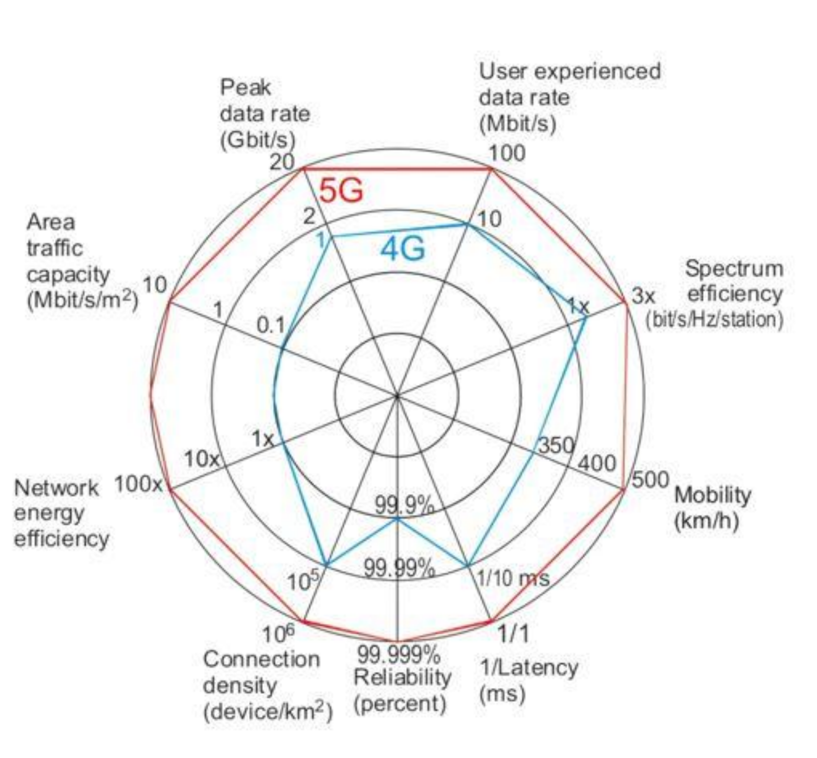
Andriamahefa RAMIARAMANANA
Zlatan KOVACEVIC
Semilogo OLUSOLA OGUNGBURE

Visible Light Communication Protocol Security

Table of Contents

Visible Light Communication Protocol Security

- **Introduction**
  - Visible light communications System (VLC)
  - 5G and Internet of Things (IoT)
  - Modulation and networking algorithms
  - Physical layer
- Is VLC Really Necessary for IoT Networks Deployment?
- Existing and Proposed Multiple Access Technique in VLC-IoT



Visible Light Communication Protocol Security

- **Existing and Proposed Multiple Access Technique in VLC-IoT**
  - **OFDMA:** bandwidth allocation scheme for high data rate communication and reduced mutual interference
  - **CDMA:** multiple VLC-IoT devices to transmit simultaneously in a shared time slot, mitigating multipath interference challenges
  - **SDMA:** enables multiple VLC-IoT devices to share frequency-time resources by exploiting spatial diversity.

- **Proposed Multiple Access Technique in VLC-IoT**
  - **OFDMA)-based VLCP**: creating frequency holes by deploying idle positioning subcarriers and then filling the frequency holes with positioning signals that are immune to OOBI from OFDM signals to achieve better positioning accuracy and bandwidth utilization performance

  - **(FBMC)-based:** leakage of each subcarrier in communication, reducing the negative impacts of OOBI. The FBMC-based approach also improves spectral efficiency, maximizes the utilization of subcarriers, and enhances the positioning accuracy of VLCP systems.

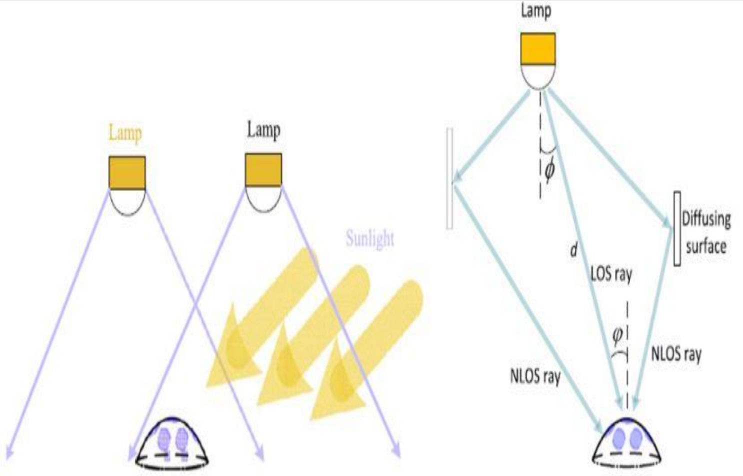
Visible Light Communication Protocol Security

- **Handover**

Existing Handover Mechanisms in VLC-IoT

Horizontal Handover: A handover mechanism commonly executed in mobile VLC-IoT devices to maintain seamless connectivity and prevent inter-cell interference.

Vertical Handover : A type of handover mechanism that occurs between different access layers in VLC-IoT systems,triggered when there is a line-of-sight (LOS) blockage.



Proposed Handover Approach

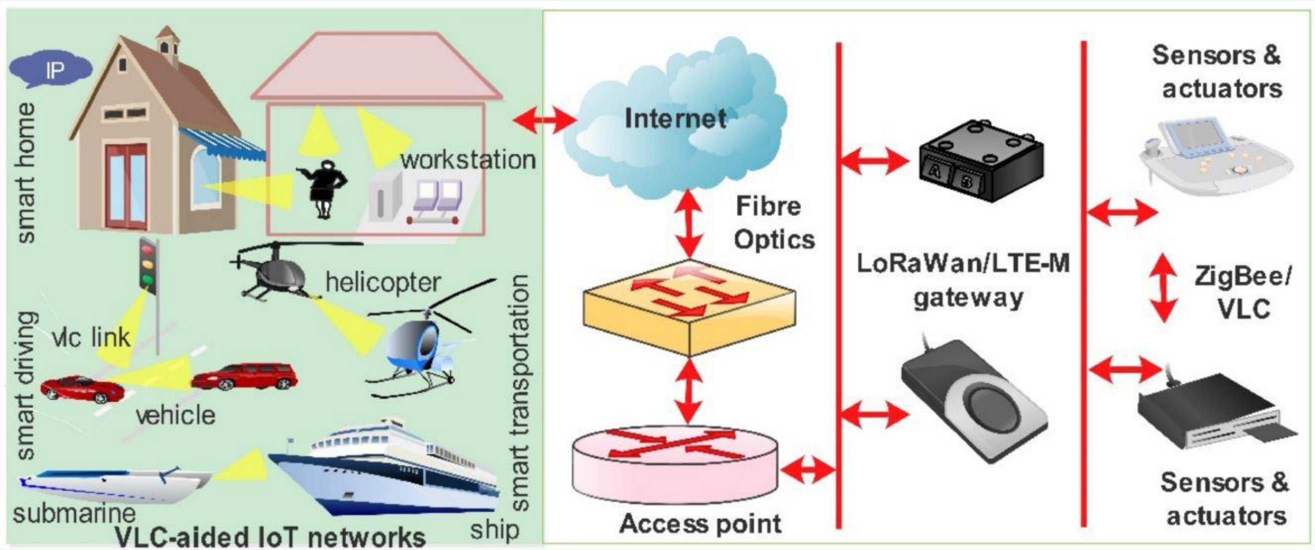
RSI-VH: is based on the received signal intensity of the APs at VLC-IoT devices. A handover is triggered when a neighbouring AP has a higher RSI value than the current AP.

Non-LOS-based VH: reduces frequent handovers in VLC-IoT systems. When a VLC-IoT device detects a LOS blockage, it waits for a set time (dwell period) before handover to a neighbouring AP with better channel resources

- Friendly Jamming/Zero-Forcing

Visible Light Communication Protocol Security

- **VLC Architecture**
  involves a central network utilizing VLC technology, connected to a network of sensors, actuators, and Access Points (APs) that communicate with VLC-IoT devices through various communication technologies.



Visible Light Communication Protocol Security

- Physical Layer Security
  - PLS Embedded Encryption: Inherent security, Cryptography for physical and data link layer
    cipher cleartext data
    key management, key generation, distribution and verification using AES parallel-to-serial rule
    private key & Public Key

- Chaos-based Physical layer security model
  encrypting the packer frame
  - random bits of data to the payload
  - Sensitive to internal parameters
  - signal-generating chaos oscillators and Parameters
  - computational delay & two synchronized oscillators
  - Active-Passive Decomposition
  - physical layer header & MAC frame
  - Frame Check Sequence and Header Check Sequence

$$S(t) = h_{enc}(t) + p_{pad}(t)$$

$$h_{enc(t)} = V_{BE1}(t)$$

$$h' = V_{BE2}(t) - V_{BE1}(t)$$

Visible Light Communication Protocol Security

- **Friendly Jamming/Zero-Forcing**
  - adds an additional transmitter (jammer) different from the main VLS transmitte
  - eavesdropper's CSI
  -
- **DRL-Based IRS-Assisted**
  - mirror array sheets
  - Intelligent Reflecting Surfaces (IRS)
  - high dimensionality
  - maximize SNR
  - deep reinforcement learning model
  - eavesdropper in proximity

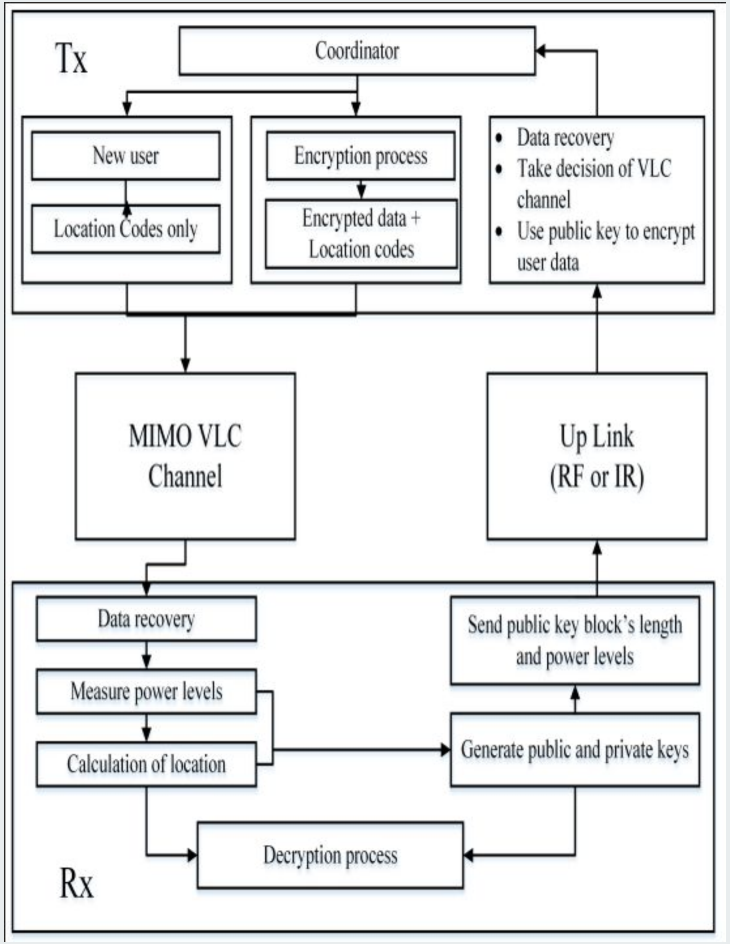
- **Data Link Layer Security**
  - MAC sublayer
  - Cryptography computational resources and power consumption
  - symmetric cryptography
  - higher layer process
  - AES in CBC-MAC mode/ Zigbee
  - MAC dead fields
  - key management and generation

Visible Light Communication Protocol Security

- **Elliptic Curve Cryptography**
  - mathematical nature of elliptic curves , encryption and digital signatures RSA, ECC
  - IoT environments and VLC
  - dedicated arithmetic module
  - shorter key lengths and lower complexity

- **Chaffing and Winnowing**
  - Message Authentication Codes
  - encryption and decryption
  - identification number to block of message
  - Chaffs, fake MAC and winnowing

- **VLC Attacks & Vulnerabilities**
  - secure VLC communications
  - setup and private data
  - Denial-of-Service, friendly jamming
  - VLC beam



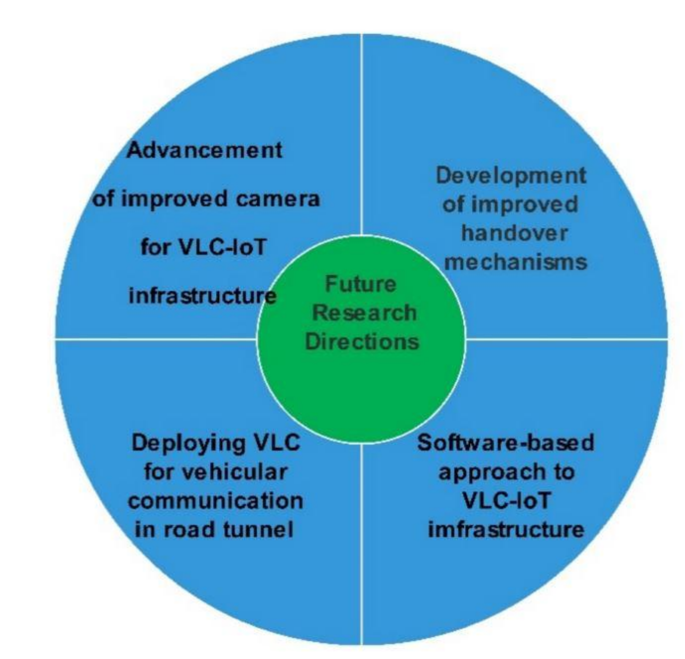
Visible Light Communication Protocol Security

Challenges, Solutions & Opportunities in VLC-IoT

VLC-IoT		
S/N	Challenge	Solution
1.	Limited modulation bandwidth of off-the-shelf LEDs	The use of MIMO advanced modulation and multiple access schemes; 2.The use of smart LEDs
2.	Extended link distance in outdoor VLC-IoT applications	1. Using relays to extend the transmission range of VLC-IoT applications; 2. Deploying LEDs-camera VLC for extended range of transmission; 3.Development of hybrid OFDM and CDMA resources allocation algorithms
3.	LOS signal loss and shadowing effects	1. Using high spatial diversity to guarantee connections; 2. Using MIMO antennas to reduce the risk of LOS signal loss due to interrupted signals; 3. Using a transmitter with ultra-wide FOVs to eliminate loss signals.
4.	Lack of recognized channel models for VLC-IoT channel models for VLC-IoT communications	1. Study characteristics and theoretical details of indoor and outdoor VLC;2. Validate identify channel model in different transmission medium for possible

Visible Light Communication Protocol Security

- **Future opportunities for exploration in VLC-IoT**
  - **Research on Improved Handover Techniques**
  - Advanced Receiver Camera Development.
    - Optical communication image sensor, communication bit rate.
  - Deploying VLC for vehicular communications in road tunnels.
    - Potential substitute for traditional RF.
    - Vehicular communications,
    - Confined locations,
    - Highest data rates,
    - Length of the link,
    - Impact on the VLC channel in tunnel
  - Software-based approach to VLC-IoT infrastructure.
    - Hardware remote control,
    - Local control decisions,
    - Infrastructure-less VLC system



Visible Light Communication Protocol Security

- # Challenges and Opportunities for VLC
  - The limited range and area coverage of VLC.
  - Reliance on LOS,
  - Interference from other sources,
  - Significant research and development efforts,
  - Advanced modulation and coding techniques,
  - Optical component development,
  - Hybrid communication systems.
  - Development of high-data-rate systems
  - competitive alternative, integrating with other, Wi-Fi, cellular, Bluetooth

Conclusion

Our research delved into the complexities of this fascinating technology in this academic analysis of visible light communications, looking at its underlying ideas, various uses, cutting-edge multiple access methods, enduring difficulties, and the crucial role of physical layer security. As indicated by its integration with cutting-edge technologies, the expansion of high-speed data systems, and the booming acceptance in both the industrial and consumer spheres, VLC is ready to spark a revolution in wireless communication with its enormous potential.

To overcome the challenges that VLC faces and reach its full potential, research and development must continue without ceasing. The scientific community is being challenged to harness VLC's power and release its transformative potential in response to this call to action. VLC's future is promising and realistic.