Crowd Monitoring and City Sensing Techniques Supported by Next Generation Mobile Networks

Riccardo Rusca

In an era of rapid technological advancement and global challenges, the paradigm of overseeing crowds, ensuring safety, and safeguarding privacy undergoes profound transformation. The COVID-19 pandemic has prompted us to reconsider how we manage large gatherings while respecting personal freedoms and privacy. As we transition beyond the pandemic, it is crucial to strike a balance between enhancing safety measures at events and safeguarding privacy rights.

Traditional crowd surveillance methods often struggle to capture the nuanced dynamics of crowd behavior and movement patterns. With ongoing health concerns, there is a growing need for advanced monitoring systems that provide timely insights and allow for proactive measures. Additionally, the advent of smart cities and new technologies like V2X communication and artificial intelligence presents ethical, legal, and technical challenges, particularly regarding personal data protection. Regulatory efforts like the General Data Protection Regulation (GDPR) [**?**] aim to address these challenges by establishing clear guidelines for data security and the responsible use of personal information in monitoring initiatives.

This thesis dives deep the intersection of crowd monitoring, public safety, data privacy, and machine learning, accentuated by the challenges and implications ushered in by the post-COVID-19 landscape. A crucial investigation into the complexities of 802.11 Probe Request messages and MAC address randomization unveils nuanced behavioral patterns and privacy concerns, notably concerning MAC addresses. Leveraging this understanding, innovative methodologies are devised to replicate authentic device behaviors, facilitating the generation of realistic data traces able to boost the development of machine learning algorithms for improved people counting, all while reinforcing user privacy through specialized data structures and sophisticated anonymization methods.

As we advance into an era where artificial intelligence and data privacy take center stage, this thesis delves into the transformative concept of federated learning. Embracing the privacy-centric design inherent in federated learning—where clients independently train machine learning models and share only model's parameters

over the network—this ensure robust data protection while also optimizing training efficiency and accelerating convergence rates. Within the realm of vehicular applications, this research shows how federated learning can harness collective intelligence to fine-tune trajectory prediction models. This approach not only delivers scalability and responsiveness but also fortifies privacy safeguards, showcasing the potential of collaborative methodologies in enhancing urban mobility solutions.

This collaborative spirit extends to the development of a innovative data-driven framework tailored for Radio Frequency (RF) mobility scenario generation. By integrating real-world mobility traces with advanced channel modeling techniques, this framework establishes a robust foundation for crafting realistic V2X scenarios for channel emulators, fostering innovation in urban mobility solutions.

As technological advancements continue to reshape our world, striking a harmonious balance between public safety, crowd monitoring, and data privacy remains paramount. This research underscores the significance of adapting innovative methodologies and collaborative approaches, such as artificial intelligence, machine learning, federated learning and advanced RF mobility scenario frameworks, to navigate the complexities of modern urban environments effectively. By prioritizing both safety and privacy, we lay the groundwork for more resilient, secure, and inclusive communities, ensuring that technological progress aligns with the values and rights of individuals.