David Falana

Plainfield, NJ

Su20-031

Sophomore
Electrical Engineering
Rutgers University

Faculty Mentors: Dr. Prasad Calyam, Electrical Engineering & Computer Science; Dr. Khaza Hoque, Electrical Engineering & Computer Science

Funding Source: NSF REU in Consumer Networking Technologies

Attack-Defense and Performance Adaptations for Social Virtual Reality Learning Environments

David Falana, Micheal Fisher, Vaibhav Akashe, Samaikya Valluripally, Khaza Anuarul Hoque, and Prasad Calyam

Social virtual reality learning environment (VRLE) allows one to be virtually present in an immersive manner and increases accessibility to remote learning. VRLE applications in critical domains (e.g. military training, education) demands continuous data delivery along with user immersiveness. Lack of maintaining robustness and high performance in such socio-technical systems, leads to disruption of user safety (e.g inducing cybersickness) and application functionality (e.g. content delivery issue). In this paper, we present a novel adaptive framework that jointly tunes performance and robustness factors using a `DevSecOps' paradigm for a social VRLE. Using a VRLE application case study viz., vSocial we characterize the robustness factors as {Security, Privacy, Safety (SPS)} and performance factors {Quality of Application, Quality of Service, Quality of Experience (3Q)}. For this, we develop an *anomaly-monitoring tool* in our framework to collect and classify anomaly data. Next, we utilize a *decision module* that relies on dynamic decision making for suitable adaptations using quantifiable metrics (e.g. *Suitability, Cost*). To facilitate an adaptive control loop mechanism in our framework, we model a priority queue, to determine the state of VRLE; reduce waiting delays and incorporate adaptations related to severe SPS/3Q anomalies before cybersickness is induced. Based on our experimental results, we enlist best practices to implement for several simulated SPS/3Q anomaly events in vSocial. Our results also detail the benefits of our proposed adaptive control loop framework by performing trade-off analysis of our priority queue model with state-of-the-art approaches, in terms of performance overhead and usability metrics (Response time, Cybersickness). Lastly, we show the effectiveness of our framework for several SPS/3Q scenarios and illustrate the impact of the incorporated adaptations on cost, cybersickness metrics. Based on our results, we demonstrate how our proposed framework takes decisions about the adaptations dynamically to develop a more secure and safer operational social VRLE.