UNIVERSITY OF MISSOURI UNDERGRADUATE RESEARCH IN CONSUMER NETWORKING TECHNOLOGIES

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

Samaikya Valluripally[a], Vaibhav Akashe[a], David Falana[b], Michael Fisher[c], Prof. Khaza Anuarul Hope[a], Prof. Prasad Calyam[a]

University of Missouri-Columbia[a], Rutgers University[b], Columbia College[c]

INTRODUCTION

- Social Virtual Reality Learning Environments are online 3D spaces designed to enhance learning capabilities of the students.
- Lack of handling performance and robustness factors can cause a disruption of user's learning experience by inducing cybersickness.
- Need to explore the inter-relationship between performance (i.e. *Quality of Application, Quality of Service and Quality of Experience* : **3Q)** and robustness factors (i.e. *Security, Privacy and Safety:* **SPS**) factors.
- **Our Contributions: (i)** Conduct a detailed analysis for quantification of cybersickness based on simulated SPS/3Q scenarios. **(ii)** propose a novel model-driven based adaptative framework, to determine the suitable attack-defense or performance adaptation. **(iii)** we evaluate our adaptive framework effectiveness and the model behavior using a VRLE application case study viz., vSocial.

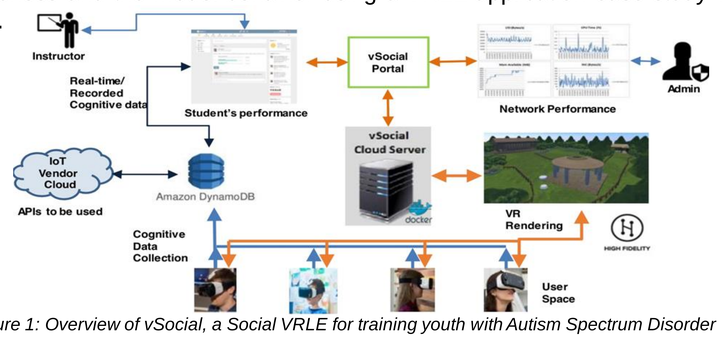

Figure 1: Overview of vSocial, a Social VRLE for training youth with Autism Spectrum Disorder

MODELING AS A FINITE PRIORITY-BASED QUEUING SYSTEM

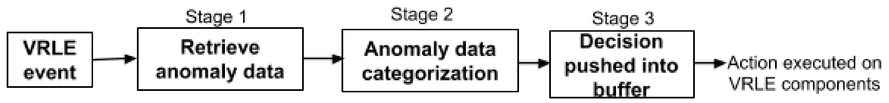

Figure 2: Modelling stages of our proposed control-loop adaptive framework as a queue

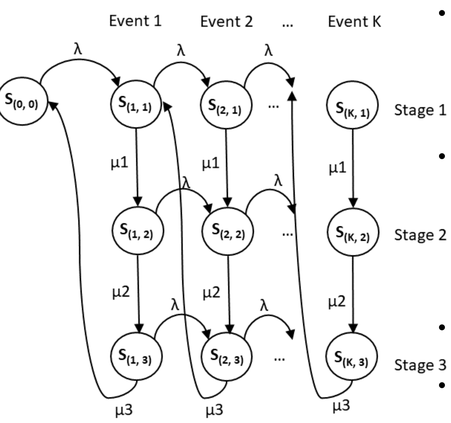

Figure 3: Markov chain with processing of three stages related to our control loop adaptive framework

- To monitor the overall system response time and perform the adaptations for SPS/3Q anomaly events, we model the stages of our adaptive framework as a priority based finite queuing (M/M/1) model.
- We formulate the arrival times (λ) and processing rate (μ) of the events to get the wait time (W_T) in the system and response time (R_T) of mitigating the anomaly events in the system.
- $W_T = W_q + (1/\mu)$, where W_q is the wait time of the queue.
- $W_q = (L_q) / \lambda$, where L_q is the number of events in the queue.
- $R_T = R_q +$ Adaptation time, where R_q is the response time of the events in the queue

MODEL-DRIVEN ADAPTIVE FRAMEWORK

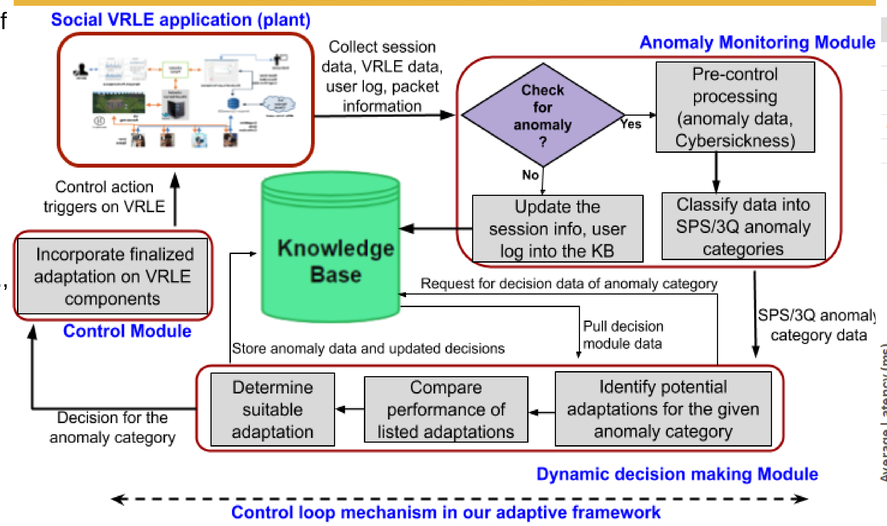

Figure 4: Control Loop Adaptive Framework for social VRLE to tune performance and security jointly

Using our proposed model-driven adaptive framework, we implement the real-time adaptations to mitigate cybersickness in social VRLEs.

- VRLE (user data, session info) and network data are collected to determine any issues related to SPS (i.e. Denial of Service (DoS) attack, Unauthorized access) and 3Q (i.e. visualization delay, packet drop) using our monitoring tool.
- Quantify Cybersickness (i.e. latency metric) for each identified anomaly category (DoS, visualization delay, time lag) and send to the decision module.

$$(W) = \left[\frac{F(A,B)}{L(S)}\right] * C$$

- To determine the suitable adaptation, we compute a weighted function (W) using the decision metrics i.e. Cost (C) is the total amount of resources required, L(S) represents the likelihood of success rate, F(A,B) is the cartesian product of resource usage (A) and run time of the adapt

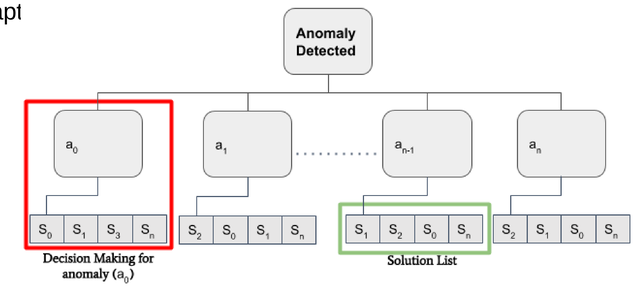

Figure 5: Decision making mechanism of the incoming anomaly events based on solution list

The control module will incorporate the suitable adaptation recommended by our dynamic decision-making algorithm and will update the results into the knowledge base module (KB).

EVALUATION RESULTS

Anomalies Detected

Type	Time	Source	Destination	Protocol	Length	Info
SPS	557.369417	128.206.20.46	128.206.20.43	UDP	92	58222 > 62054 Len=50
SPS	421.962237	128.206.20.43	128.206.20.46	UDP	89	40102 > 58222 Len=47
SPS	553.712925	128.206.20.46	128.206.20.43	UDP	90	58222 > 62054 Len=48
SPS	113.666930	128.206.20.46	128.206.20.43	UDP	78	58222 > 62054 Len=36
SPS	421.248308	128.206.20.43	128.206.20.46	UDP	83	62058 > 58222 Len=41
QoA	82.558665	3.20.240.238	192.168.10.68	UDP	128	48001 > 52766 Len=86
SPS	223.134959	128.206.20.46	128.206.20.43	UDP	90	58222 > 62054 Len=48
SPS	556.242194	128.206.20.46	128.206.20.43	UDP	92	58222 > 62054 Len=50

Figure 6: Detected Anomaly events in Social VRLE using our anomaly monitoring tool

Model Considered	Response Time of events in the queue for 20 simulations (in seconds)	% of the no. of events in the queue that with decision on suitable adaptation
First in First Out (FIFO)	5.24	50.07%
Linear Priority Queue (LPQ)	5.32	35.08%
Binary Heap Priority Queue (BHPQ)	4.54	34.88%

Figure 8:Performance analysis of our priority queue modeling (BHPQ) with state-of-the-art approaches (LPQ, FIFO)

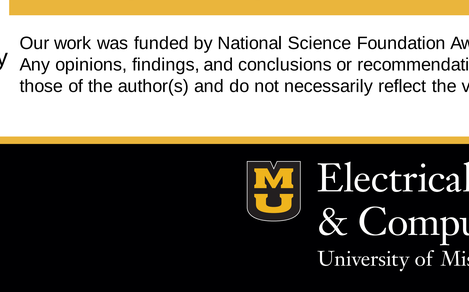

Figure 7:CS mitigation based on the incorporation of best adaptations (A1) and (A2)

Adaptation	L(D) for anomaly event=QoS	Impact (change in CS)	Risk Level
A1 (Upgrading instance)	0.75	26.43%	**Medium** (next best solution for QoS)
A2 (scaling of resources)	0.60	13.47%	**Near to high** due to the high cost, resource usage and the low impact on CS
A3 (Enhanced network)	0.89	30.28%	**Low** due to the cost, time and also the huge impact on CS reduction
A4 (SPS guard duty)	0.80	N/A	**Risk** in terms of cost can be **high**, because it is self monitored and mitigates using by AWS autonomy

Figure 9: Risk Analysis approach for a QoS anomaly vs different adaptation decisions

Key Findings:

- Determined cybersickness occurrence can be quantified using certain QoS (packet loss), QoA (visualization delay) metrics from our simulation experiments in vSocial.
- Compare the performance of our queuing model with the state-of-the-art approaches in terms of overhead in addressing the events with high CS.
- We perform trade-off analysis of our framework for the decision making of the adaptation in terms of different threshold metrics, system response time, resource usage and cost metric..

CONCLUSION

- Proposed a novel model-driven adaptive framework to address the performance and security issues that induces cybersickness in a social VRLE application.

In the future, we plan to expand our framework to make active decision making for zero-day anomaly events.

ACKNOWLEDGEMENTS

Our work was funded by National Science Foundation Awards: CNS-1647213 and CNS-1950873. Any opinions, findings, and conclusions or recommendations expressed in this publications are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.