GRAPH-BASED SIMULATION OF EMERGENCY SERVICES COMMUNICATIONS SYSTEMS

Jardi Martinez Jordan,[*] Victoria Salvatore,[*] Barbara Endicott-Popovsky,[†] Vivek Gandhi,[*]
Christopher O'Keefe,[*] M. Scott Sotebeer,[‡] and Michael Stiber[*]

[*]Computing & Software Systems Division, School of STEM,
University of Washington, Bothell, WA, USA, stiber@uw.edu, jardiamj@uw.edu
[†]Portland State University, endic@pdx.edu
[‡]USA Strategics, scott@usastrategics.com

ABSTRACT

Although fragile under extreme circumstances, Emergency Services Communication Systems (ESCS) – such as 9-1-1 in the US – are a critical part of emergency response and disaster preparedness systems. We are developing a first-of-its kind, graph-based, generalized framework for large-scale simulations of ESCS-like systems, including a detailed model of Next Generation 911 (NG911).

Keywords: graph-based simulation, emergency services communications, GPU computing, cybersecurity.

1 SIMULATION OF EMERGENCY SERVICES COMMUNICATIONS SYSTEMS

We define Emergency Services Communications Systems (ESCS) as the aggregate of organizational, electronic, and virtual entities that take part in answering emergency calls and responding to emergency events, along with their policies and procedures. In the US, this is colloquially known as the 9-1-1 system and is the basis for this work. Originally implemented in 1968, the 9-1-1 system organically evolved into a system of systems dependent on dated technology that now requires a paradigm change to take advantage of modern technology; said change comes in the form of the nationwide Next Generation 911 (NG911) project. On the road to implementing NG911, individual states have the responsibility for deciding the specifics of a set of network elements, software applications, databases, and operations and management procedures. The FCC has provided recommendations on actions that can be taken to optimize cybersecurity, operations, and funding; but in the end, the actionable decisions will depend on the circumstances, priorities, and knowledge of a given PSAP (Task Force on Optimal PSAP Architecture (TFOPA) 2016).

ESCS simulations have potential uses in cybersecurity, crisis preparedness, and strategic and operational decisions. Guri *et al.* (Mirsky and Guri 2021) and Xue and Roy (Xue and Roy 2021) separately developed purpose-written simulations to explore ESCS performance and susceptibility to distributed denial of service (DDoS) attacks; the former found that fewer than 6K bots could block emergency services in an entire state for days. In crisis preparedness, simulations could be leveraged to identify critical sub-networks, mitigation actions, and weaknesses in case of a catastrophic event. Another example is a common issue amongst 911 implementation that was most evident during the September 11 attacks: interoperability. Simulations could be used to explore response times, load distribution, and time intervals at various levels of interoperability.

Rather than implementing one-off simulators, we are developing a first-of-its kind, generalized framework for easily implementing models targeting specific research questions. We are developing this by re-

architecting a special-purpose, high-performance neural network simulator, BrainGrid (Stiber, Kawasaki, Davis, Asuncion, Lee, and Boyer 2017), into a general-purpose simulator for graph-based systems, Graphitti (O'Keefe, Salvatore, Stiber, Dukart, and Presland 2021).

ESCS is an example of a large class of systems that are naturally modeled with graphs; Graphitti is designed to simulate hybrid discrete/continuous graph-based systems and facilitate the migration and validation of large-scale (tens of thousands of vertices, millions of edges) and long-duration (billions of time steps) simulations to GPUs. We have already demonstrated use of Graphitti in simulations of development and tuning in biological neural networks at that scale (achieving a roughly 70x speedup, GPU vs. CPU) and in an initial adaptation to a simple ESCS model. Associated with Graphitti is its Workbench, which helps researchers understand the interactions among mathematical models, algorithms, software implementation, simulation configuration, and results by tracking software and data provenance (Conquest and Stiber 2021). Other simulators that might be adapted exist, but this is the only one that we know of being used for this purpose.

We are modeling ESCS as a graph $G = (V,E)$ of their physical and virtual elements. We identified the following types of vertices: 1. Caller Region, 2. Public Safety Answering Point (PSAP), 3. Emergency Responder, and 4. Selective Router (SR)/IP Selective Routing(IPSR). Linking said vertices are communication-based edges, embodied in the physical and virtual network connections between devices and software elements. While communication is at the center of an ESCS, geographical boundaries and location are the basis for call routing and dispatching emergency responders. PSAPs and Emergency Responders are responsible for events originating within their boundaries but depending on saturation and assets availability, calls might be routed to an alternate PSAP or a neighboring Responder could be dispatched. Essential to ESCS are emergency events that generate messages, with spatiotemporal patterns, that are communicated through the network connections. These type of discrete-event systems are well modeled using a Finite State Machine (FSM) where the vertices state transitions will be driven by events such as call initiated, call answered, unit dispatched, unit arrival at scene, call end, end of emergency response, etc.

Our current focus is on detailed modeling of ESCS components to build a simulation of NG911, first during routine operation, then under a crisis situation. One major goal is to apply machine learning and data analytic tools to understand data patterns within the operation of ESCS. Future work concerns modeling very large-scale systems, mobile devices, Internet of Things (IoT), and distributed attackers. We also plan to investigate incorporating physical devices to evaluate hybrid scenarios of individual devices, or small network of actual hardware, operating within the context of large, complex simulated networks.

REFERENCES

Conquest, J., and M. Stiber. 2021, September. "Software and Data Provenance as a Basis for eScience Workflow". In *IEEE eScience*. online, IEEE.

Mirsky, Y., and M. Guri. 2021. "DDoS Attacks on 9-1-1 Emergency Services". *IEEE Transactions on Dependable and Secure Computing* vol. 18 (6), pp. 2767–2786.

Christopher O'Keefe and Tori Salvatore and Michael Stiber and Kyle Dukart and Lizzy Presland 2021, April. "UWB-Biocomputing/Graphitti: Dangerous Scribbles".

Stiber, M., F. Kawasaki, D. Davis, H. Asuncion, J. Lee, and D. Boyer. 2017, May. "BrainGrid+Workbench: High-Performance/High-Quality Neural Simulation". In *Proc. International Joint Conference on Neural Networks*. Anchorage, Alaska.

Task Force on Optimal PSAP Architecture (TFOPA) 2016, January. "Adopted Final Report". Technical Report DA-16-179, Federal Communications Commission.

Mengran Xue and Sandip Roy 2021. "Cyber-Physical Queueing-Network Model for Risk Management in Next-Generation Emergency Response Systems".