Poster: Qualia Exploitation of Sensing Technology (QuEST) for Vehicular Network Optimization

Teresa Hawkes*, Trevor J. Bihl†, Steven K. Rogers‡
* Department of Psychology, University of Oklahoma, Norman, OK, USA
†Department of Operational Sciences, Air Force Institute of Technology, Wright Patterson AFB, OH, USA
‡Sensors Directorate, Air Force Research Laboratory, Wright Patterson AFB, OH, USA
teresa.hawkes@gmail.com

***Abstract*—Qualia-based Exploitation of Sensing Technology (QuEST) is a dual process framework that leverages what is known about human neurophysiological and neuropsychological processes to create an artificial cognitive exoskeleton functioning similarly to the human mind. In this paper, we present a quick QuEST overview and a visionary approach using QuEST methods that can improve cognitive V2V network resistance to hacking. QuEST tenets and designs have been used successfully in cyber security, facial recognition, and cancer detection; thus V2V information security in the open internet context can be enhanced via QuEST. Of note, QuEST's focus is on intelligence amplification (IA) versus artificial intelligence (AI) and developing a machine architecture which closes the loop between human and machine.**

Keywords—cognition, information fusion, intelligence amplification, security.

I. Introduction

ACCURATE and timely exploitation and dissemination of relevant sensor, semantic, statistical, and graphic information is critical to secure internet of things (IoT) functionality. IoT has been extended to vehicular network (VN) systems, which aim to improve transportation efficiency via information sharing between vehicles. Unfortunately, IoT devices can be exploited by hacker organizations to perpetrate denial of service and other attacks on internet nodes [1], websites and databases. Thus, security in VN systems is of concern and a currently open research area [2], [3]. To combat this problem, development of an intelligence amplification (IA) guardian between VN networks and the open internet is recommended. Data transfer can best be guarded in a robust manner if a dual systems representational approach is used. This permits quick reflexive responses to expected information transfers and more deliberative 'conscious' responses to unexpected or bogus directives to VN systems. This dual process system resembles the way the human brain handles incoming information and thus facilitates trust. The human brain is composed of circuit nodes called microcircuits that are specialized for processing down-sampled sensory data into perceptions (qualia) which are then associated into whole brain-spanning networks composed of compound-qualia from which contextual meaning is calculated and appropriate actions generated [4], [5], [6]. V2V networks could be organized into specialized processing nodes including: public safety, traffic congestion, and car-to-car data, as well as VN node and agent interactions with the open internet. This will provide the context for hacker signal identification and isolation.

II. QuEST

The human brain down-samples from a high dimensional visual, auditory, and memory information space as a matter of course. Just so, intelligence amplification machines (IAMs) must down-sample from a high dimensional data space, whether we are talking about information flowing between VN vehicle agents, nodes, and networks or the IoT. Since it is impossible to anticipate all possible hacking events relevant to successful VN security, information management and routing, new approaches are necessary to permit secure and effective VN operations in the IoT context.

To meet this need we propose utilizing a relatively new approach: Qualia-based Exploitation of Sensing Technology (QuEST). The overarching goal of QuEST is to design an IAM [7], [8] that can effectively partner with human operators (facilitating tight coupling between human and machine). QuEST is composed of three key modules: 1) agents (sense and act upon an environment), 2) qualia (agent-experienced data and constructs derived from sensed data), and 3) a dual-process framework that posits two qualitatively different yet related processing modes (see Figure 1).

A. Recent QuEST-based Implementations

QuEST concept implementations have been instantiated in various applications, including Breast Cancer detection [9], cyber [10], and facial recognition [11]. In these problems, algorithms were employed to consider features in a general-to-specific sense, e.g. shape, texture, spatial, spectral, and interest points, in a fusion hierarchy. Each algorithm was first considered as a QuEST agent; agents were connected through various links with such connections used to extract context [11]. Agent internal representation was improved through adaptive feedback with methods termed "adaptive gallery" and "multi-look" [11]. Adaptive gallery architecture changed library dimensionality by removing low scoring matches, multi-look considered alternating library images if and when new information became available.

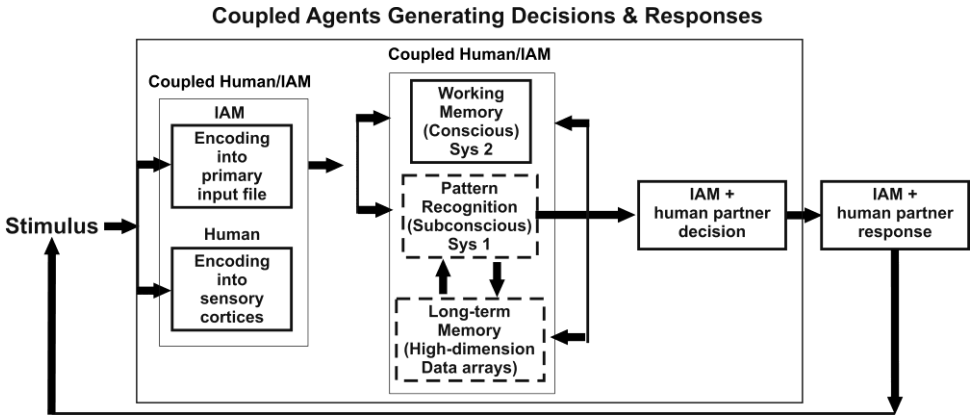

Fig. 1 – Coupled Agents Processing Model [7], [12].

III. Proposed QuEST-based IAM System

The human-machine partnership is key to solving any unexpected, anomalous, or ambiguous information presentations to the IAM system. Humans are optimized to make inferences in cases of ambiguity or unexpected queries [13] [14]. Thus, an effective QuEST-based coupled IAM guardian/human system will fuse information from various sources including the open internet, the human's experiences, and devices within their network, then determine if incoming information is 'normal' or a part of hacking operations. So, a QuEST-based IAM system captures various categories of data available to human and machine, shares information and knowledge from this data, then appropriately applies relevant knowledge to infer if an anomalous command or event is hacker-based. These inferences can then be fed back to the IAM/human system for testing and learning.

A. Novel 'Mirror' Algorithm

This novel approach to IAM architecture leverages knowledge of human mirror neuron assemblies which allow humans to understand, imitate, and improve on the actions of others [15]. Thus, we propose a novel mirror algorithm capable of writing into the guardian IAM agent working memory (see Figure 1) information from V2V networks as well as IoT information. Then the IAM guardian agent can interact with that representation as a basis for comparison between what it knows about what has occurred in the past to what is incoming.

IV. Conclusions

A visionary concept of QuEST as an approach to protecting VNs from IoT hackers was presented. This is but one possible approach of a QuEST methodology for VN use. QuEST involves modeling human mental processes in a computational framework to aid in IA machine design. QuEST design for an IAM partnered with a human can protect VNs from IoT hackers, and aid in vehicle and fleet operation.

References

[1] D. Sanger and N. Perlroth, "A New Era of Internet Attacks Powered by Everyday Devices," *New York Times,* 22 Oct. 2016.

[2] F. Dressler, F. Kargl, J. Ott, O. Tonguz, and L. Wischhof., "Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl Seminar," *IEEE Commun. Mag.,* 49(5), pp. 158-164, 2011.

[3] F. Da Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. Loureiro "Data communication in VANETs: a survey, challenges and applications," *INRIA Saclay*, 2014.

[4] L. Carillo-Reid, F. Tecuapetla, D. Tapia, A. Hernández-Cruz, E. Galarraga, R. Drucker-Colin, and J. Bargas, "Encoding network states by striatal cell assemblies," *J. Neurophysiology,* 99(3), pp. 1435-1450, 2008.

[5] M. Cole and W. Schneider, "The cognitive control network: integrated cortical regions with dissociable functions," *NeuroImage,* 37, pp. 343-360, 2007.

[6] M. Silver, D. Ress, and D. Heeger, "Topographic maps of visual spatial attention in human parietal cortex," *J. Neurophysiology,* 94, 2005.

[7] E. Blasch, S. Rogers, J. Culbertson, A. Rodriguez, L. Fenstermacher, and R. Patterson, "QuEST for information fusion.," *IEEE National Aerospace and Electronics Conf.,* pp. 215-223, 2014.

[8] S. Rogers, M. Kabrisky, K. Bauer, and M. Oxley, "Computing machinery and intelligence amplification," in *Computational Intelligence: The Experts Speak*, IEEE Press, 2003, pp. 25-38.

[9] S. Rogers, P. Amburn, T. Berkey, R. Broussard, M. DeSimio, J. Hoffmeister, E. Ochoa, T. Rathbun, and J. Rosens, "Method and System for Segmenting Desired Regions in Digital Mammograms" US Pat 6091841, 18 Jul. 2000.

[10] B. Birrer, R. A. Raines, R. O. Baldwin, M. E. Oxley, and S. K. Rogers., "Using qualia and multi-layered relationships in malware detection," *IEEE Symp. Comput. Intelligence in Cyber Security,* pp. 91-98, 2009.

[11] D. Ryer, T. Bihl, K. Bauer, and S. Rogers, "QUEST hierarchy for hyperspectral face recognition," *Advances in Artificial Intelligence,* 2012.

[12] J. Evans and K. Stanovich, "Dual-process theories of higher cognition advancing the debate," *Perspectives on psychological science,* 8(3), pp. 223-241, 2013.

[13] G. Pezzulo, F. Rigoli, and K. Friston, "Active inference, homeostatic regulation and adaptive behavioural control," *Prog. in Neurobiology,* 134, 2015.

[14] K. Friston and C. Frith, "Active inference, communication and hermeneutics," *Cortex,* 68, pp. 129-143, 2015.

[15] G. Rizzolatti and L. Fogassi, "The mirror mechanism: recent findings and perspectives," *Phil. Trans. Royal Society,* 369, 2014.