Towards Connecting the Disconnected Internet

Jim Martin
School of Computing
Clemson University
Clemson, USA
jmarty@clemson.edu

Manveen Kaur
School of Computing
Clemson University
Clemson, USA
mkaur@clemson.edu

Long Cheng
School of Computing
Clemson University
Clemson, USA
lcheng2@clemson.edu

Abolfazi Razi
School of Computing
Clemson University
Clemson, USA
arazi@clemson.edu

Abstract*—We live in a world where social and economic disparity has led to many 'disconnects' that collectively provide unfair bias towards the top 1% of of the wealthiest individuals and elite industry behemoths. This bias can be seen in the technical world leading to 'disconnects' including limited access to broadband access and advanced technology. In this paper we identify hidden 'disconnects' that we believe are stifling innovation. We introduce an abstraction called 'application systems' (APPSYS) which, with more development, could move our Nation's disparate forms of large scale technology use (Facebook, Tik-Tok, and 'the Internet') to a technology fabric that includes current Internet applications but supplemented with an overlay of APPSYSs forming a 'tech-fabric' that can benefit all citizens, and that promotes citizens to contribute to the evolution of the concept. The 'fabric' is potentially a merging of our Nation's Critical Infrastructure with commercial innovation. These two worlds historically have been isolated however there are clearly overlaps and synergies that can no longer go unchecked. As the Nation enters the 'Age of Machines', this fabric would provide the unique architectural model required to facilitate more secure, dependable Critical Infrastructure in a manner that reflects Internet-like attributes such as transparency, and policies/protocols for joining individual Autonomous Systems to form a unified system. Critical to the concept is an APPSYS which will have incentives to 'contribute to the greater good'. In this paper, we summarize the APPSYS concept and identify necessary incremental mandates by the FCC to broaden access to advanced technology for all citizens primarily by shifting the FCC's bias away from current policies that promote the disconnect between economic success centered on the allocation of wealth that has seen the allocation move from 80-20 (80% of the wealth is owned by 20% of the population to the current 90-10 allocation split.

I. Introduction

We live in a world where social and economic disparity results in a technological 'disconnect' that unfairly impacts citizens' access to critical technology. The lack of fair access to resources like wireless and Internet access are examples of this trend. Our Nation's Critical Infrastructure sectors, which are defined by the DHS and include the financial, transportation, energy sectors, are highly dependent on ultra reliable intelligent communication-oriented cyber-physical systems (CPSs) to provide services [1], [2]. These systems are characterized primarily by nodes that are AI-based autonomous systems, or that are mobile, likely resource-constrained in computation, memory, communications, and battery power. Examples of the latter include Vehicular Ad-Hoc Networks (VANETs), groups of Unmanned Aerial Vehicles (UAVs) called UAV swarms, and even groups of wireless mobile handheld devices. VANETs use vehicle-to-everything (V2X) communication to incorporate safety-critical applications aimed at reducing road safety, increasing traffic mobility, and improving fuel efficiency [3]. Video-capable UAVs survey agricultural land, conduct high-precision crop monitoring, and are instrumental in supporting a variety of tactical missions on the battlefield [4]–[6]. Communication within these systems is typically provided through limited access to a standards-based WiFi access method or certain 3GPP standards, and by being confined to narrow and limited portions of the available radio spectrum.

Technological 'disconnects' further manifests as the disparity between the rate at which the technology surrounding CPS innovation is growing versus the current Internet's ability to support them. This rapid growth of these systems can be attributed to the evolution of embedded hardware platforms that can be programmed to create these systems. The introduction of low-cost Internet-of-Things kits [7], Unmanned Aerial Vehicles (UAVs) [8], and embedded platforms [9] creates an economic underpinning that drives the advancements within these systems. This growth trend, coupled with developments in fields like Machine Learning, Artificial Intelligence, and Edge/Cloud computing, provides us with the ability to use CPSs for complex data-oriented applications that can truly augment and compliment the services provided by critical infrastructure. However, certain factors limit the innovation. First, the current Internet protocols which have evolved to be quite efficient for traditional flow-oriented applications are not designed to comprehensively support the communication requirements of these systems. For instance, WiFi does not well accommodate the extremely requirements of fleets of short range UAVs. Second, there is a lack of standardization in these systems to support interoperability. Third, the current spectrum policy where these systems can only utilize certain 'allowed' portions of the spectrum results in challenging environments for these systems to operate in. To succeed, the coexisting systems must be able to integrate with the Internet, interoperate with each other, and utilize any/all portions of the spectrum available.

The concepts presented in this work are motivated by the factors that limit the growth of current and emergent communication-oriented CPSs. This work introduces a system abstraction called the Application System (APPSYS). An APPSYS is not a standard application of the Internet but a system comprising hardware and software tightly coupled to

a specified objective. It is a new breed of Internet applications that represents an emergent generation of CPSs that are being utilized by critical infrastructure sectors. It differs from current Internet applications primarily due to its ad-hoc nature and 'out in the wild' operations. An APPSYS comprises mobile or relatively mobile resource-constrained nodes. It typically forms in an ad-hoc manner and dynamically establishes its communications and computation environment to provide a distributed CPS that is capable of using any available portions of the radio spectrum for communication backhaul. UAV swarms, VANETs, and home and neighbourhood wired or wireless networks can utilize the APPSYS concept as their networking and communication solution.

Our constitution designates that access and usage to spectrum are for the use of all citizens and can not be owned by private enterprise. Today's complex cellular industry, incubated, nurtured by the Federal government, reflects a disconnect between citizen's rights and corporate greed. The FCC has successfully stimulated the economy but there is a philosophical dilemma surrounding how to define economic success. Raw, aggregated economic indicators are quite deceiving as they fail to show how economic growth reaches all of our citizens. To use a parable, the FCC's children (cellular companies) have grown into monsters. We need to reset policy to favor the majority through equal access to technology and education [10]. Many of the disconnects we can identify within our country can be addressed by a similar re-focus across all federal agencies. The companies that seem to have an abnormal impact of our Nation's policies will continue to grow and increase the disconnect between the 'haves' and the 'have-nots'. The monsters in our country are effectively given a pass with respect to limiting access of technology and to failures in our Nation's Critical Infrastructure.

Our ideas are not intended to punish or do away with the incumbents. Instead, our goal is to present a technology path that allows all citizens fair access to technology, including contributing to our Nation's development and usage of advanced technology. The expected outcome will be a less vulnerable Nation, a larger portion of the population with access and knowledge of technology, and a new architectural model that modernizes the Internet, particularly the disconnect between the Internet and wireless access. In order for the APPSYS concept to thrive, federal policy change is required that enhances access to citizens in a manner that does not involve the monsters. We advocate a 20 Mhz block of US DOT spectrum (half of which is now available to WiFi) be licensed to APPSYSs allowing the concept to evolve with protection from the monsters. Further, mandating all autonomous wireless systems (similar in concept to the Internet's Autonomous System) must contribute a spectrum slice that can be used by APPSYSs is also necessary. The initial set of APPSYSs will likely be components of our Nation's Critical Infrastructure. These will have missions such as ensuring nuclear power stations do not fail, ensuring autonomous vehicles can improve safety through decentralized coordination that can not fail. Critical to dependable systems is agility - APPSYSs requires new degrees of design freedom such as software defined radios that can leverage the spectrum made available, or able to interact with co-located APPSYSs to leverage connectivity and communications options. We have stated we are at a perilous point in time - we need to democratize access and usage of national resources. We need future systems to share a common architecture, including a standardized control plane that has specific incentives rewarding APPSYSs to consider the greater good. If we allow technology to continue to benefit a small sampling of our population, the tragedy buried within the Tragedy of the Commons will be cemented in our reality.

The APPSYS abstraction leads to an architectural framework that will facilitate innovation in areas where CPSs face barriers to their growth. The APPSYS architecture provides the system with the ability to integrate with the Internet and interoperate with other APPSYSs. Interoperability also provides the ability to share access to the radio spectrum as secondary users utilizing incumbents' spectrum and create reliable system connectivity. The architectural design also provides data services and system-level optimizations that can support complex CPS applications that depend on substantial data collection and analysis. Overall, the APPSYS and its architectural framework provide systems with the design freedom to operate in a variety of conditions and adapt to dynamically changing application requirements and availability of wireless access methods.

Two examples shed light on our motivations: when a cable access customer has an issue with the cable back-haul, there are virtually no backup methods. The typical household has on average roughly 3 smartphones. That capacity is purposely isolated to serve a single device. A second example is related to the US Department of Transportation's 30 year effort to bring wireless technology to vehicles to literally save ten's of thousands of lives (millions world wide). Transportation was allocated a block of 75Mhz spectrum, but because there was not a mandate requiring all vehicles to obtain the wireless radio, the lobbying efforts by the top cellular companies to alter the US DOT's direction and to designate one carrier to build out the infrastructure required for vehicle-to-Infrastructure. The latest WiFi products embrace the FCC's decision allowing shared use of US DOT's spectrum. The constitution clearly specifies that access to spectrum is a fundamental right for our Nation's citizens and can not be owned by private entities. Granted, the FCC was enormously successful in stimulating economic development through its efforts to grow nurture and grow both the cellular and WiFi ecosystems. However, the benefits of the technical innovation driving WiFi and cellular is not equally accessible to all citizens. Further, the success of the FCC's policies has revealed an unexpected outcome: our Nation's Critical Infrastructure is highly vulnerable to failures due to malicious actors, natural disasters, and the reliability of third party service providers. The motivations behind the ideas presented in this paper are meant to raise awareness of this reality and to pose illustrative solutions that are specifically designed to be incremental to current systems. However, there are strong forces in place to keep the status quo. We believe the genesis of the type of

change we describe is the Department of Homeland Security's Critical Infrastructure and Security Agency (DHS CISA) with support from other agencies including the FCC, DOT, DOJ, and the DOD. Our ideas would lead to more equal access to emerging technology, which could stimulate the economy in a less bias manner than current policies. We introduce an abstraction called 'application systems' (APPSYS) which, with more development, could move our Nation's disparate forms of large scale technology use (Facebook, Tik-Tok, and 'the Internet') to a technology fabric that includes current Internet applications but supplemented with an overlay of APPSYSs that adhere to Internet-like rules for openness and an architecture and protocol providing incentives for APPSYSs to grow, interconnect, facilitate innovation but with incentives so that each APPSYS has incentives to 'contribute to the greater good' rather than operate in a greedy manner. We identify incremental mandates by the FCC that broadens access to wireless and supporting technology in a manner that shifts the FCC's bias away from current tech giants towards the majority of the population.

The rest of the paper is organized as follows. In Section II, we elaborate on the APPSYS concept and provide conceptual examples. In Section III, we discuss the fundamental APPSYS architectural framework. In Section IV, we discuss the details of an exemplary APPSYS that is the focus of our ongoing work. We conclude our work in Section V with an outline of the present and future work that will bolster the APPSYS concept.

II. Application System (APPSYS)

The APPSYS concept is motivated by the limitations of the current Internet in supporting CPS and the requirement for a fundamental standardized architectural framework that promotes interoperability among CPSs. It comprises a group of mobile wireless nodes that can collaborate to achieve a common goal or objective. These nodes are resource-constrained and form ad-hoc computation and communication environments. Nodes in the cluster are equipped with agile radios that can adopt to any suitable Radio Access Technology (RAT). An APPSYS is expected to have a communication capacity equivalent to the FCC mandated capacity provided for the Citizens Broadband Radio Service (CBRS) spectrum sharing model. A part of the communication environment is utilizing a suitable backhaul connectivity option from available wireless access methods. The APPSYS accomplishes this through specific designated nodes within the system. Section III discusses this part of the APPSYS architecture in more detail. Through the communication flexibility and support for data services built into the APPSYS design, an APPSYS has the ability to support safety-critical applications and critical infrastructure requirements reliably.

One or more APPSYSs operate under the ownership of a single entity or organization. For example, one or more APPSYSs comprising of mobile, wireless vehicular nodes could form Vehicular-APPSYSs (V-APPSYSs) owned by the US Department of Transportation (DOT). The APPSYS owner assigns the objective to one or more nodes within the APPSYS. APPSYSs can be owned by various organizations within the government or the private sector and applied to a variety of critical and non-critical use-cases. The shared spectrum usage by various APPSYSs follows a priority method where 'critical' and 'high-priority' APPSYSs are provided prioritized access to the spectrum. Fig.1 illustrates through an example the relative priority of some exemplar APPSYSs operating within the same shared spectrum region. We further refer to all APPSYSs owned by a single organization as an APPSYS Wireless System (AWS). The AWS is conceptually similar to Autonomous Systems (AS) utilized in traditional Internet architecture. Like AS, the AWS concept provides abstractions for interoperability among APPSYSs with different ownerships. Ownership of an APPSYS and AWS by a suitable government organization allows the government to maintain much-needed oversight over security in critical infrastructure sectors while also leveraging spectrum resources from spectrum portions privately owned by telecommunication providers through economic incentives and compensation.

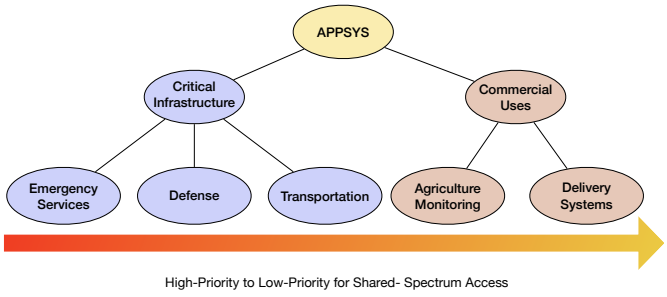

Fig. 1. Example of Priority Access for Shared Spectrum

Conceptual APPSYS Examples

- Broadband APPSYS: The Broadband APPSYS aims to meet the objective of providing reliable broadband Internet access to each participating home in a neighborhood. This APPSYS allows a group of static or relatively mobile (cellular) nodes in a neighborhood to be able to use a suitable backhaul broadband access link for connectivity to the Internet. The suitable backhaul access method for a home could be wired backhaul access through cable-providers, access through participating cellular devices' cellular networks, or access through other Internet connected nodes in the neighborhood. The APPSYS determines which of the available resources to utilize through a designated APPSYS node that can intelligently understand the users' requirements and then provide suitable connectivity. We note that the incumbents do everything in their power to prevent any innovation that is not consistent with their business models (which were incubated by all citizen's taxes).
- Vehicular APPSYS (V-APPSYS): V-APPSYS is a system of vehicles that can discover each other, organize, and

cooperatively perform tasks such as platooning and multi-lane autonomous driving. A V-APPSYS may belong to a state or federal DOT. The V-APPSYS also leverages the backhaul access mechanisms discussed in the earlier Broadband APPSYS example. The V-APPSYS has the capability of connecting to the Internet and to other vehicles in the APPSYS through an open wireless overlay network formed by various telecommunication provider networks and maintained by the APPSYS or AWS owner. For example, the AWS owner could leverage a telecommunication provider's Access Points as edge nodes within an V-APPSYS. This edge node can provide the vehicular nodes with relevant set of security and communication protocols, standard messaging formats, and a unified naming ontology which the vehicles can use to exchange data. This system also promotes robustness and scalability as edge nodes can be provisioned as required by the APPSYS.

- UAV swarm APPSYS: The UAV swarm APPSYS is a system of highly mobile UAVs that can group together to cooperatively achieve an objective. An example of a UAV swarm APPSYS is a group of UAVs tasked with a disaster mitigation use-case such as identifying areas impacted by a forest fire. Such an APPSYS depends on sensor-equipped UAVs within the swarm to collect video streams of regions that are transmitted to a backend or to other nodes within the swarm for processing and analysis. Current UAV swarms utilize the unlicensed spectrum for communication. However, due to the safety critical nature of the swarm's objective, robustness of communication methods provided through high-priority access to the shared spectrum can increase the ability of this APPSYS to succeed in its mission.

III. APPSYS Architectural Framework

The primary components of an APPSYS are one or more groups of mobile wireless nodes, called clusters. An APPSYS comprises one or more clusters of wireless mobile nodes. A cluster is identified as a group of wireless nodes within the broadcast range of each other. Theoretically, multiple clusters organized in a flat or hierarchical architecture reducing the system complexity compared to a single extensive system. The mathematical problem of optimally partitioning a group of nodes into clusters has been addressed in numerous works such as [11]; and the present APPSYS design takes it for granted. Each cluster is heterogeneous and comprises nodes with a range of power, compute, sensing, and physics-based mobility capabilities. Depending on the type of the APPSYS, nodes within the cluster may support a multitude of data-sensing capabilities. A cluster also supports multiple wireless access methods using a variety of interfaces or agile radios, thus, allowing a flexible choice of communication methods.

The APPSYS connects to a back-end infrastructure, called Control Station (CS), which may be located in the cloud, edge, or a physical data center. The CS is operated by the owner of the APPSYS and may support multiple APPSYSs in its AWS through dedicated control nodes. The CS can be considered as an extension of the APPSYS. The CS may interact either with one designated node within the APPSYS and leave cluster formation and local interactions up to the APPSYS, or it may take an active role in cluster formation and interact with designated nodes within the cluster. Further, the CS may assign this set of designated nodes or the APPSYS may elect them. We call these nodes as leader nodes. In the detailed design of the APPSYS, practical considerations such as the requirement for primary and backup leader nodes are accounted for. The CS is responsible for assigning objectives and communicating relevant details through control messages to the leader nodes.

Overall, the cluster leader node serves as a gateway between the CS and the cluster in the APPSYS. It receives and processes control messages from the CS and forwards them to the correct destination within the APPSYS. In addition to cluster leader nodes, a cluster may include nodes with heterogeneous sensing and compute capabilities. The availability of sensing capabilities is utilized in APPSYSs like V-APPSYS or UAV swarm APPSYS. A sensing capable node typically contains one or more sensors and able to transmit data over the APPSYS network. Depending on the scenario, the node might be capable of lightweight computation. For example, a node with a camera sensor might detect moving objects in the video stream. Conversely, the node might be constrained and only transmit the video stream to a different node within the APPSYS. Further, it might be able to participate in a distributed application such as collective monitoring with peer nodes in the cluster. A compute node is typically a highly functional node in an APPSYS capable of handling computation off-loaded from various compute-intensive processes in the APPSYS. It should be noted that the APPSYS has flexible role assignments where any node may operate as a cluster, sensor, or compute node depending on the application requirements at that time. Fig. 2 shows a logical diagram representing the APPSYS architectural framework in the context of a UAV swarm APPSYS connected through a satellite backhaul network.

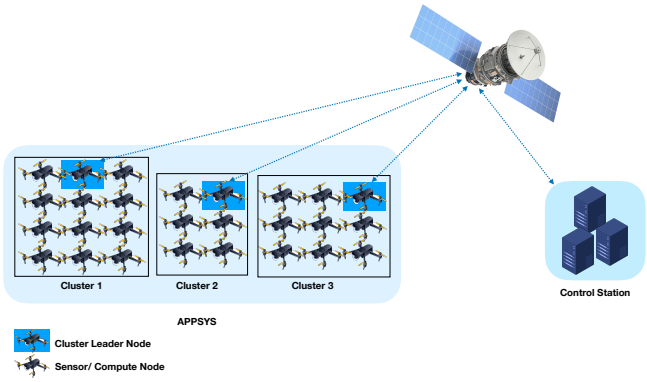

Fig. 2. UAV Swarm APPSYS Architecture

Communications Framework

The APPSYS utilizes Information-Centric Networking (ICN) approach to facilitate communication within the system, with other APPSYSs, and to use the appropriate backhaul connectivity. ICN is a robust named-data-based communication alternative for APPSYS-like mobile networks where conventional host-centric communication does not necessarily meet the communication requirements, e.g., when data sources of interest are geographically and temporally distributed [12]. The use of ICN has been explored in CPSs resembling APPSYSs, e.g., UAV swarms [13]. The ICN implementation employed in the APPSYS communication framework uses a publish-subscribe implementation where all communication sessions are conducted through distributed and decentralized software-based brokers provisioned in each cluster. Nodes transmit and receive data through knowledge of data names, called *topics*, as opposed to the system requirement of prior knowledge of all nodes' IP addresses. The APPSYS design refers to these brokers as *Control Brokers*. These brokers may be co-located with the cluster leader nodes or located in a separate elected node depending on the application and system requirements. Control brokers in each cluster are responsible for facilitating intra-cluster communication. Some or all control brokers from all clusters in an APPSYS also form a communication overlay for inter-cluster communication. This control broker overlay, called the *broker mesh overlay*, provides rich multi-path connectivity for communication between clusters and contributes to the APPSYS's robustness. Fig. 3 illustrates the APPSYS communication framework through brokers located within each cluster.

The control brokers designed for the APPSYS are extended to incorporate a separate control plane. The control plane provides abstractions for the applications running on an APPSYS to interact with the underlying system and exert software-level control over decisions related to selection of appropriate backhaul communication options, spectrum sharing coordination, and system resource coordination to meet an application's QoS and data-dissemination requirements. The system-wide control plane offered jointly through all control brokers within a system can also be used to interact with established control planes such as the one included with 3GPP's Evolved Packet Core (EPC) [14]. Overall, the objective of the offered control plane functionality is to better customize the software-level control functionality of Software-Defined Networking (SDN) for an APPSYS environment.

IV. Illustrative Example of a UAV Swarm APPSYS

In our current work on the APPSYS concept, we are implementing a UAV Swarm APPSYS supporting a Coordinated Search and Tracking (CSAT) application on the battlefield. The UAV swarm APPSYS comprises one or more clusters of wireless mobile UAV nodes as shown in Fig. 2. Each cluster is heterogeneous and comprises UAVs with different ranges of power, compute, sensing, and physics-based mobility capabilities. Most UAVs in the cluster are micro UAVs with a small payload, limited speed/altitude, and constrained compute

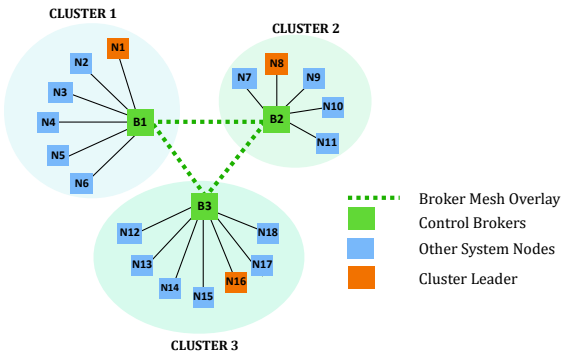

Fig. 3. APPSYS Communication Framework

and memory capabilities. The primary objective of this UAV swarm APPSYS is the CSAT application. The CSAT application involves using the integrated sensing capability of sensor nodes equipped with a visual sensor to locate and track evasive targets on the battlefield [15]. For example, a CSAT application objective might be to locate a vehicle of interest fitting a particular description in the streets of an urban area and then follow it. In its simplest form, CSAT involves sensor nodes in the swarm partitioning and scanning the region of interest for a target and transmitting near-real-time video streams to the CS. A more evolved form of CSAT allows processing of video streams within the swarm in an ad-hoc manner. The sensor nodes equipped with camera modules collect relevant video data and transmit it either to compute nodes within the UAV swarm APPSYS or the CS.

The CSAT application is safety-critical. It has strict Quality-of-Service (QoS) requirements in terms of the low latency and high reliability in receiving the data at the compute nodes or the CS. Further, the UAV swarm APPSYS may be required to relay this data to other APPSYSs on the battlefield, e.g., a tactical vehicle APPSYS. Therefore, this APPSYS requires robust communication access that can be provided through the selection of an appropriate backhaul method using the APPSYS architecture. As the battlefield might have various APPSYSs using the shared spectrum, the UAV swarm APPSYS requires interoperability and communication with other APPSYSs to negotiate and coordinate priority-based spectrum usage. Fig. 4 illustrates the use of multiple wireless access options by the UAV swarm APPSYS in communicating with the CS and the tactical V-APPSYS on ground. The communications requirements may dynamically change on the battlefield and are monitored by the interaction of the brokers with the CSAT application and the control plane abstraction within the communication framework. The control plane abstraction also simultaneously implements system-level communication optimizations that can be used for resource-optimizations required to support a data-intensive application in a resource-constrained system.

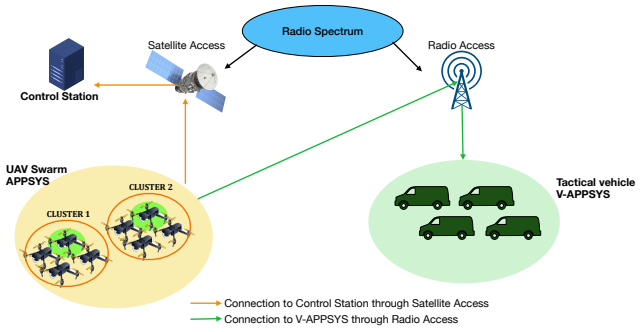

Fig. 4. UAV Swarm APPSYS communicating on the Battlefield

V. Discussion & Conclusion

In this paper we have pointed out that we (citizens, private sector, government agencies) are at a critical point in the evolution of technology and the expected and unexpected adoption and further evolution by stake holders that range from government agencies, private sector entities developing, maintaining critical systems, and future business oriented and consumer oriented application systems. We suggest the key communities consider the warnings described in this paper and use our APPSYS concept as a possible new design paradigm. From the government's perspective, investing in RD to further define the problems, requirements, possibly in the context of an APPSYS will likely allow existing system architectures and software development methodologies can 'catch up' with the extreme rate at which new technology is becoming adopted by users. The current systems have been designed and maintained with assumptions that are becoming archaic, and consequently almost surely will lead to cyber or reliability vulnerabilities that pose potentially catastrophic harm to our Nation. We are at a point where technology is moving faster than government policy and software development evolutions. Historically, our Nation's critical infrastructure could be isolated from non-essential personal through spectrum allocation or proprietary systems that will not be able to evolve at the rapid timescales at which all aspects of society adopt new technology. We conjecture that as we enter the age of a society that blurs human work with that performed by machines and systems that reflect human attributes, we will continue to see massive failures of critical systems due to unexpected outcomes of intelligent systems or due to rogue employees or nation states learn how to manipulate software systems that are not fully understood by developers. We are seeing a tight coupling between seemingly harmless AI-based systems developed to examine large amounts of data to make better decisions for businesses become potentially weaponized as data centric systems become entangled with other business systems that present threats and vulnerabilities to our Nation's citizens. Sophisticated systems are now in place that are decentralized and purposely designed to avoid government regulation. While our country is divided as to the role of the federal government, we urge government agencies to consider the preliminary ideas we have presented. In the future, systems will interact with other systems. The Internet was wildly successful by embracing a global unified system based on hundreds of thousands of Autonomous Systems participating with governing organizations that manage resources, continuously evolve policy to incorporate new technology. We have seen however that the Internet core technology is now outdated. Software Defined Networking, Information Centric Networking, Named Data Networking have been considered as incremental enhancements. Bigger ideas are needed.

A brief example involves how broadband access can be reinvented by incorporating APPSYS design paradigms. Any form of cloud computing, fog computing, or IoT systems are short sighted as they are still being designed as block box systems. We anticipate a world where the most interesting and impactful new applications inherently include infrastructure. Currently, APPSYSs are limited as far as degrees of real-time design freedom to adapt the applications and infrastructure to ensure the APPSYS meets requirements. Today, there is clear disconnect between broadband access and the divide due to race, economic classification, and a varity of tribal artifacts that exist in today's society. An APPSYS design to broadband access would redefine our current broadband providers to a provider that supports the deep interactions between many APPSYSs. If a cable plant in a neighborhood goes out for a day, we turn to hot-spot service with 3GPP devices. An APPSYS paradigm would abstract the 'access' through APPSYS interaction and remolding the infrastructure to avoid the outage in a manner that is transparent to users. A neighborhood could form an APPSYS fabric perhaps based on community mesh nodes and cellular backhaul. Broadband operators can view this as opportunities for new revenue. A Nation that is served by a system of small APPSYSs that cooperate will provide economic growth potential. Currently, incumbents want to be the providers of future services. But a nation that is controlled in part by incumbent entities will not allow the additional degrees of APPSYS design freedom that is needed. A simple incremental mandate by the FCC that reserves a 20MHz channel from the US DOT's DSRC spectrum, combined with a mandate requiring autonomous wireless systems to contribute a spectrum slice would be sufficient to create an overlay that spans all wireless and wired AS's. A Broadband Provider could reinvent gateway equipment to enable the level of APPSYS tangles. A large cable operator could sell backhaul or APPSYS support and services to entities, such as the US DOT, that are currently at a loss as to how they should move forward ensuring that decisions are 'enablers' rather than single purpose, expensive, overly complex systems and government regulatory processes or significant new systems (such as coordination of autonomous vehicles) The new Internet will need to embody an infrastructure driven by thousands of APPSYSs to 'interact' forming Internet scale APPSYSs. We anticipate the Internet eventually replaced by this 'fabric' of APPSYSs that is somewhat equivalent to a world of APPSYSs that can grow and modify services and

capabilities literally in real-time. The ideas we have described address significant vulnerabilities in our country's Critical Infrastructure, and would stimulate innovation to any citizen, not just the dozen largest tech companies that seem to drive our country. In today's age of machines, data is a form of currency and technical knowledge along with access to our APPSYS fabric seems like a very effective and timely direction for our Nation.

REFERENCES

[1] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161–166, 2011.

[2] "Critical infrastructure sectors." https://www.cisa.gov/critical-infrastructure-sectors. Accessed: 04-13-2022.

[3] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, p. 100310, Apr. 2021.

[4] J. Kim, S. Kim, C. Ju, and H. I. Son, "Unmanned Aerial Vehicles in Agriculture: A Review of Perspective of Platform, Control, and Applications," *IEEE Access*, vol. 7, pp. 105100–105115, 2019.

[5] N. Gempton, S. Skalistis, J. Furness, S. Shaikh, and D. Petrovic, "Autonomous control in military logistics vehicles: Trust and safety analysis," in *International Conference on Engineering Psychology and Cognitive Ergonomics*, pp. 253–262, Springer, 2013.

[6] F. Xiong, A. Li, H. Wang, and L. Tang, "An SDN-MQTT Based Communication System for Battlefield UAV Swarms," *IEEE Commun. Mag.*, vol. 57, pp. 41–47, Aug. 2019.

[7] "Arduino products - internet of things." https://www.arduino.cc/en/Main/Products/. Accessed: 11-08-2021.

[8] "Dji phantom 4." https://www.dji.com/phantom-4/info/. Accessed: 11-06-2021.

[9] "Raspberry pi personal computer kits." https://www.raspberrypi.com/products/. Accessed: 11-08-2021.

[10] E. P. Goodman, "Spectrum auctions and the public interest," *J. on Telecomm. & High Tech. L.*, vol. 7, p. 343, 2009.

[11] A. Gogu, D. Nace, A. Dilo, and N. Mertnia, "Optimization problems in wireless sensor networks," in *2011 International Conference on Complex, Intelligent, and Software Intensive Systems*, pp. 302–309, IEEE, 2011.

[12] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[13] P. Boccadoro, M. Losciale, G. Piro, and L. A. Grieco, "A Standard-Compliant and Information-Centric Communication Platform for the Internet of Drones," p. 6.

[14] J. Kim, D. Kim, and S. Choi, "3gpp sa2 architecture and functions for 5g mobile communication system," *ICT Express*, vol. 3, no. 1, pp. 1–8, 2017.

[15] P. Vincent and I. Rubin, "A framework and analysis for cooperative search using UAV swarms," in *Proceedings of the 2004 ACM symposium on Applied computing - SAC '04*, (Nicosia, Cyprus), p. 79, ACM Press, 2004.