2020 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
CYBER/VEA TECHNICAL SESSION
AUGUST 11-13, 2020 - NOVI, MICHIGAN

Secure Wireless Communication supporting Vehicle-to-Vehicle and Vehicle-to-EUD for Mounted and Dismounted Connectivity

[1]David Gregory, [1]Jeff Nelson

[1]Pacific Star Communications, Portland, OR

ABSTRACT

The goal of Secure Wireless Communications is to provide controlled access to classified or controlled unclassified information (CUI) over <u>any</u> RF transport in the field – between vehicles and end users alike. Secure – yet simplified – system deployment, node integration, managed accessibility, network situational awareness, and configuration management are all essential for maintainability.

Citation: D. Jedynak, C. Kawasaki, D. Gregory, "Managing Next Generation Open Standard Vehicle Electronics Architectures", In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2019.

1. INTRODUCTION

Future ground vehicle platforms, such as: Command Post Integrated Infrastructure (CPI2), Next Generation Combat Vehicle (NGCV), Manned Fighting Vehicle (MFV), and Robotic Combat Vehicles (RCV) – will significantly improve fleet speed and mobility and cannot be fielded too soon.

These ground vehicle programs will greatly benefit from vehicle-mounted secure wireless communication architectures utilizing small form factor, rugged, commercial-off-the-shelf technologies (COTS) to interconnect vehicles, tents, users, etc. while maintaining sufficient security postures to meet various cybersecurity objectives.

Pacific Star Communications (PacStar®) has pioneered the tactical implementation of secure wireless communication solutions on small form factor hardware – leveraging NSA approved commercial components – ideally suited for meshing vehicle-to-vehicle (V2V) and vehicle-to-EUD (V2E) for mounted (on-platform) and dismounted (off-platform) end-user devices (EUD). These solutions are designed to support voice, video, and data for C2 communications and have been optimized for size, weight, and power (SWaP) to fit within the limited spaces onboard vehicle platforms. These secure wireless solutions are transport agnostic and compatible with Wi-Fi and VPN encryption components – making it possible to eliminate the need for external Type1 cryptographic equipment and controlled key material.

Using properly configured, layered commercial technologies to correctly implement secure wireless communication promises multiple benefits including true mobility and maneuverability for both mounted and dismounted EUDs.

As an example, providing secured wireless local area network (WLAN) services inside vehicles and vehicle-mounted shelters – while simultaneously providing communications between vehicles over wireless mesh networks – will dramatically reduce (if not eliminate) setup

time over current "mobile" command post deployments involving the installation of thousands of feet of networking cable and "physical" network infrastructure to interconnect vehicles and/or tents.

Utilizing Commercial Solutions for Classified (CSfC) or Controlled Unclassified Information (CUI) architectures makes it possible to wirelessly interconnect vehicles and host secure WLAN service from vehicle platforms for various EUDs – such as smartphones, tablets, laptops, soldier wearables, IVAS goggles, etc. – to enable various use-cases for classified, unclassified, and/or coalition partner networks, such as: augmented reality (AR), mobile command and control, wireless intercom, condition based maintenance (CBM) offload, ISR collection and dissemination, etc.

As seen in the commercial market, implementing WLAN communication (securely) will open the door for innovative solutions to existing and future operational challenges.

2. CHALLENGES AND BENEFITS

Challenges surrounding secure wireless communication include cybersecurity resiliency (i.e. intrusions detection and prevention), network configuration management and situational awareness:

Cybersecurity of Secure Wireless – Given existing and emerging Electronic Warfare and Cyber threats it is assumed that cyber-attacks will increase in sophistication and complexity. Without a robust monitoring and management solution the inclusion of wireless network technology at the tactical edge will increase both the attack vector diversity and the training requirements of the Soldiers.

Although the primary objective for a secure network is to, "plug all holes," it isn't entirely realistic. Detecting (and preventing) intrusion attacks and continuously monitoring network access are essential to wireless communication since the "RF transport" is a physically unguarded transport medium. Leveraging a robust communication management tool is needed to:

- *Automate IDS & IPS response:* Trigger conditions and rapid responses are invaluable for secure networks. Detecting anomalies and responding with appropriate action (i.e. shutting down port access) will dramatically improve security.
- *Save Time:* Simplify complex, time-consuming, and error-prone work-flows with powerful automated task wizards and standard user interfaces across components
- *Reduce Configuration Errors:* Significantly reduces configuration errors, assist in maintaining uptime and compliance with cybersecurity requirements

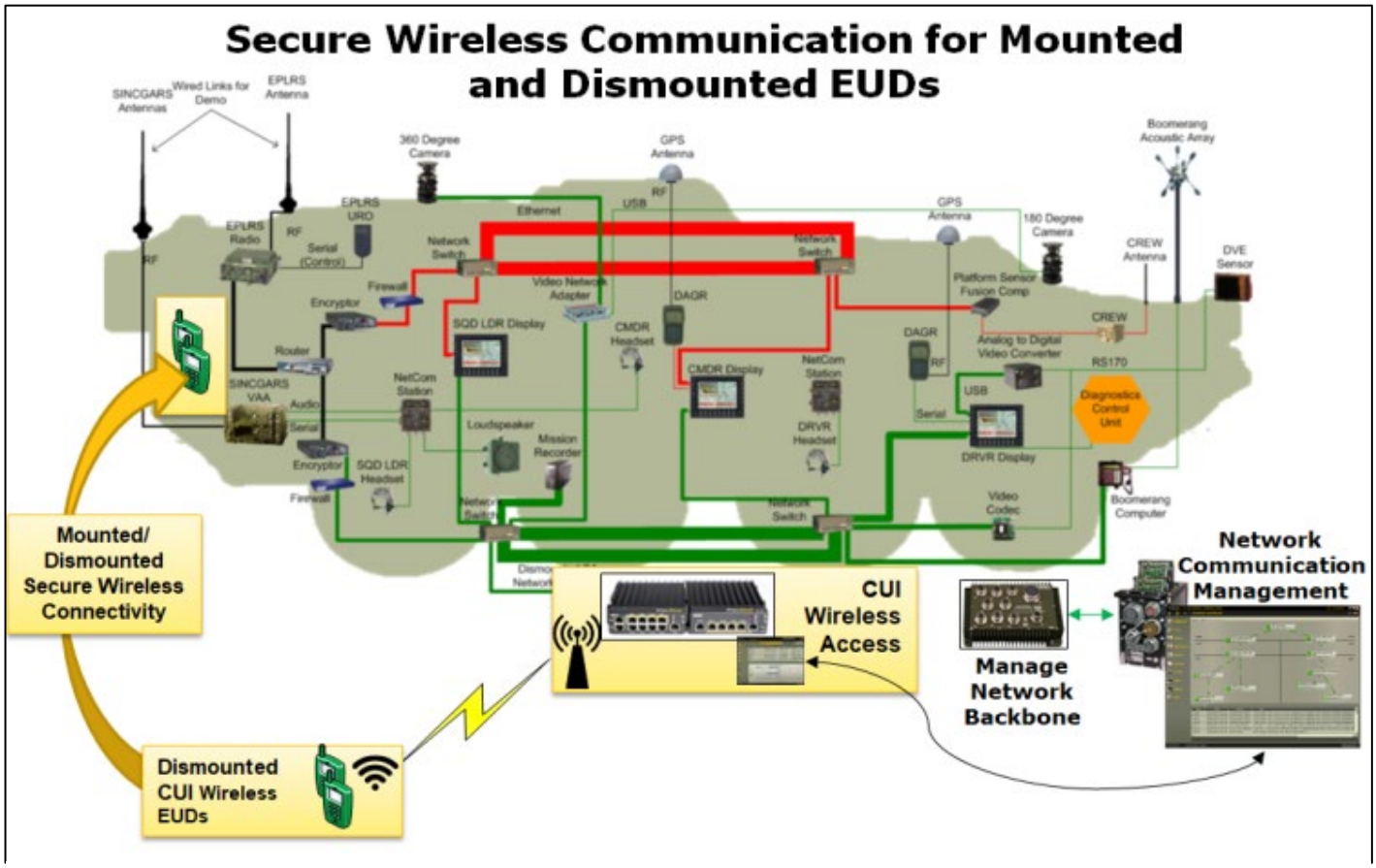

Figure 1 - Example of CUI Secure Wireless Communication

Network configuration management and situational awareness – Eliminating configuration errors and inconsistencies is a primary objective of any network security administrator - both human error and manual configuration introduces unnecessary risk.

Sharing essential device configurations and network information with users at different echelons, and creating a collaborative, hierarchical, network operations and management structure is a daunting task for any communications team. Intuitively unifying configuration management and network situational awareness under a "unified interface" across the entire network possess a significant challenge for wireless networks – especially in disconnected, intermittent and limited (DIL) environments.

Further, introducing multiple classifications and cross-domain functionality increases the necessity for robust, intuitive, and consolidated monitoring and management of the underlying infrastructure. In many cases there will be significant differences between classified and unclassified systems, further fueling the configuration management challenges.

To overcome these challenges, it is necessary to introduce a remote operations and management tool on both central and distributed vehicles (even some EUDs) to provide redundancy and continuous monitoring needed for real-time status, alerts, and auditing. Similarly, such a tool will be needed to disseminate configuration files, record revision history, and simplify troubleshooting for both entry-level and advanced network administrators.

Major benefits of secure wireless communication include scalability, transport flexibility, and cost:

Scalability – Once correctly implemented, a robust secure wireless communication environment for V2V and V2E is easily used and easily scaled – like Wi-Fi networks we are all familiar with – to support numerous remote support vehicles and EUDs. New devices can be provisioned and joined to the network (within limits) without adding additional infrastructure.

Vehicles, mounted and dismounted users are able to freely maneuver while remaining connected anywhere within the wireless footprint. Further, device access is controlled with certificates – supporting a flexible and expandable authentication mechanism.

Transport Flexibility – PacStar's CSfC and CUI secure wireless solutions are transport agnostic on the black transport between vehicles and EUDs– meaning it can use nearly any transport with sufficient internet protocol support as black transport, including: tactical and mesh radios, Wi-Fi, Wi-Fi6, 4G LTE, 5G, optical line-of-site, and even host-nation cellular

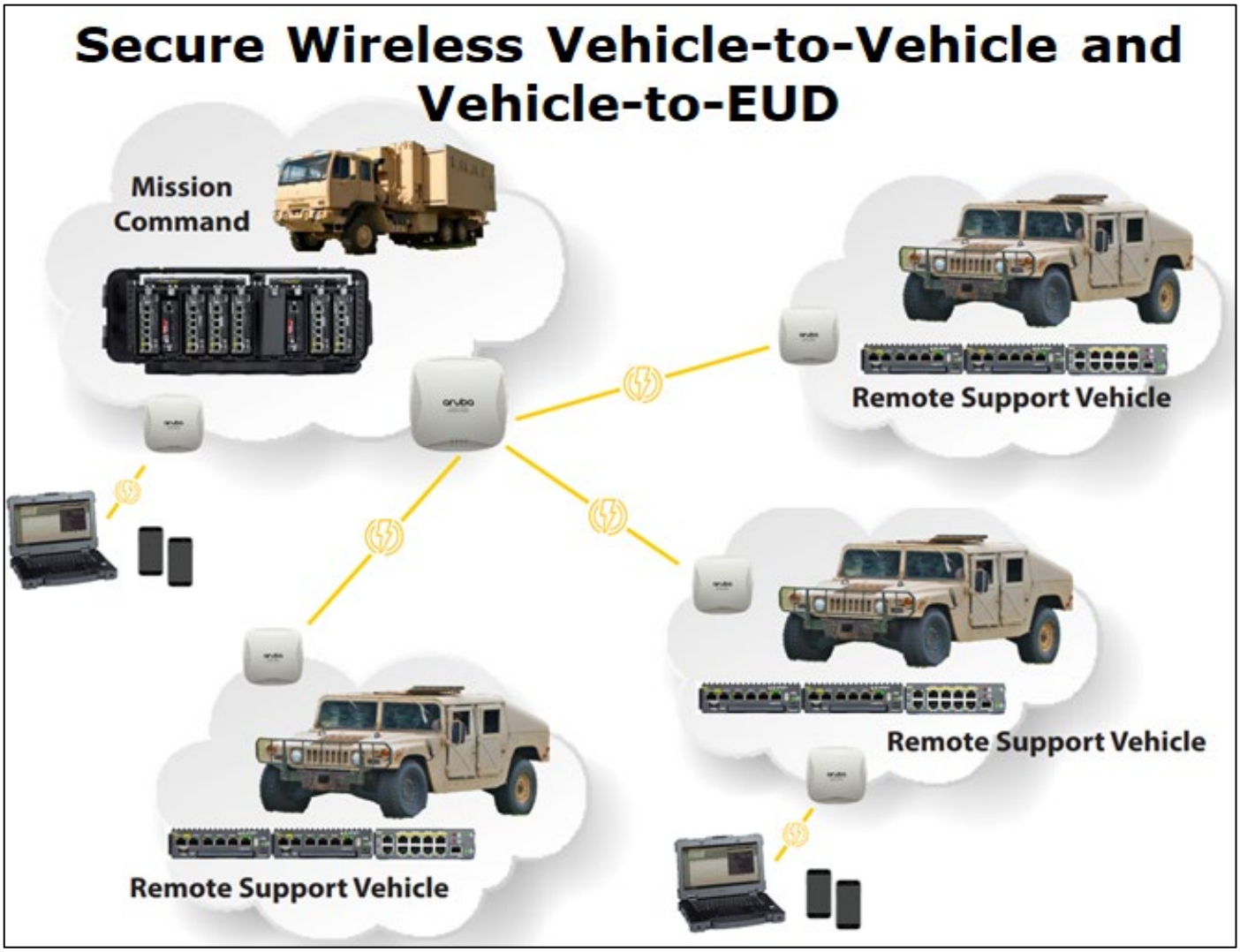

Figure 2 - Secure Wireless V2V and V2E Reference

Cost – Properly implemented, secure wireless doesn't require redundant physical network interconnects (access switches, cables, etc.) between devices or nodes. As such, the entire secure wireless environment is re-usable with little to no deployment time – reducing costs in time, space, and power.

3. TECHNICAL APPROACH

PacStar has demonstrated a robust secure wireless communication solution for V2V and V2E using PacStar's Secure Wireless Command Post (SWCP), SWCP-Extension (SWCP-X), and IQ-Core® Network Communication Management (NCM) software with Remote Operations and Management (ROAM) capability.

The complete secure wireless communication architecture includes PacStar SWCP generally mounted on main command post platforms, and PacStar SWCP-X on remote (smaller) support vehicles. PacStar SWCP provides Central Site encryption, PKI and management services for the entire fleet of connected vehicles and EUDs. PacStar SWCP also provides Wi-Fi access points on the main command platforms for secure EUD Wi-Fi access.

On remote support vehicles, for V2V communications, PacStar SWCP-X uses layered IPsec VPN gateways over meshing radio, enabling the transport of one or more classified and/or unclassified networks between remote support vehicles and main command post vehicles.

On remote support vehicles, for V2E communications, PacStar SWCP-X includes Wi-Fi access points configured to meet CSfC requirements that provide network access to EUDs. The Wi-Fi network uses layered encryption, managed by the PacStar SWCP in the main command post vehicle, to extend Wi-Fi services to remote vehicles while minimizing the SWaP requirement on the remote platform.

This architecture is efficient and managed by PacStar IQ-Core® Software to minimizing complexity.

3.1. PacStar® SWCP

PacStar Secure Wireless Command Post (Wi-Fi) is a small modular communications package that enables secure wireless and mobility for smart phones, tablets and laptops for classified networks in deployed, expeditionary and tactical environments.

The solution architecture follows the NSA Commercial Solutions for Classified (CSfC) Campus WLAN Capability Package v2.0 to enable EUDs to utilize built-in commercial Wi-Fi on mobile devices to provide one layer of the required two-layer NSA encryption requirements. Combined with a single VPN client, end user devices are able to transmit classified information over Wi-Fi.

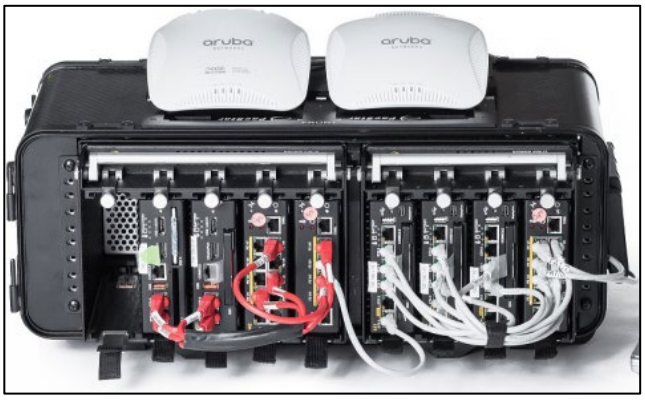

Figure 3 - PacStar SWCP (Wi-Fi)

PacStar Secure Wireless Command Post as shown above provides transport for access to a single secure network. The solution is configurable (with additional equipment) to provide transport for multiple classified networks (including networks of different levels of classification up to Top Secret) over a single wireless infrastructure. It can also be configured to serve a wide range of team sizes, and can be customized with additional software and solutions to ensure interoperability with existing infrastructure.

3.2. SWCP-X Contents

PacStar SWCP-X supports one or multiple networks and can be scaled to meet mission requirements – typically utilizing the following components configured in accordance with Commercial Solutions for Classified Multi-site Connectivity Capability Package v1.1 – as a Remote Centrally Managed Site:

Figure 4 - PacStar® SWCP-X

3.3. IQ-Core

IQ-Core Software is designed to reduce administration complexity and provides a single user-interface under a unified interface – connecting with various technologies using SNMP, SSH, REST Application Programming Interfaces (APIs), VICTORY, etc.

IQ-Core Software is a light-weight application running within each node (i.e. mission command vehicle, remote support vehicles, command tents, etc.) to interact and manage on-platform and off-platform network components. The IQ-Core Remote Operations and Management (ROAM) component adds robust capabilities to enable centralized management of distributed network nodes at multiple tiers in a hierarchical and efficient manner.

Figure 5 – IQ-Core® Software Unified Dashboard

IQ-Core ROAM is designed to manage networks in disconnected, intermittent and limited (DIL) environments – making optimal use of network bandwidth and working reliably where loss of connectivity is a regular occurrence. Additionally, it also works well for enterprise networks with multiple, distributed, remote locations by converging management of all essential systems.

Key IQ-Core benefits for secure wireless include:

- *Common User Interface* - upper network tiers (echelons) and Network Operation Centers (NOCs) that mirrors remote systems, offering simplifying navigation and consistent management throughout the network.
- *Auto-Generated Network Diagrams* – dashboard showing the logical structure of hierarchical nodes (including ability to drill-down and see important data at-a-glance.)

- *Reduced Configuration Errors* – automates deployment of network planning and configuration files across the network, ensuring consistent configuration of all network devices.
- *Optimized for Situational Awareness* - designed for tactical and distributed networks to provide enhanced network situational awareness, with extensive real-time visibility of connected nodes. Operates seamlessly in disconnected, intermittent, and limited environments.
- *Automated Cyber Defenses* – improves cyber visibility by securing, consolidating and forwarding alerting information at each tier of the network.
- *Field Proven* – based on the widely deployed IQ-Core Software communications management platform.
- *Unified View* – provides network monitoring and diagnostics in a unified interface with real-time snapshot of the health of the network, and ability to provide backup and restorations of entire network.
- *Adapts to User Level* – designed for non-specialists, it offers the flexibility and capabilities to meet the needs of advanced power users.
- *Enhanced Ability to Meet Mission Objectives* – Reduces setup time – allowing communication systems to adapt to rapidly changing circumstances. Improves up-time – allowing personnel to focus on fighting the fight, not fighting the network.

4. CONCLUSION

Secure wireless communication technology combinations for V2V and V2E communication will deliver benefits for tactical environments by improving network flexibility and operational maneuverability while reducing management complexity and cost.

As seen in the commercial market, implementing WLAN communication (securely) will open the door for innovative solutions to existing and future operational challenges.

This secure wireless communication capability can provide distributed, hierarchical, and efficient management of V2V and V2E connectivity across multiple platforms and at multiple tiers for future ground combat ecosystems.

5. REFERENCES

[1] National Security Agency Central Security Service, *Commercial Solutions for Classified Program (CSfC)*, National Security Agency, Ft. George G. Meade, MD, USA, Active Program. [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/