Military Wireless Communication (MWC) Group
TNT / CBE 10-1 AFTER ACTION REPORT

Executive Summary

The Wireless Military Communications Group, a collaborative team of researchers from the CS and ECE Departments, partnered with the CENETIX team and leveraged the Tactical Network Topology (TNT) Capabilities Based Experimentation (CBE) 10-1 venue to test a proof-of-concept for an integrated COTS/GOTS, high-capacity tactical information dissemination system concept. This system aims to integrate voice, text, imagery, streaming video and web functionalities into a small, user-friendly form-factor suitable for employment in all but the most arduous combat environments. Furthermore, it relies on the scalability of IP networks to support rapid integration of other force elements, including local government and non-government coalition partners.

Initial results from the TNT tests call for more robust exploration of this capability. The agile functionality achieved from the integration of the Commercial-Off-the-Shelf (COTS) personal communication systems (PCS) and the robust militarized tactical radio systems shows great promise for delivering a robust capability to our military sponsors within a compressed timescale. The observed flexibility of the PCS devices as the primary human interface device provides for rapid application development and dissemination focused on the evolving needs of the combatants themselves rather than disassociated commercial applications developers.

It is well recognized that current acquisition strategies for militarized systems cannot maintain currency with commercial capabilities. Further, the unit cost for military-grade systems makes it fiscally impossible to field systems that keep pace with the innovation of mass-marketed commercial systems. While military members struggle to squeeze as much capacity as possible out of their combat communications systems they are bombarded with new and innovative ways to exchange high resolution information in their personal lives. This disconnect between the tactical information access capacity and the explosion of commercial PCS leads to frustration for combatants who know the capability they so deeply need in

the field, and upon which their lives may depend, is available to the average civilian as entertainment.

The team of students integrated commercial mobile wireless access points, small form-factor cellular base station systems, and tactical radios in Highly Mobile Multi-wheeled Vehicles (HMMWV) to form mobile tactical cellular and local wireless hotspots. User access to these communications capabilities was provided through various “smart phones” (cellular PCS). WiFi routers were only leveraged to maximize the potential traffic for throughput testing across tactical radios. The purpose of the architecture was not intended for showcasing a deployable proof-of-concept, but to illustrate the potential of our current tactical radios with attached base stations.

The operation context provided by the TNT venue has proved invaluable to demonstration of the targeted capability. However, the mechanical and electrical integration of the communications equipment in the vehicles needs more careful consideration. While tactical mounts were used where available, the improvised power connections proved insufficient during vehicle operation. This issue must be remedied before more stringent demonstrations can be performed.

I. Background

The research is driven by the lack of communication capabilities observed by front-line troops while providing disaster relief, humanitarian assistance, or conducting full-scale combat operations. The diversity of these mission sets place a wide range of constraints on the systems required to support the operations. Traditionally, the U.S. and Allied ground troops are briefed a mission order, allocated specific communication assets, and deployed to diverse austere environments. Since the operational impact of communications failures and compromises increases with mission importance, the focus of sophistication is significantly geared toward security and reliability, limiting opportunities to incorporate rapidly advancing commercial-off-the-shelf (COTS) capabilities often taken for granted by civilian populations in developed and many third world countries. Therefore, communication capabilities are inadvertently limited to prevent expediential cost increases. Our research goal is to increase the communication capabilities of front-line tactical forces, while mitigating security and reliability vulnerabilities relative to COTS systems and reducing the cost-to-capability disparity inherent in tactical military communications systems.

As one venue for acquiring current commercial quality capacity, we are evaluating the feasibility of leveraging commercial cellular technology and mobile wireless "hotspots." However, since the traditional commercial cellular and wireless networks were designed for less restrictive requirements, with respect to component robustness and transmission security, the technology is not sufficient directly off the shelf for military applications. The project aims to bridge this requirement gap. Our current focus is on content protection, infrastructure security, military spectrum access, and decentralizing the communications architecture. With a decentralized architecture the services are distributed down to the lowest level communication asset in parallel with the flow of information to the task force commander and staff. Therefore, this peer-to-peer network facilitates a scalable solution and minimizes the potential for catastrophic failures (i.e. where current information may be concentrated at a single location and one downed server could affect thousands of clients).

The TNT Exercise is an opportunistic environment for testing and developing our ideas, especially as we are taking an evolutionary development approach to the concept such that user input can be considered at each step in the research effort. Our research group partners with the Center for Network Innovation and Experimentation (CENETIX) team. As suggested by the CENETIX group we have decided to leverage their resources and experience. Therefore, the TNT Exercise was chosen as the testing platform for our integrated cellular concept. We plan on attending the exercise on a quarterly basis to identify and resolve possible shortfalls normally experienced with laboratory environments. The purpose for attending TNT CBE 10-1 was to implement a contrived topology suitable for evaluating the feasibility of cellular traffic across a military radio network backbone.

II. Scope of Experiment

Since the main purpose for participating was feasibility testing, our scope was limited to incorporating the tactical radio throughput restrictions, the commercial base station throughput requirements, and the resource requirements needed to support common cellular capabilities. The testing during this CBE was limited to commercially available equipment for proof of concept design considerations. The plan was developed to explore the currently available solutions without any modifications. The concern is that perhaps our initial conjecture is short-sighted and the commercial industry already possesses a valid solution. Therefore, this exercise was limited to configuring COTS cellular mobile base stations or WiFi access points to host local networks and GOTS tactical radios to interconnect the local networks. WiFi access points were added to supplement the low data rates inherent to the 2.5G technology used by the mobile base stations and maximize channel capacity utilization for the tactical radios.

As characterized by the assortment of COTS and GOTS devices, the technology readiness level does not apply. However, the anticipated results will establish a baseline for future development. For example, how many reliable cellular channels can a single channel half duplex tactical radio support? Compared to what was measured in the lab environment, do the throughput rates fluctuate and directly correlate to channel capacity in a field environment?

For this TNT exercise, we enlisted 12 students from an internal NPS Mobile Devices class. These students planned and conducted small experiments within the scope of our research. The lists of topics included were: tactical wireless routers, TwiddleNet integration, mobile web servers, distributed Position / location reporting, and a cellular traffic monitoring tool implemented on the handset.

III. Results of Experiment

Our Capabilities Based Experimentation (CBE) convened on 16 Nov 2009, at Camp Roberts Army National Guard Base. The plan was to setup our experiment(s) during the morning hours and execute the testing each day following lunch.

However, the first two and a half days were expended trying to configure newly released tactical radio firmware upgrades due to the lack of vendor documentation. The decision to perform a firmware upgrade a week prior to our experiment was determined based on the limitations of the previous releases and complexity of our architecture. During those two and a half days some unexpected troubleshooting uncovered some valuable insight into the true difficulty of the research. Since our overall intent is to evaluate the feasibility of cellular integration into military communications the implementation consisted of mobile base stations as a cellular network overlay interconnected by military communication backhaul links. Once the design was executed questions arose: how sophisticated or smart should the base stations or tactical radios be? If the mobile base stations are capable of routing and locally hosting cellular services do the tactical radios need to provide additional capabilities other than interconnecting the base stations? After the initial delays (i.e. refitting HMMWVs with compatible equipment, reloading crypto devices, reinstalling mission sets, and reprogramming routers to account for unexpected external IP conflicts), we were successful in recording one and a half days of observations / results. The following is a list of issues/considerations raised during all the experiments, which we will address during the next several TNT iterations:

Channel Capacity of Tactical Radios

Traditionally, tactical radios have a comparatively limited data capacity. Therefore, this became our first major concern when evaluating integration feasibility. The 2.5G cellular technology was chosen because of its limited data capacity. Using an academic approach for the evaluation, we benchmarked our results from measurements obtained in a lab environment. For the relatively small number of trial runs the channel capacity of the tactical radio network was sufficient and did not result in a bottleneck. However, the channel capacity of mobile base stations proved to be a bottleneck with the GPRS technology. Aside from our empirical testing (which used ttcp as the measurement tool), the capability of the tactical radios is evident by the observed six simultaneous GSM phone conversations across a single hop half duplex single channel tactical radio link.

Signal range tactical radio vs. base stations

At the start of one experiment all cell phones were originally paired with the Tactical Operations Centers (TOCs) base station. The purpose of the test was to map out signal connectivity for the tactical radios. As the vehicle departed the TOC, about at the 2 mile mark, the tactical radio backhaul link dropped (not as a result of equipment failure), but unexpectedly the TOC mobile base station cell phone connections were still active. The cell phones aboard the vehicle were expected to drop the TOC base station and pair with the mobile base stations within their vehicle. However, this never occurred. Regardless of whether the vehicle mounted base stations were not functioning properly, the situation suggests better reception for the base station for this instance as compared to the tactical radio. This is partly attributed to the higher power output from the TOC mobile base station vises the tactical radios.

GOTS / COTS Disparities

Intermittent connections between the tactical radio and the mobile base stations caused frivolous association drop-outs between the two components. The mobile base stations were not designed for extreme weather conditions, intermittent backhaul associations, and varied DC power fluctuations. These issues along with the black box proprietary network waveform onboard the tactical radios could potentially be blamed for the majority of the observed inconsistencies. The contrived architecture was not designed as a system, but as individual modular parts.

The tactical radio subsystems incorporated an IP routing capability bridging the “red” sub-networks over the “black” networks that interconnected the radio suites as a wireless wide area network. Any changes to the connected “red” subnet router required re-cycling of the radios even though changes were not made within the corresponding interface. Additionally, the radios incorporated a proprietary route exchange mechanism between configured radio subsystems. Any changes to any one of the radios required a reload of the configuration on all radios, indicating a limitation to the adaptability of the radio to network topology changes. Furthermore, the tactical radio routing scheme requires a considerable amount of manual static configuration prior to operation. The current configuration interface is difficult to use and lacks documentation.

Cellular Base Station Observations

The cellular mobile base stations are not IP routers. They are best described as switches with Dynamic Host Configuration Protocol (DHCP) functionality. For our test configuration a global synchronization of their phone association tables was required. WiFi routers maintain routing tables in a manner different than Global System for Mobile Communications (GSM) base stations. In the GSM/ General Packet Radio Service (GPRS) configuration used at this experiment each cellular system functioned as a pico-cell of a single logical mobile switching center. As such the association parameters, which define the authentication and access authority of individual handheld devices, are shared between the pico-cells to form a single replicated table. The forwarding information represented by these tables is independent from the forwarding tables generated by the WiFi routers by which the handheld devices acquire 802.11 capabilities. This implementation is not scalable without the ability to control the devices remotely (e.g. through a switch controller).

Mobile base station reliability

The backbone links across the tactical radio network had a significant drop in reliability in comparison with the connections through a single mobile base station. Future testing will identify the root cause through quantifiable measurements to determine the weak link. This CBE was not designed to test multiple hops, but instead provide a proof-of-concept for consideration.

Video Transfers

As expected, the video transfer across the GPRS link had significant quality of service degradation in comparison against the WiFi. Surprisingly, the degradation persisted when both links were present. For example, two inherent interfaces resident on the majority of worldwide cellular handsets are WiFi and GSM. The devices automatically decide on the best path. Therefore, we assume the GPRS link has the priority over other interfaces by default. Future experiments will investigate the idea of forced prioritized links based on capabilities. This algorithm is different for every phone. Some of the phones were built with WiFi being the highest priority and the GRPS link being a secondary.

The proprietary video distribution software worked well which provided live video feeds between cell phones, client computers, and from the two IP based cameras. One noticeable difference as mentioned above was the increased throughput observed from leveraging the WiFi routers instead of the GPRS links. However, we didn’t observe a difference between video frame rates when the connection was routed across the tactical radio network or remained locally hosted in the TOC LAN.

Social networking application implementation

TwiddleNet is an internal Naval Postgraduate School designed, developed, and tested social networking application used for distributing information between low bandwidth devices. This event was important for testing the functionality of the system. The employed version of TwiddleNet made significant improvements beyond the last version by adapting to a more mobile concept.

Cell phones hosting local web server functionality

Every cell phone used for the experiment had the capability of providing mobile web server functionalities. This proved to be extremely valuable in an intermittent wireless environment. Once the backhaul connection for the access point was severed the local clients could still share information via a peer-to-peer (P2P) method. Each client remained connected to the access point (i.e. WiFi or GPRS mobile base station) therefore providing the bridge between other local clients.

Command and Control Utility

We specifically designed the topology to evaluate the feasibility of using cell phones as Situational Awareness sensors. This can be extremely useful if users wish to share or retrieve local information (e.g. phones could be configured to share their Position Location Information (PLIs), network status, and system status without a centralized server). With the use of video distribution software we were able to view all provisioned cell phones PLI information from a remote Command and Control (C2) location. Essentially, every cell phone had the GPS capability, which reported the PLI information back to the C2 site. We observed every phone provisioned with the PLI software locally at the C2 site. This gave us a global real time view of every device deployed throughout the exercise. Future research will need to consider the security vulnerabilities this information may pose.

Remotely controlling vehicle mounted IP cameras

Both cameras controlled remotely were easily accessed through the inherent web portal. However, when attempting to connect via a third party application the results were not as successful. The third party application sometimes paired to one camera but not the other. Once paired the streaming video seemed to be at a faster rate through the web page than the application. However, this live video stream capability is extremely valuable. To obtain the capability of viewing and controlling the IP cameras no additional hardware outside of the camera itself is required. The camera can connect directly to the leveraged tactical radio. This enables commanders to view, record, and remotely control video during any operational exercise.

Cell phone operating system limitations

On numerous occasions the Nokia phones OS (Symbian) proved to limit popular applications (e.g., packet sniffer) easily found for Window Mobile, Blackberry, or iPhone. On multiple occasions our explorative research required readily available popular open source applications. However, these applications weren’t available for the Symbian OS. For future considerations, the cell phone OS flexibility should be considered when developing a concept of operations.

Situational Awareness degradation by adding a technology focal point

The participants executing the test were at times drawn to the technology, while abandoning the concept of situational awareness. Thus, the enhanced capabilities may actually pose a distraction hazard. Potentially complicating factors include the small size cell phone screens, the glare from the sun, or the idea of running a proof-of-concept test and not representatively implementing a realistic operational test.

IV. Lessons Learned

Monday morning setup

Our experiment was set up in a lab context the week prior for validation purposes. In the process of transferring equipment between NPS and Camp Roberts the Controlled Cryptographic Items (CCIs) were wiped out from the tactical radios. This is required when transporting CCI material outside of the local installation. This additional logistic constraint required a crypto fill device for reloading the keys once aboard Camp Roberts. Since these devices are extremely hard to come by our research group was not able to sufficiently acquire a device for the duration of the exercise. Therefore, we were dependent on the good graces of our tactical radio vendors CYZ-10. Refilling the radios cost us about a half day’s work.

Lack of support

Technical support for some of the equipment including software was not readily available from vendors. The architecture initially designed required a last minute firmware upgrade on our tactical radios for the additional capabilities. However, this caused a domino effect effecting two and a half days of work.

Equipment problems

Black box equipment caused more confusion and troubleshooting hours. The majority of the equipment leveraged for this experiment was pulled from proprietary solutions. The delays directly resulting from this issue were evident when assuming a traditional approach. For example, the tactical radios have partial routing / switch functionality. This encouraged the idea of configuring the devices similar to our Cisco routers. As traditional network architectures are designed and established to thrive on dynamic configuration. However, the tactical radios are designed to be configured with mission plans beforehand, therefore, forcing a static mission plan / network configuration, inhibiting real-time adaptability.

Power supply inverter problems

The power supply calculation did not include the extra devices like the remote camera. Planners should budget extra padding for last minute equipment changes. We used a 700W inverter, which calculates to about six amps at 115 volts. Initially, we only calculated a requirement for three of the five amps. However, once we added the IP cameras (3 amp requirement) the inverters became overloaded. Therefore, we were forced to disconnect other devices accordingly. The connections to the batteries were alligator clips and these may be prone to intermittent connection variability. Another problem found was that the power supply would short out to the metal frame under the seats. A further problem was that the initial connection of the power supply inverter was made between two batteries in series and not one battery and therefore increasing the voltage (sum of two batteries) to dangerous levels.

VI. Conclusion

Our composite experience with TNT CBE 10-1 was overwhelmingly positive. While there were issues to overcome, it provided a great venue for exploring concepts in an austere environment. We plan to continue our participation and expand our efforts. The results from our exploratory research suggest cellular integration is feasible for missions not requiring emission security or classified content exchange.