Military Wireless Communications

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. Traditionally, the U.S. and Allied ground troops are briefed a mission order, allocated specific communication assets, and deployed to diverse austere environments. Since communication failures and compromises have increasing potential with mission importance, the level of sophistication is significantly geared toward security and reliability. Therefore, communication capabilities are limited to prevent expediential cost increases. Our research goal is to increase the communication capabilities, maintain security and reliability, and reduce the overall cost.

In an effort to reduce cost and increase capabilities, we are evaluating the feasibility of leveraging cellular technology. However, traditionally a cellular infrastructure is designed around a reliable land-based centralized architecture. As depicted below. The architecture is dependent on the Mobile Switching Center for cell phones to communicate.

Is this topology suitable for military application? For example, we could put the base stations in an air platform to provide a 15 mile radius cellular coverage area. We could attach these base stations to vehicles assigned to specific areas of operations. Lastly, we could install these base stations on our forward operating bases. However, the tradeoff is the dependency on the connections to the mobile switching center and the limited communication security inherent to cellular technology; limited in comparison to traditional military communications. There are many ways to mitigate the majority of these security limitations, but as security increases so does the cost.

Problem Statement:

What is the optimal solution for integrating the capabilities associated with typical smart phones into a secure and reliable wireless ad-hoc highly mobile tactical military communications network?

Questions to investigate:

Primary Research Question: Is it feasible, while maintaining cost efficiency and security integrity, to establish with a connection via a standard cell phone device to an ad-hoc wireless highly mobile tactical network with the ability to send data or voice across the attached wide area network?

Subsidiary research question #1: Is it feasible to create a secure wireless cellular network from a tactical radio network via standard military waveforms without significant hardware change or compromising military communications security (COMSEC) requirements?

Subsidiary research question #2: Is it feasible to create a secure wireless cellular network from a tactical radio network via an external 3G/4G bridge device without significant hardware changes to standard cell phones or compromising military COMSEC requirements?

Subsidiary research question #3: Is it feasible to wirelessly connect a cell phone to a dual mode / channel tactical radio via a Radio Frequency (RF) 3G/4G chip-set internal to the tactical radio?

Subsidiary research question #4: Which of the three topologies listed as question 1, 2, and 3 are more effective in delivering information to end host?

Subsidiary research question #5: Is it feasible to create an ad-hoc wireless network of cell phones without the attachment of cell towers (i.e. using mobile base stations instead)?

Subsidiary research question #6: Is it feasible to reprogram the radio stack onboard open source cell phones?

Subsidiary research question #7: Is it feasible to reprogram the radio stack onboard inherent tactical radios to integrate a cellular stack?

Subsidiary research question #8: What limitations arise for the tactical and cellular wireless links in realistic operational channels (fading channels with Doppler effects)?

Subsidiary research question #9: What capabilities does the cell phone bring to the network?

Subsidiary research question #10: What is the data throughput for each of the proposed topologies?

Subsidiary research question #11: What communication security issues develop?

Subsidiary research question #12: Of the new security vulnerabilities, what actions can be taken to minimize risk?

Subsidiary research question #13: What are the disadvantages / advantages of the traditional MSC-BSC architecture (centralized approach)?

Subsidiary research question #14: What are the disadvantages / advantages of the independent modular mobile base station and tactical radio combination (decentralized approach)?

Subsidiary research question #15: What modulation and/or coding techniques should be considered when designing the next generation WNW and/or SRW for JTRS?