SDR STRATEGIES FOR INFORMATION WARFARE AND ASSURANCE

Scott Chuprun, Chad Bergstrom, and Dr. Bruce Fette
Motorola Systems Solutions Group
MS-R2202, 8220 E. Roosevelt, Scottsdale, Arizona 85257
Phone: (480) 441-4542, Fax: (4802) 441-2584, Email: Scott.Chuprun@motorola.com

ABSTRACT

As software defined radios (SDR) proliferate and the capability and functionality of radios expand, the opportunities for attack by either side increases. Modern networks are evolving into a combination of wired, wireless, and Internet components with attacks possible on any component against any other component. Understanding those attacks to identify vulnerabilities and formulate defensive approaches is the first step in a comprehensive system design. Furthermore, a complete understanding of adversarial vulnerabilities enables development of offensive strategies that leverage the power of Network Centric Warfare (NCW). Computational capabilities of emerging SDRs provide the means to coordinate attacks against the adversary. Further, these capabilities will enable new methods for overcoming classical attacks against the terrestrial, UAV, and Satcom information systems. Part of the protection strategy for these systems will require that classical Information Assurance (IA) techniques be distributed to various SDR nodes within the infrastructure.

INTRODUCTION*

The starting point for developing both defensive Information Assurance (IA) and offensive Information Warfare (IW) techniques is an understanding of the various component and network vulnerabilities. These attacks run the gamut from brute force physical attacks such as jamming, to more sophisticated network and higher level attacks, such as man-in-the-middle attacks that simulate network management commands. By evaluating these attacks against coalition force and adversarial systems, we can develop a catalog of potential vulnerabilities. For coalition systems, we can then develop appropriate countermeasures to harden the systems against the discovered weaknesses.

Because of the interconnection of wired, wireless, and Internet components, the attacks considered are not restricted to classical radio attacks but must include the plethora of computer network attacks that are continuing to evolve. Figure 1 illustrates several wireless and wired links supported by the SDR systems that could provide opportunities for intrusion. Attack detection, attack response recovery mechanisms, and quantitative performance assessment metrics can be developed to indicate the relative performance of each network subsystem. This assessment can be entered into an appropriate database, to allow real time quantitative recommendations to be provided to the network security manager.

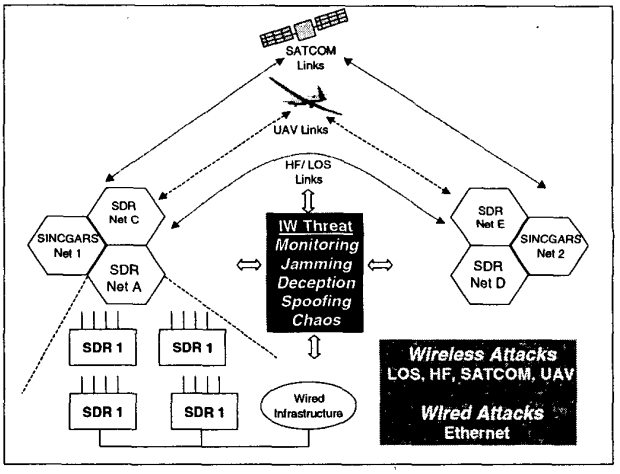

Figure 1. Wireless and Wired IW Attacks on SDR

Motorola's WITS Model 6004 is an example of a SDR that has the capability to detect and carry out IO / IW / IA. Illustrated in Figure 2, the 6004 SDR provides a 4 channel full duplex gateway, with interoperability between existing legacy products and new communication systems, and also serves as a router for data distribution over wireline and wireless paths [1]. Without changing hardware, the Model 6004 provides a programmable frequency range from 2 MHz to 2 GHz, including receive capability from 0.1 MHz to 2 MHz. The DMR Ethernet ports allow local networks to be formed and enables remote control with a laptop HMI.

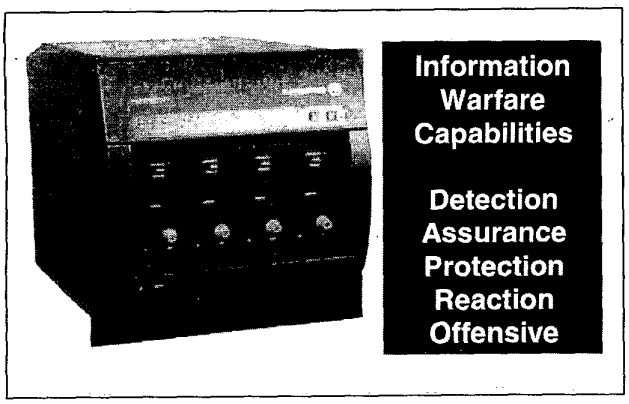

Figure 2. Digital Modular Radio (6004) IO/IW/IA

IW Wireless and Wired Attack Scenarios

Legacy wireless networks are a likely target of adversary attacks against our communications infrastructure. The SDR will provide protection against adversarial wireless attacks and the means to launch attacks against the adversary. Traditional IW attacks concentrate on the waveform physical layer by matching the jammer type to the radio target. New jammers may include smart strategies that focus on disruption of specific waveform segments, file or command insertion, and ethernet local area network intrusions.

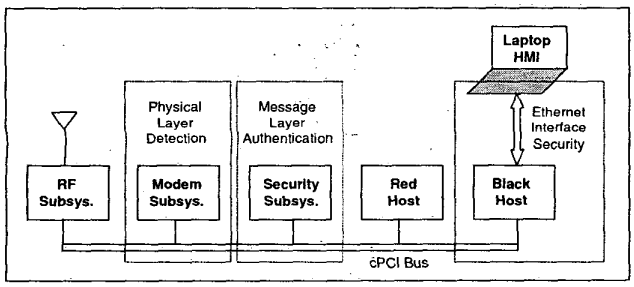

Figure 3. Fundamental SDR Subsystem IW Detection

Wireless attacks can occur on specific waveform fields such as initial synchronization, crypto synchronization, address information, message packets, or on CRC postambles. Wired attacks can occur if a computer has access to the internal LAN or the controller HMI is contaminated by a file or virus. Careful subsystem design, bus access control, message authentication, and physical LAN security are key to SDR IW protection and detection. The basic elements of a SDR system are shown in Figure 3, which highlights three areas involved in IW subsystem protection: *1) Physical Layer Detection, 2) Message Layer Authentication, and 3) LAN Ethernet Security*

Physical Layer Detection

These attacks can be reduced or mitigated in the future during waveform design efforts. Specifying waveforms with processing gain options for frequency hopping, spreading, and interference suppression are methods of protecting the SDR from RF jamming [2,3]. Multiple access methodologies may be exploited to provide enhanced protection against physical layer adversarial attack. For example, frequency hopped systems can elude most follower-jammers by hopping at rates in excess of 3 Khop/s [4,5,6].

As such, SDR networks must be designed with the flexibility to minimize the opportunities for successful enemy action or disruption. This includes providing multiple modulation formats, frequency bands, and algorithms that randomly change the active combination, but also adding intrusion attack detection and sender verification algorithms. Computational complexity must be considered at each design stage to trade off protection level with system resource loading [7]. In addition, message verification provides early detection before the data moves up the protocol and application stacks.

Currently, the SDR is capable of providing protection from jamming for legacy waveforms that have inherently inadequate antijam capabilities. The SDR has the sensing capability to determine jammer signal characteristics, quantity of simultaneous jammers, waveform segments being targeted, and location or direction of arrival. This information can be communicated to the radio network to decoy or elude the jamming threat, thus strengthening existing legacy and commercial systems.

In response to sophisticated attacks on legacy systems, it is feasible to build attack detection capability into SDRs or into the network infrastructure to enable information assurance for legacy wireless network systems. The network infrastructure approach is the more convenient way to retrofit legacy wireless networks with attack detection and response methodology. Furthermore, the infrastructure approach offloads the high power and computational burden requirements of broad spectral analysis, multiple channel demodulation, and pattern matching. In some cases these detectors find discrepancy in "reported versus expected" characteristic, in authentication code, or some other metric of the received signal. A well designed system must minimize error rate and know the level of the residual errors in the real world due to motion dynamics, multipath, noise, friendly co-site interference, and unintentional interference of commercial radio service. As part of the detection proc-

ess, multiple SDRs can coordinate TDOA and AOA information to determine location of the hostile source. This information can be used to for antenna steering control strategies and offensive responses.

In addition, powerful new sub-modulation features can be developed, which can convey user authentication certificates. By evaluating these attacks against SDR waveforms and the adversary's radios, we can develop a catalog of offensive and defensive strategies. For our own systems, we can develop appropriate countermeasures to harden battlefield systems.

Message Layer Authentication

A critical SDR design element is authentication of incoming or out going messages and isolation from vulnerable Red and Black Host subsystems. When any message is received it must be validated by the Security Subsystem as a valid net member with exact crypto synchronization. This normal screening process will eliminate most IW attempts to control or spoof coalition systems. Only playback jamming or active radio capture scenarios can pass the proper cryptographic security functions. At this point additional checks (e.g., time-of-day, direction-of-arrival, signature sync. etc.) must occur to validate the message or command structure against the source and network mission objectives. It is also appropriate to run virus checks at intermediate points within the coalition system. Detection of old time stamps, old sequence numbers, or failed authentication can also reflect various attack methodologies. Detection occurs at the FEC processor or the crypto-processor. Failure to acquire vocoder sync or failure to synchronize video or data compressors indicates failures higher in the protocol stack. The application layer may report application errors, such as failure to parse messages, incorrect or incomplete messages, out of sequence messages, or completely inappropriate messages for the current active state.

Ethernet LAN and HMI Security

The SDR includes Ethernet ports that are designed to enable remote control and to support LAN connectivity. Normally, at battlefield TOCs or within a Navy vessel, the connecting cables are in a protected environment that prevents unauthorized access to the network. The SDR architecture shown in Figure 3 allows the HMI running on a laptop computer to control the SDR configuration on each channel. The system security measures prevent entry into this HMI network. It is not sufficient to authenticate the computer sending commands or extracting information, but it is equally important to protect against files entering and launching within the authorized controller. As files are stored on the HMI it is important to run virus checks and determine the file status.

IW Event Processing and Management

IW events occurring at any subsystem produces an audit message, which should be delivered to the network manager. Detailed audit reports can provide evidence of attack methodologies, range of capabilities, and objective or purpose of the attack. This information can provide the network security manager with data to make an informed selection of management and recovery process. It is recommended that network recovery strategies be delivered over covert networks dedicated to network management.

At the completion of an attack analysis phase, quantitative performance assessment metrics must be computed to indicate the relative performance of each subsystem. The subsystem performance database allows real-time quantitative recommendations to be provided to the network security manager. The network security manager control will be distributed between the SDR dynamic management functions and a rear echelon manager. The rear manager has a display of ongoing attacks and hyperlinked data regarding the sequencing of the attacks, vulnerabilities, damage inflicted, possible objectives, possible recovery strategies, and likelihood of recovery (if a specific recovery process is selected), and associated collateral damage.

Since not all attack evidence will be the result of true IW attack, some of it may reflect spectral fratricide or misuse [8]. Fratricide data can be passed to the network spectral manager for prioritization and resolution. Identified spectral holes and overcrowding can be identified, and the SDR networks can be semi-automatically commanded to minimize fratricide [9]. Misuse can result in immediate security audit reports.

Emphasizing the importance of spectrum issues to the Military, in 1998, the DoD established the Spectrum Management Directorate and the Office of Spectrum Analysis and Management (OSAM) [10]. Even for nonmilitary applications, automated spectrum management using SDR technology is receiving attention from government regulators [11].

IW Spectral Monitoring

Software defined radio systems will provide significantly increased functionality and flexibility relative to prior-art communication system paradigms [12]. These programmable open radio systems will enhance information flow on the digital battlefield by enabling new situation awareness and spectrum analysis benefits to mounted and dismounted units. This technology enables fusion of traditional communication functions and signal intelligence functions in a single architecture that provides comprehensive signal analysis. SDR embedded tactical functions will enable threat assessment applications, including noncooperative RF sensing, intelligence gathering, and hostile emitter time difference of arrival (TDOA) and geolocation [13].

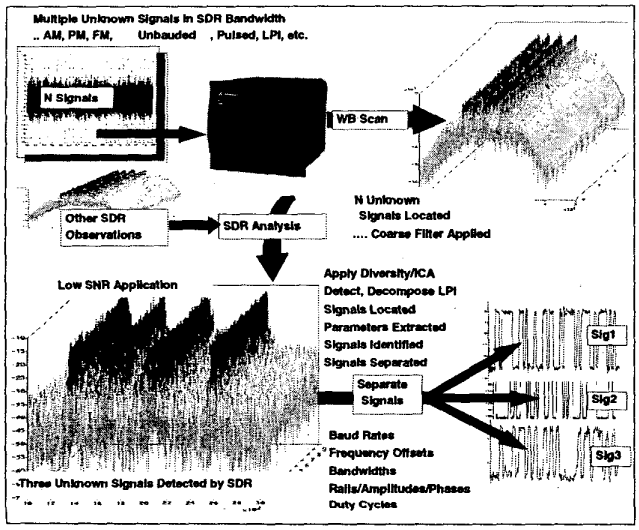

Figure 4. SDR Spectrum and Signal Parameter Identification Capabilities for IW Monitoring

This approach can even be extended to identify and verify expected signals within the band of interest with emitter tags, such as SINCGARS, cellular, Have Quick, EPLRS, Satcom, broadcast, GPS, pager, JTIDS, and MSE. Data of interest may also include network identification tags, such as 'friendly', 'commercial', 'hostile', or 'unknown'. These emitter analysis modes will provide commanders with expanded situational awareness in tactical environments, improving the chances for mission success. Figure 4 shows multi-signal observation data detected by an SDR based wideband scan function, and the resulting filter process that isolates the region of interest (ROI) for further analysis.

Near real-time signal processing may be applied to this region to determine candidate signals of interest.

Each candidate signal must be identified and separated from the composite observation to isolate the data for further parameter extraction. In addition to single antenna signal separation methods, approaches that exploit antenna diversity can be applied to provide detailed spectrum data [14,15]. Signal parameter extraction algorithms will estimate signal information such as power level, bandwidth, duty cycle, and center frequency (offset). This information is used with detection-based spectrum correlation to select the correct domain for baud symbol synchronization and extraction, resulting in an estimate of the original data stream, and baud rate information for each candidate signal within the band of interest. If the detector can have sufficient awareness of all friendly theatre networks, and can have a way to recognize friendly communications, then false positives can be suppressed. This will leave the remainder as intentional and unintentional detections due to noise and due to the adversary.

Offensive IW Techniques of SDR

The SDR can be configured to either jam the enemy's node or to emulate the node and thus become the "man-in-the-middle" providing misinformation. SDRs can provide additional mapping capability to more precisely locate adversary nodes and nullify them through jamming or specific radio or network attacks targeted to the specific type of equipment and software use. Also, because of the flexibility in format and modulation bands and techniques, it can be used to optimize the SDR communications waveforms to maximize the impact of classical or new sophisticated adversary jamming. Through the capability of the reconfigurable assets on the SDR, selection among the variety of possible options can be satisfied with the same equipment, operated in different modes.

The multi-platform aspect of SDR provides platforms that can, simultaneously with the communications mission, intercept and locate high priority targets. The SDRs provide the ability to analyze the intercepted waveform and provide the ability to do multi-platform geolocation. These assets in combination provide a detailed description of the target. The response (IW attack) can take on several forms. Part of the assets will continue to intercept the target node. Other assets can (1) jam totally or surgically within the target infrastructure, (2) provide misinformation to either or both nodes of the enemy net.

Reaction

When attacks are detected, the system must have the means to command changes in operating band and modulation to avoid or mitigate the attacking threat. It also must have the ability to steer antenna nulls in the direction of the attacker and refine the routing tables to assure that messages from valid systems continue to maintain full connectivity. In addition, the systems must be able to respond to information-style attacks that attempt to subvert operation and data in the radios.

Conclusions

This paper presents the versatility of the SDR and develops IW/IA/OI concepts for integration into these battlefield communications systems. The SDR offers the ability to better control and coordinate the total battlefield information assets to obviate or minimize the impact of enemy action such as jamming.

The wireless IW attack capability can be implemented for ground troops, navy vessels, and other forces to provide an effective IA capability. This capability provides for the secure operation of friendly forces in the face of enemy action and for the secure segregation of information among coalition partners with different levels of authorized access.

Also proposed are functions and subsystems that increase the IW capability for battlefield communications systems. Described in this paper are the concepts on which to base the formation of passive IW collection and offensive Information Warfare attacks against adversary systems.

The wireless IW attack capability can be implemented for ground troops, navy vessels, and other forces to provide an effective IW remote capability for the Army, Air Force, Navy, Marines and SOF. For example, ground troops could one day have a wearable computer with multiple peripherals and antennas for launching IW attacks from the front lines or special ops positions using the ACN platform. Navy vessels could expand their current wireless communications, sensors, and networking infrastructure to include these concepts as well. The Air Force could incorporate this with their other sensor platforms to provide support to their tactical elements.

References

[1] "Software Redefinable Communication System Model 6004", Spec. Sheet, Motorola, September 1998

[2] S. Chuprun, C. Bergstrom, "Interference Resistant Modulation Using Transform Domain Processing", Proceedings, RAWCON '98, Colorado Springs, Co, USA.

[3] C. Bergstrom, S. Chuprun, D. Torrieri, "Anti-Jam and Spectrum Awareness Processing For Frequency-Hop Transceivers", Proc., 3rd Annual Fedlab Symposium, Feb 2-4, 1999, College Park, MD.

[4] D. Torrieri, "Frequency Hopping and Future Army Mobile Communications", *Proceedings, ATIRP Annual Conference*, University of Maryland, 1997.

[5] D. Torrieri, "Fundamental Limitations on Repeater Jamming of Frequency-Hopping Communications", *IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, May, 1989.*

[6] U.S. Government, "Contractor's Design Handbook for Protecting RF Transmissions", Revision 1, July 1994.

[7] Susan Gilfeather and Scott Chuprun, "Complex Arithmetic Processor Performance Metrics on LPI Waveforms", *MILCOM '95 Classified Proceedings*, November, 1995.

[8] J.C. Capps, "Systems Engineering Lessons Learned During The Task Force XXI Advanced Warfighting Experiment", 01 July 1997.

[9] C. Bergstrom, S. Chuprun, D. Torrieri, "Adaptive Spectrum Exploitation Using Emerging Software Defined Radios", Proc., 3rd Annual Fedlab Symposium, Feb 2-4, 1999, College Park, MD.

[10] Defense Information Systems Agency Office of Spectrum Analysis and Management, http://www.disa.mil/d3/depdirops/spectrum /index.html.

[11] R. E. Shrum, "Software Defined Radio (SDR) Spectrum Management and Policy Implications", FCC Technological Advisory Council, Spectrum Management Focus Group, August 20, 1999.

[12] "Operational Requirements Document (ORD) for Joint Tactical Radio (JTR)", http: // www.dtic.mil / jcs / j6 / jtr23_mar.html.

[13] C. Bergstrom, S. Chuprun, B. Verhoven, D. Torrieri, "Computationally Efficient Spectrum Analysis and Interference Decomposition For Advanced Manpack and Handheld JTRS Applications", Proc., ATIRP Symposium, March 2000.

[14] K. Torkkola, "Blind Signal Separation In Communications: Making Use of Known Signal Distributions", Proceedings, 1998 IEEE DSP Workshop, Bryce Canyon, UT, August 10-12, 1998.

[15] K. Torkkola, "Blind Separation of Radio Signals in Fading Channels", Advances in Neural Information Processing Systems 10, Denver, MIT Press, Dec. 1-6, 1997.