COMMON SOFTWARE DOWNLOAD REQUIREMENTS FOR SOFTWARE DEFINED RADIOS

John Polson (General Dynamics Decision Systems, Scottsdale, Arizona, USA; john.polson@gd-decisionsystems.com); Eric Christensen (General Dynamics Decision Systems, Scottsdale, Arizona, USA; eric.christensen@gd-decisionsystems.com), Byron Tarver (General Dynamics Decision Systems, Scottsdale, Arizona, USA; byron.tarver@gd-decisionsystems.com), and Steve Gifford (General Dynamics Decision Systems, Scottsdale, Arizona, USA, steve.gifford@gd-decisionsystems.com)

ABSTRACT

Benefits of a Software Defined Radio (SDR) include the flexibility and reconfigurability to accommodate a wide range of features, functions, and capabilities. Infrastructures can support a greater number of services, and subscriber equipment can accommodate individual needs and requirements while maintaining a high Quality of Service (QoS). All of these features are possible while decreasing total cost of ownership for both the service provider and subscriber.

Software download, the protocol and transfer of configurations, features, functions, waveforms, or applications, is a key enabler to fully exploit the features and capabilities of a SDR. With the evolving standards for SDRs it is important to take into consideration all aspects of use cases for software downloads. This paper addresses some of the key issues for consideration in the military environment for use of SDRs. The majority of requirements for SDRs in the commercial and military sectors are identical but not necessarily for the same reasons. A robust protocol with considerations for the military market is a focus of this paper.

Commercial and military security concerns merit attention. Both sectors have a lot of the same fundamental requirements. For example, both commercial and military systems require mutual authentication, on the commercial side to fight fraud and on the military side to fight denial of service attacks and espionage. Both systems require privacy, capability exchange, non-repudiation exchange, and initiation by infrastructure or subscriber.

Additional requirements are needed in a military system that may be useful in a commercial system. Support for special usage in a community of interest and detection of rogue behavior including scripted responses to that behavior are needed. Complete download path authentication (all nodes) is needed in a military networked SDR environment to mitigate information warfare attacks and ensure integrity. It is important in a dynamic military environment for a client and server to handshake after re-acquiring a link and pick up about where they left off in the download process. Additionally, high assurance simplex delivery is necessary in defense situations where radio silence is required. Disadvantaged users in the military typically operate well below the commercial level of acceptable and tolerable communications. The disadvantaged user also influences the software download requirements. Finally, joint and coalition mission planning requires software download support.

1. INTRODUCTION

Software-defined radios (SDRs) are the “PC” of the communications world. While SDRs are still in their infancy and their growth may never be as explosive as personal computers, they still have the flexibility and adaptability that comes from von Neumann computational engines supporting high-level languages. Two definitions of software-defined radios follow:

Software-Defined Radio. Software defined radios are elements of a wireless network whose operational modes and parameters can be changed or augmented, post-manufacturing, via software [1].

Software-Defined Radio. A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions [1].

The benefits of a software-defined radio are flexibility and reconfigurability. A waveform is a collection of choices in a transmitter, a receiver, and a common protocol that enables the transfer of information. A software-defined radio may easily change waveforms by changing the choices. Modulation may be selected from at least AM, FM, PSK, and QAM. Forward Error Correction may be selected from at least the following: none, convolutional codes, block codes, or Turbo codes. Interference suppression filters, equalizing filters, VoCoders, connection oriented or connectionless links can all be specified through software. This reconfigurability allows a single SDR to support numerous waveforms and communicate with numerous legacy radios.

SDRs are flexible and can, in general, support any software application. Such applications include but are not limited to: databases, e-mail, and signal processing. The growth of multi-mission applications hosted on SDRs is expected to accelerate.

SDRs support legacy waveforms and are capable of supporting as yet undefined waveforms. As new features, functions and capabilities are deemed desirable; the same hardware can support them through software only changes. This lowers the cost of hardware upgrades by reducing the frequency of actually acquiring new hardware.

The total cost of ownership is reduced through the use of software-defined systems. Less frequent hardware upgrades, fewer sets to acquire, and fewer models of hardware for vendors to develop and support reduce costs for both the subscriber and service provider.

Quality of Service (QoS) is maintained through adaptive protocols, and the ultimate adaptation is total reconfiguration of the radio through the use of SW download. As new QoS enhancing techniques are developed and implemented, QoS improves when the software is distributed or updated.

There are differences between commercial and military SDRs. A military SDR is commonly partitioned into red and black security domains while the commercial SDR is not. The black side is where the RF and MODEMs are located and is considered insecure. The red side(s) is considered secure at some level. The level of security is determined somewhat by the structure of the radio but primarily by the encryption procedures associated with the data being transformed into and out of that red side. Between the black side and the red side is usually a cryptographic engine. In a true SDR, the cryptographic functionality is also defined in software.

In ever-changing environments, objectives sometimes are modified. When objectives change, the capabilities of a RF Spectrum resource such as a SDR may be non-optimally configured. Software download allows a mission planning infrastructure application to better optimize the software configuration of many SDRs dynamically. For example, when changing from a holding force to an attacking force, the mission planning infrastructure may wish to have certain elements use low probability of detection (LPD) waveforms and can download to them the appropriate software just before the mission commences. In the commercial sector, if a new office building is erected a service provider may wish to upgrade the code division multiplexing factor of a subscriber's equipment.

2. SOFTWARE DOWNLOAD

Software download is the protocol and transfer of information (configurations, features, functionality, waveforms, or management directives). Software download enables SDRs to fully exploit their features and capabilities. Software download includes software installation through direct physical contact (CD, land network) or over-the-air.

Over-the-air software download utilizes radio links to download information and is the primary topic of this paper. Three classes of software download, from smallest size to largest, are: transfer of a parameter set, transfer of a protocol stack, and transfer of a full application.

2.1. Software Download Protocol

Figure 1 shows the commonly accepted sequence diagram for software download [2], [3], [4], [5], [6], and [7]. It is assumed that either a pilot channel or an existing channel is utilized for the handshaking and information transfer required. Generally, a software download is a pull request or a push request generated by the client or server respectively. The download begins after mutual authentication and capability checks are performed. Once a complete and 100% accurate download is successful, installation and testing are done. The last step of the over-the-air software download is a non-repudiation exchange. The motivation for these steps is discussed in Section 2.4.

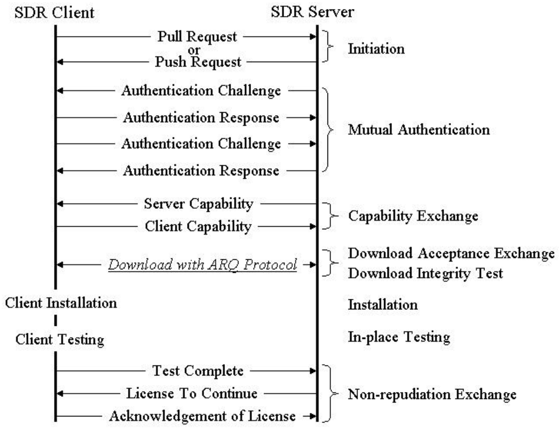


Figure 1 - Sequence Diagram of Software Download Protocol - Commercial and military over-the-air software download use the same protocol framework

2.2. Commercial Use Cases

Figure 2 shows three use cases associated with commercial over-the-air software download. These three cases are typical but clearly not exhaustive. Use cases i, j, and k are described below.

In use case i, the service provider has a new version of waveform A and wishes to propagate it to the subscribers. A request from the System Administrator initiates a push software download. The subscriber may or may not be required to approve the new installation.

In use case j, the subscriber requests the installation of waveform X. This causes a pull software download that may or may not be approved by a System Administrator.

In use case k, the subscriber changes his options on his SDR. This initiates a pull software download of the appropriate set of parameters.

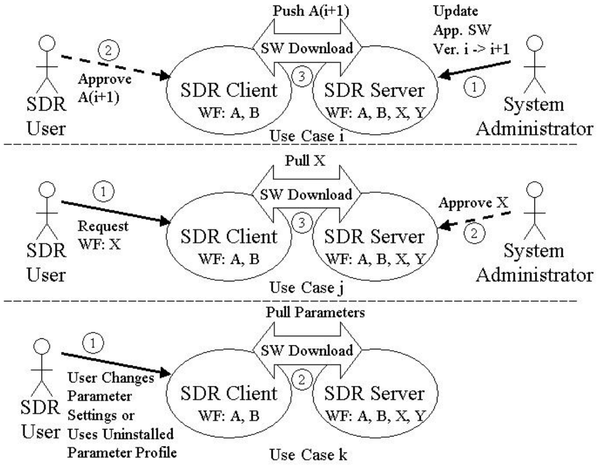


Figure 2 - Three Commercial Software Download Use Cases - Push and pull initiated downloads are optionally approved by the Client or Server's users and vary in size

2.3. Military Use Cases

Figure 3 shows three use cases associated with military over-the-air software download. These three cases are typical but clearly not exhaustive. Use cases l, m, and n are described below.

In use case l, the commander wants all his communications to change to a different waveform at a certain time. He requests a push of that waveform with an inhibit before the switch over time or an enable after the switch over time. The user simply changes at the right time automatically.

In use case m, the user wants to join a community of interest such as a special operation communications channel. This generates a request for a parameter set that when authorized is pushed to the user's SDR.

In use case n, the user attempts to utilize a waveform that is not installed and an automatic pull from the server is accomplished. This may happen in real-time (on-demand without noticeable latency).

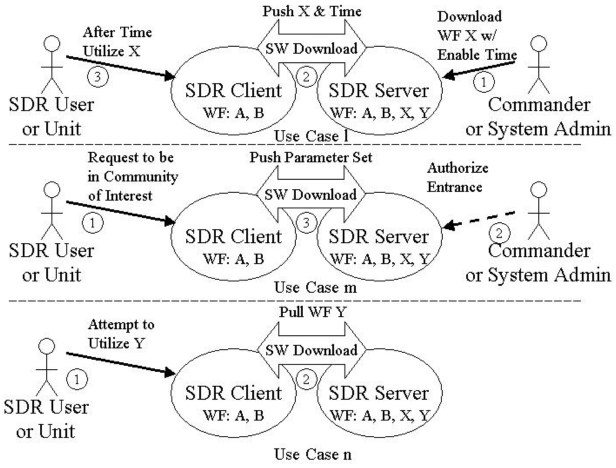
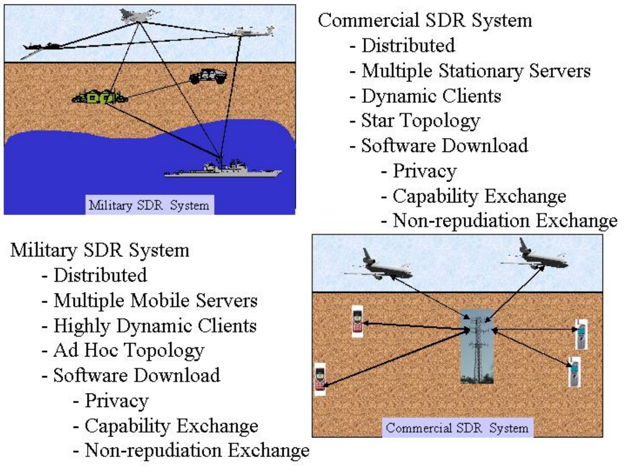


Figure 3 - Three Military Software Download Use Cases - Over-the-air software download protocol for military use is the same as for commercial use but has support for special usage

2.4. Comparison Of Requirements

Figure 4 shows a comparison between military and commercial SDR systems. They are more alike than they are different. Of course, the waveforms utilized are somewhat different, and the cryptographic support for operational use is higher in a military system.



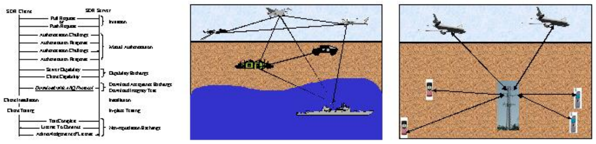


Figure 4 - Military and Commercial SDR Environments - While military and commercial SDR environments utilize the same point-to-point software download protocol; they do have different topologies

Requirements for SW download are the same for commercial and military systems, but the motivation for these requirements are different. Figure 5 summarizes the unique motivations for the common requirements of over-the-air software download.

Software downloads are initiated through either a pull request from the SDR Client or a push request from the SDR Server. Military and commercial systems should support both initiations to increase flexibility.

The client and the server want to mutually authenticate. In the military world, a client does not want to download potentially malicious software from an enemy server and military server does not wish to provide software to an enemy client. In the commercial world, authentication is performed to reduce fraudulent use of the communication system.

Capability exchange is performed in both worlds to avoid a software download that will not execute on the SDR Client. This maximizes responsiveness of the server by conserving resources.

Finally an over-the-air software download begins and an ARQ Packet Protocol is utilized to ensure a 100% accurate image is delivered. This is required for correct operation. In a military environment where handshaking is not possible due to radio silence requirements a simplex delivery may be required. This is discussed in Section 3.5.

Military and commercial systems install and test the download and a final non-repudiation exchange is conducted. The non-repudiation exchange provides billing evidence for the commercial side, and provides assurance that the download has taken place correctly for the command authority.

It is clear that basic military and commercial software download requirements are the same. A standardized over-the-air software download protocol is practical.

Capability	Military Motivation	Commercial Motivation
Mutual Authentication	Avoiding IW Attacks	Avoiding Fraud
Capability Exchange	Minimizing Response Time and Maximizing Responsiveness	Minimizing Resource Utilization
Download Acceptance Exchange	One or more correct copies of each packet with high probability for simplex delivery or ARQ Protocol for minimal retransmissions	ARQ Protocol for minimal retransmissions
Download Integrity Testing	Integrity required for operation	Integrity required for operation
Installation	Required to operate	Required to operate
In-place Testing	Minimizing Dropped Messages Under Newly Installed Capability	Customer Satisfaction
Non-repudiation Exchange	Command Responsibility	Billing

Figure 5 - Motivations for Protocol Attributes - Military and commercial software download protocols use the same framework but for different reasons

3. MILITARY SOFTWARE DOWNLOAD

There are several considerations that benefit military users and may benefit commercial users. Special usage for a community of interest, detection of and response to rogue behavior, download path authentication, resumption of interrupted downloads, simplex delivery, and joint coalition mission planning are discussed below.

3.1. Special Usage In A Community Of Interest

A definition of *Community of Interest* is: a subset of the available parties in a communication system with common communication requirements is a community of interest.

Support is needed for the following: creation of a community, deletion of a community, addition of user to a community, and removal of a user from a community as mission parameters dictate. For example, a military operation may have three small units that need to talk during infiltration including the transportation unit. When the operation is active, the transportation unit should be excluded from the communication network and a control unit added, and during exfiltration a transportation unit may join the community of interest. An example of a commercial community of interest is a taxicab company that wishes to provide dispatch radios on a point-to-point basis along with cellular phone service to communicate with customers. This is a less dynamic community, but dynamic support is still required. One possible mechanism of providing this support is through the use of software download.

In a military SDR system, special usage criteria may be desirable. Requirements for software download special usage should be included. Some of these special usage cases are: only provide waveform during a certain time period such as from date 1 to date 2, only provide a waveform a certain number of times, only allow members from a community of interest to download a waveform such as by region, unit, certain destination, or by security clearance level.

3.2. Detection Of Rogue Behavior

In a hostile information warfare environment, it is important to be able to detect rogue behavior in a SDR system and disable it. This is particularly important to base stations and or download servers. The software download requirements should provide support for authenticated audit reports to be exploited to this end. The reports should include usage and installation information.

Scripted responses to improper behavior may include the download of a clean waveform to misbehaving SDRs, or the downloading of "malicious code" or offensive code that disables the SDR. Another alternative is a command to revert to an archived waveform.

3.3. Complete Download Path Authentication

Integrity of all communications is required in a military software download situation. Therefore, every node that handles the data should be authenticated.

This process makes a man in the middle attack more difficult. However, the software download has built in tamper detection features (integrity or signature) and these may be deemed sufficient.

3.4. Reacquiring A Lost Link To Disadvantaged Users

In a dynamic environment radio links may be intermittent due to a variety of factors. It is important for a client and server to handshake after re-acquiring a link and pick up about where they left off in the download process. A plausible software download size is approximately 15KB (see Section 3.5. for justification). At 2400 bps, the download time is about one minute. It is advantageous to pick up approximately where the download is interrupted to save bandwidth resources and to reduce latency.

For a disadvantaged user, it may be impossible to keep a data link intact for the whole download and resumption after reacquiring the link enables the completion of the download in poor conditions. The server should request the last known good download status and pick up from there. Flexibility for providing a list of missing packets should be considered. The client should provide an appropriate response with the requested information. The details of this handshake have not been specified. Additionally, picking up part way through a download with a different server may also be advantageous, but requires sophisticated service handover protocols.

3.5. Simplex Delivery

Certain military units requiring radio silence need a simplex delivery protocol. The three most important characteristics of such a protocol are redundancy, redundancy, and redundancy. Forward error correction is insufficient because, the probability of a packet error may be driven to a small value, but the probability of a download error is a function of a potentially large number of packets. Redundancy may be introduced by planned retransmission of each packet and a CRC on each packet to detect errors in the packet.

Assume a k = 7 and r = ½ convolutional error correcting code, QPSK modulation in AWGN, a packet error rate of 10^{-3} is achievable at a reasonable E_s/N_0 ratio. Simulation results are shown in Figure 6.

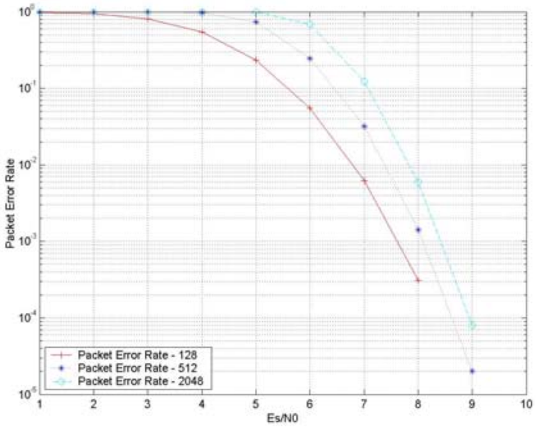


Figure 6 - Packet Error Rate - The packet error rate for three different packet sizes using a k = 7, r = 1/2 convolutional encoder and a QPSK modulation scheme in AWGN is shown

A reasonable download size, as estimated by the average executable size on several hand held computers (Palm Pilot and two way pagers), is 15 KB. For 2048 bit packets, there are 59 packets required for the data payload. Adding authentication and checksums etc. is much less than 10% and an exaggerated 100 packets is used as the download length.

The probability of message error, assuming independence between packets and retransmissions, is 10^{-3} * 100 or 10%, and sending each packet n times yields probability of success as ($1 - 0.1^{n}$). If n = 3, the probability of success is 99.9%.

If the data rate for the download is 2400 bps, the download time is about 4.3 minutes. While this is a simplistic analysis that warrants re-work, it clearly indicates the potential for a simplex delivery with operationally acceptable probability of error.

3.6. Joint And Coalition Mission Planning

Every modern military and every region acquires their own communication systems. When a traveler visits a new place, it is likely that his software-defined radio will not be using the same protocol or waveform as his destination. This incompatibility may be overcome by over-the-air software download.

When a coalition force is created, the communication systems of the different militaries are probably incompatible. Software download of legacy waveforms enables SDRs to communicate with local legacy equipment. This technology allows SDR equipped units to communicate with other units and to re-configure dynamically to support various missions.

During joint operations, server initiated over-the-air software downloads can be scheduled to be used to synchronize disparate SDR users to a common waveform. A pre-planned download is one mechanism possible, but dynamic user initiated concept of operations are also attractive. Selection of local preset configurations that have previously been stored is the most bandwidth efficient. Consideration for avoidance of orthogonal waveforms at a point in time warrants discussion.

A CINC may need to route data through an uninterested node as shown in Figure 7. For example, a SDR on a ship may be a router between users from another service. A joint mission planning approach is required and software download capability for pushing a waveform and enabling it is required.

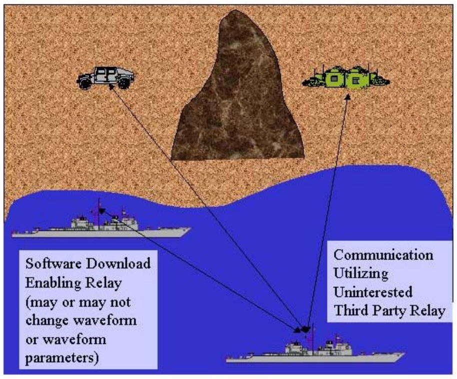

Software Download Enabling Relay (may or may not change waveform or waveform parameters)
Communication Utilizing Uninterested Third Party Relay

Figure 7 - Routing Through a Disinterested Party - A CINC may wish to enable beyond line of sight communications with an uninterested SDR acting as a relay between two or more units

SW Download enables distribution of a computational load necessary for highly complex tasks. SDR A may wish to accomplish a task that requires more resources such as memory or computation rate than SDR A has available. One example of interest to the military is signal processing functions. The application may be distributed among several SDRs by SDR A and the results collected at SDR A for interpretation. Another example may be distributed database functions.

4. CONCLUSIONS

Over-the-air software download is a powerful enabling technology. Added flexibility and lower total cost of ownership for both the subscriber and provider are the primary benefits of software downloading.

The fundamental requirements for military and commercial software download are the same, but the motivation for these requirements are different. The commercial systems are concerned with financial fraud and the military systems are concerned with denial of service and eavesdropping.

There are special cases in the military environment that warrant support for disadvantaged users, for simplex delivery, or for special characteristics of a waveform.

We believe that over-the-air software download will become a commonly supported feature for software defined radio systems in a reasonably short period of time.

5. REFERENCES

[1] SDR Forum. “Overview and Definition of Radio Software Download for RF Reconfigureation”. *Working Document SDRF-02-W-0002 Version 1.33* May 2002.

[2] Cummings, Mark and Steve Heath. “Mode Switching and Software Download for Software Defined Radio: The SDR Forum Approach”. *IEEE Communications Magazine* August, 1999.

[3] Jennings, Andrew and Neil Bryden. “Base Station Software Download and Management”. *SDRF-001-I-0018-v0.00 http://www.sdrforum.org* April 3, 2001.

[4] Farnham, Tim, et. al. “IST-TRUST: A Perspective on the Reconfiguration of Future Mobile Terminals using Software Defined Radio”. *Personal, Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on , Volume: 2 , Page(s): 1054 -1059 vol.2* 2000.

[5] Drew, Nigel J., Markus M. Dillinger. “Evolution Toward Reconfigurable User Equipment”. *IEEE Communications Magazine* February, 2001.

[6] Moessner, K. and R. Tafazolli. “Terminal Reconfigureability – The Software Download Aspect”. *3G Mobile Communications Technologies, Conference Publication No. 471* 2000.

[7] Jamadagni, Satish and M.N. Umesh. “A PUSH download architecture for software defined radios”. *Personal Wireless Communications, 2000 IEEE International Conference on , Page(s): 404 -407* 2000.

6. ADDITIONAL BACKGROUND REFERENCES

[8] Ralston, John D. "SDR Forum Proposal for Liaison with WAP Forum and MExE". *SDR Forum-Download Working Group* November 30, 1999.

[9] Rummler, R., et. al. "Traffic modelling of software download for reconfigurable terminals ". *P ersonal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium on , Volume: 1 , Page(s): 90 -94* Sept. 2001.

[10] "Before the Federal Communications Commission". FCC 00-430 December 8, 2000.

[11] Mehta, Mehul, Nigel Drew, and Christoph Niedermeier. "Reconfigurable Terminals: An Overview of Architectural Solutions". *IEEE Communications Magazine* August, 2001.

[12] de Boer, Gerrit, et. al. "User Requirements for Reconfigurable Mobile Communications". *http://www.ist-trust.org* August, 2000.