Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 703642, 9 pages
doi:10.1155/2012/703642

Research Article

Case Studies of Attacks over Adaptive Modulation Based Tactical Software Defined Radios

David Fernandes Cruz Moura, Fabricio Alves Barbosa da Silva, and Juraci Ferreira Galdino

Divisão de Tecnologia da Informação, Centro Tecnológico do Exército, Avenida das Américas, Prédio D10, Guaratiba, 28705 Rio de Janeiro, RJ, Brazil

Correspondence should be addressed to David Fernandes Cruz Moura, david@ctex.eb.br

Received 9 May 2012; Revised 9 November 2012; Accepted 25 November 2012

Academic Editor: Rui Zhang

This paper presents case studies of attacks aimed at tactical software defined radios based on a classification with the most common sources of vulnerabilities, classes of attacks, and types of intrusions that military radio sets may suffer. Besides that, we also describe how attack mitigation strategies can impact the development of SDR infrastructures. By using such approach, we identify several possible sources of vulnerabilities, attacks, intrusions, and mitigation strategies, illustrating them onto typical tactical radio network deployment scenarios, as an initial and necessary step for the definition of realistic and relevant security requirements for military software defined radio applications.

1. Introduction

In the past, military radio design was totally focused on dedicated electronic components. Afterwards, we have witnessed the appearance of software configurable radios (SCR), in which users have the opportunity to choose the most appropriate waveforms for different combat scenarios. In recent years, though, the development of radio communication technology solutions has been submitted to a huge paradigm change—the software defined radio (SDR) technology upspring, in which previously hardware-based features became software defined and users may also introduce new application waveforms on the fly.

Such progress is due to several enhancements in different areas like embedded systems, analog-to-digital converters, digital transmission, digital signal processing, multiband antennas, software architectures, and especially in novel General-Purpose Processors (GPP) evaluation capacity. Based on that, SDR foreshadows important consequences and advantages for the development of wireless solutions for military communications systems. Among the envisioned features, we can list interoperability, waveform portability, and the possibility to be updated with the most recent advances in radio communications without hardware replacement requirements. Moreover, SDR is envisioned as the most appropriate platform for cognitive radio development.

At a glance, the high level functional model of an SDR consists of a front end RF subsystem which performs channel selection, downconversion to baseband, and data forwarding onto a software-based processing unit, where the associated digital bitstream is submitted onto appropriate layers (e.g., data link, network, and security modules) to perform suitable decoding tasks to extract the desired information. This process is reversed on the transmit side, where the input signal is coded and a modulated signal bearing the associated information suitable for transmission is created. This signal is then passed to the RF subsystem for insertion into the wireless channel.

Due to the multitude of concepts related to the described functional model, several efforts have been done towards the standardization of key elements within the SDR architecture, providing a common platform for the development of SDR sets. The standards supported may be proprietary or

industry-developed through a consensus process—while the former approach brings product differentiation to manufacturers, the latter strategy deals with the technology as a commodity, allowing support by third parties in creating the radio platform to achieve specific business objectives.

One of the most typical areas of standardization is the application framework, which provides a common software operation environment, with vendor-free interfaces to set up, configure, control, and release application waveforms under operation on an SDR platform. Examples of application frameworks relevant to SDR systems include the Open Mobile Alliance, the Service Availability Forum, and the Software Communications Architecture (SCA), which is supported by the US Department of Defense.

The SCA standard was originally proposed by the Joint Tactical Radio System program (JTRS) [1–3], which is a program for the development of military tactical radios sponsored by the US Department of Defense. The SCA/JTRS standard is becoming the *de facto* standard for the construction of tactical military radios. Nowadays, the interest in the SCA goes beyond the military domain, since this standard has inspired academic and commercial projects [4].

However, among various trending topics for associated research and development efforts, there are several security issues associated with SDR set development that need to be addressed, not only for civilian users but also for military-driven stakeholders [5]. Such issues were dealt in several works available in literature and present related but distinct concepts, namely, attack, vulnerability, and intrusion.

An *attack* is a malicious action that aims to explore one or more vulnerabilities, subverting the system security policy. In this paper, we identify the person or organization performing the attack as the *adversary*. A *vulnerability* is a defect in the system (either in software or in hardware) relevant for its security [6]. The vulnerabilities can be classified as design, implementation, or operational.

Design vulnerabilities are introduced during system design. An example is to use weak encryption and signature mechanisms for secret data. Another example is a protocol design subject to replay attacks.

Implementation vulnerabilities are introduced during the manufacturing and delivery processes. This class of vulnerabilities can be divided into two subclasses: software implementation and hardware implementation vulnerabilities. An example of software implementation vulnerability is the lack of verification of the boundaries of a buffer, leading to buffer overflow vulnerabilities [7]. An example of hardware implementation vulnerability is the introduction of hardware trojans [8] during chip fabrication. Vulnerabilities related to the supply chain [9], like device cloning [10], are also included in this subclass.

Operational vulnerabilities are vulnerabilities caused by how the system is operated or is configured. One example is the use of weak passwords in authentication systems.

Finally, an *intrusion* is defined in [11] as a successful event from the adversary's point of view and consists of (1) an *attack,* in which a vulnerability is exploited, and (2) a *breach*, which is the resulting violation of the security policy of the system. Essentially, the authors consider two dimensions when classifying intrusions: intrusion techniques and intrusion results. So, we can state that an attack exploits a vulnerability and becomes an intrusion due to a security breach in the system security policy.

Several works available in the literature deal with SDR security aspects, and the associated mitigation techniques to overcome these flaws. In [12], the authors describe classes of vulnerabilities, threats, and attacks aimed at software defined radios application middleware (SCA). It also proposes a Radio Platform Security Architecture. However, this work focuses mainly on commercial and public safety radios. In [13], it is presented a threat analysis aimed specifically at the GNU Radio platform, handled as a case study for the process of threat modeling based on data flow graphs. In [14], classes of threats associated with 3G networks and security requirements related to these threats are listed. In [15, 16] vulnerabilities, threats, and attacks on WiFi devices (IEEE 802.11) are described. In [17], the requirements associated with secure SCA military radios, as well as high level security architecture and the corresponding security mechanisms, are presented. However, none of them present a study cycle comprising vulnerabilities, attacks, intrusions, and mitigation issues on a military-focused software defined radio.

Thus, the objective of this paper is to present case studies of attacks aimed at tactical software defined radios based on a classification with the most common classes of attacks on military tasks. By using such approach, we identify several possible sources of vulnerabilities, attacks, intrusions, and mitigation strategies, illustrating them onto typical tactical radio network deployment scenarios.

This paper is organized as follows. Section 2 provides definitions of attacks, vulnerabilities, and threats and also identifies vulnerability classes and several classes of threats, describing possible flaws in military scenarios. Section 3 presents several case studies of attacks for general tactical SDR sets. Finally, Section 4 contains our concluding remarks.

2. Classes of Attacks for General Tactical SDRs

In this section, we describe several classes of attacks that a tactical radio set can suffer. Our goal in this paper is to include the classes of attacks that we consider the most relevant, considering expected losses to legitimate users of the tactical radio network, and it is worth remembering that this classification is based on attack results.

The scenario for defining attack classes is of a radio set based on GPPs that implements waveforms that go up to the third OSI layer (network) and built on top of the Software Communications Architecture (SCA). Such SCA-compliant tactical radio set is part of a military radio network consisting of a finite and predetermined number of radios, depending on the combat echelon on duty [18]. The data transmission between two devices on the radio network always uses some form of encryption. The adversary can act externally to the radio network or can have direct access to the network by capturing one or more radio sets, with the loss being

Table 1: Attack classes, associated attacks (in bold) and vulnerabilities.

Attack classes	**Attacks**/vulnerabilities
Radio control	**Software injection** (i) Buffer overflow (ii) Waveform download vulnerabilities (iii) Start-up vulnerabilities
Personification	**Replay** (i) Protocol vulnerabilities **Authentication break** **GPS spoofing**
Unauthorized data modification	**Software injection** **Hardware injection** (i) Implementation vulnerabilities (ii) Hardware trojans (iii) Device cloning
Unauthorized access to data	**Hardware injection** **Software injection** **Traffic analysis attacks** **Side-channel attacks** **Fault-based attacks** **Social engineering attacks**
Denial of service	**Hardware injection** **Software injection** **Jamming** **Flooding**

Table 2: System performance comparison between authorized and spoofer stations.

Metrics	Actual AU	Expected AU	Spoofer
ASE (bps/Hz)	2.0385	2.0708	0.7264
PDP	0.0426	0.0266	0.6377
PLR	0.0427	0.0267	0.6413

unnoticed during a finite amount of time. The adversary has the ability to monitor all frequency bands used by the radio network. The adversary is also capable to intervene in the process of manufacturing and delivery of a limited, but crucial, number of components that compose the radio set. As stated in the introduction, the attacks considered in this paper target the radio set. Attacks aimed at other elements of the communication infrastructure (such as waveform download servers) are not included in the scope of this work.

Considering this scenario, the most important classes of attacks for general SDRs identified in [5], and their related attack techniques and vulnerabilities, are shown in Table 1, as a basis for our military-oriented analysis.

2.1. Radio Control. In the *Radio Control* class of attacks, the adversary aims to gain control of all or part of the radio set. This goal can be achieved through the injection of spurious or malicious software through the RF interface or via physical access to the SDR, using, for example, a local interface, altering the proper functioning of an SDR partition in order to compromise the system security, for example, by violating its security policy. Through radio control, an adversary can, for example, force the device to behave in a Byzantine, seemingly random, way.

The most common ways of introducing malicious code on an SDR are *buffer overflow* and *waveform downloading* [19]. The latter process introduces several important security issues [20], especially when malicious software is loaded instead of the original waveform. In this type of attack, the adversary may exploit vulnerabilities associated with the download protocol and the process of waveform instantiation on the SDR, changing the mechanisms that ensure code authenticity, integrity, and versioning. For instance, it may force a military network to operate with a nonoptimal waveform—for example, a waveform typically used for low-error rate channel conditions, as line-of-sight UHF low-mobility networks, may be downloaded for operation on a harsh environment, like a VHF ground-to-air multipath propagation channel or a non-line-of-sight VHF urban scenario, which would severely degrade a previously agreed quality-of-service level, in spite of being a previously authorized waveform.

The buffer overflow attack occurs when the adversary exploits buffer overflow vulnerabilities present in the system software to inject malicious code [7, 21], making the data stored in a buffer to exceed its capacity. There are two basic types of buffer overflow vulnerabilities: heap based and stack-based [6]. The heap based buffer overflow occurs when the buffer is located in the heap, which is the area of memory where dynamic data are stored. The stack buffer overflow occurs when the buffer is located in the stack, which is the area of memory where local data and return addresses of a function are typically stored. In military scenarios, buffer overflow attacks may degrade overall system performance, reducing application data traffic throughput, and levering global packet loss rate [22], which compromise previously agreed quality-of-service levels in combat radio networks.

The malicious software can also be embedded in nonvolatile memory used for initialization, during the radio set manufacturing process, or through physical access to the SDR. This type of attack is associated with vulnerabilities in the system start-up [8], which are generally related to the integrity verification of the start-up routines before execution.

For instance, malicious software may alter the transmission power level adopted by a radio set on a military network. Such modification does not keep the agreed communication to take place, but inserts vulnerabilities on allied communications, since it may allow an enemy force with electronic warfare capabilities to monitor, search, intercept, and decode unauthorized data.

2.2. Personification. For attacks belonging to this class, the goal of the adversary is to fool the radio set, or to introduce himself to the SDR as an entity belonging to the radio network or authorized to access it. In the *Personification* class of attacks, the adversary presents himself as another entity, different from the original. For example, an adversary can impersonate a server, a network, or a radio set or act as a man in the middle. An attack of this class can have several goals, for example, to access or modify information in transit,

to send outdated or invalid data to the SDR to reduce its functionality, or simply to allow the adversary to present himself as an authorized correspondent, gaining access or changing the SDR behavior.

This class of attacks can explore various types of vulnerabilities, often associated with protocols, and that may be also applied to typical military radio networks. For example, vulnerabilities in the data transmission protocol of a waveform may allow replay attacks [12]. In the replay attack, the adversary captures a copy of the transmitted information and relays it later, and it can be exploited, for example, in any SCA-compliant data transmission waveform that does not implement sequence numbers, challenges, or a freshness scheme [23]. An example of a waveform that allows replay attacks is the IEEE 802.11-WEP [24]. Replay attacks can also be used to distribute obsolete waveforms (possibly with known vulnerabilities), which were previously stored by an adversary, for several radio sets belonging to a radio network.

If the SDR deploys waveforms that require some form of authentication between devices, another type of attack can occur if the authentication protocol contains vulnerabilities. Examples of waveforms with authentication vulnerabilities are several implementations of IEEE 802.11 (WiFi) including WEP, WPA-PSK, or EAP/LEAP [32].

Several radio sets implement internal geolocators. Examples include military radios (SCA compliant or not) and cognitive radios. One of the easiest ways to implement a geolocator is via a civilian GPS receiver, which can also be set by software in an SDR. GPS receivers may be subject to an impersonation attack known as GPS spoofing, which consists of sending wrong location signals to a receiver position [13]. These attacks are relatively simple to perform in civilian GPS receivers, since these receptors do not implement countermeasures against such attacks. In fact, impersonation attacks on civilian GPS receivers can be performed even through commercial GPS signal simulators. However, this simple attack is also the easiest to detect. More sophisticated attacks require the use of portable receiver-spoofer devices [13]. This latter attack can be done by a single device or a set of coordinated devices.

2.3. Unauthorized Data Modification. This class includes attacks that alter the data being transmitted by the radio set. In this case, the adversary aims to modify data that is stored or transmitted by SDR. The unauthorized modification of data or software can impair the security or functionality of the radio set. This class of attacks includes the possibility of unauthorized modification of internal parameters of a waveform. So, it may alter different radio set features, like a protocol internal configuration setup, a control data flow, or even a user-driven message data that is under transmission, compromising military network security and performance.

The unauthorized modification of data can also be performed by exploiting vulnerabilities in hardware. A processor is usually described in about 500 000 lines of VHDL code, which usually are not submitted to a formal verification process. Thus, it is expected that a processor may have multiple vulnerabilities that can be exploited by an adversary. Attacks can also make use of vulnerabilities introduced deliberately by an adversary. An example of vulnerability introduced by the adversary is the hardware trojan [16]. A hardware trojan is a deliberate, malicious, and difficult to detect hardware modification in an electronic device. The hardware trojan can modify the functionality of an integrated circuit and undermines the system reliability and security. For example, we may consider a cryptographic processor that normally sends encrypted data to an output. When the trojan is active, the encryption is disabled and the data is sent in clear, without the system operators' awareness [16].

2.4. Unauthorized Access to Data. The attacks of this class seek sensitive internal data and information, without modifying them. Unauthorized access to information can be done by exploiting several vulnerabilities, such as those related to the injection of malicious code and the use of hardware trojans and device clones. For example, in SCA-compliant radios that have a single partition for storing sensitive data and nonconfidential information, privileged execution of malicious code can allow the adversary to access all data stored in the nonvolatile memory of the radio set, including the cryptographic keys. Critical information can then be transmitted in clear using a data transmission waveform deployed in the SDR itself, or the adversary may use any other external interface available.

Another type of attack that belongs to this class is traffic analysis attacks. In such attack, the adversary aims to get mission-critical radio network information by observing traffic statistics [12, 25]. Critical information that can be obtained includes senders and receivers identities, the establishment and termination of connections, consumption of bandwidth, bursty traffic, signal strength, and so forth. This type of attack can be divided into two types: passive and active. In the passive traffic analysis, the adversary passively collects data and performs several analysis tasks on the collected data. In the active traffic analysis, the adversary uses active probes in the process of gathering information to obtain additional data that cannot be obtained by passive collection. In this case, the adversary seeks to analyze the behavior of radio network elements when subjected to a specific stimulus [25]. Besides that, any modification on the transmission power level adopted by a military radio set is a potential tool of unauthorized access to any type of data, since it may allow an enemy force with electronic warfare capabilities to monitor, search, intercept and decode messages, or even identify traffic patterns by mapping control and configuration data flow.

When the adversary has possession of an operational SDR, sensitive information (e.g., cryptographic keys) can be obtained through side-channel attacks, as described in [26, 27]. In this type of attack, the adversary collects and analyzes data related to several physical quantities, such as power consumption, processing time, and electromagnetic emissions of the SDR internal circuitry, to gain access to sensitive information. As an illustration, there are several examples in the literature of how an attack of this type can be performed with the aim of breaking implementations of

cryptographic algorithms [6, 21, 28, 29]. For example, in [29] the authors focus on the analysis of electromagnetic signals emitted by the device under attack to break cryptographic algorithms and overcome countermeasures against other side-channel attacks, such as those based on power. The electromagnetic emissions of interest are originated from data processing operations, such as those observed in CMOS circuits. The authors describe successful attacks to block ciphers (DES) and public key algorithms (RSA) in chip cards, and to SSL accelerators using a single electromagnetic signal sensor (antenna). It is noteworthy that all the attacks described in [29] are nonintrusive, noninvasive and does not require precise positioning of the electromagnetic sensors.

Another type of attack that belongs to this class is fault-based attacks, which, as is the case of several side-channel attacks, requires ownership of an operational radio. In this type of attack, the adversary induces faults in hardware in order to gain access to sensitive information. An example of this type of attack is described in [23]. In this paper, the authors describe how to obtain a 1024-bit RSA private key in a Linux SPARC system through the insertion of processing errors by decreasing the supply voltage of the processor. By introducing faults in the processing of the fixed window exponentiation algorithm (FWE) used in OpenSSL-0.9.8i, the authors were able to get the 1024 bits private key after 100 hours of offline processing, in a Pentium 4 cluster with 81 nodes. It should be highlighted that this type of attack does not damage the target machine, leaving no signs that its security has been compromised, as is the case for side-channel attacks.

Social engineering attacks [15, 30, 31], which consist on the manipulation of people to obtain confidential information, can also be used to obtain sensitive information from a radio set. These attacks involve the use of tricks to deceive one or more individuals within an organization, and often the adversary never meet personally with the misled individuals. Social engineering can be applied through various methods, for example, personification of superiors or colleagues and phishing [15]. This attack involves individuals who have specific knowledge or have physical access to the radio device and can be highly effective in military institutions [31]. For example, the action of a single operator can enable an electromagnetic emission side-channel attack by placing a data collector device near the SDR, influenced by an adversary impersonating a superior officer. The data collector device would then be returned by the operator to the adversary, who can process the collected data offline.

2.5. Denial of Service. In this case, the adversary objective is to make the SDR unavailable or nonoperational. A denial of service attack aims to make the SDR unavailable or nonoperational. This type of attack can exploit several vulnerabilities, for example, buffer overflow vulnerabilities, protocol vulnerabilities, hardware trojans, jamming, and flooding. In the scope of this paper, jamming is defined as the deliberate transmission of radio signals that interfere with the radio communication between two devices by reducing the signal-to-noise ratio. Jamming attacks can be used in wireless data transmission to stop the flow of information between two communicating entities [27, 32]. In turn, in the flooding attack an adversary sends a large number of messages, related to a particular waveform, to a radio device at a rate so high that the SDR cannot process all the messages in time [27]. This overcapacity processing can result in a partial or total denial of service.

As an illustration of possible attacks on military radio set, consider the frame structure for all MIL-STD-188-110 B waveforms [30], used to convey interoperability for data modems on HF bands. Based on that standard, an initial 287 symbol preamble is sent, being followed by a 72 frames sequence of alternating data and known symbols. Each data frame is made of a data block consisting of 256 data symbols, followed by a miniprobe sequence with 31 symbols of known data. After that 72 data frames sequence, a 72 symbol subset of the initial preamble is reinserted to facilitate late acquisition, communication channel impulse response estimation [31, 33], adaptive equalization, and synchronization adjustment. So, any change on the preamble data sequence, on the block information, or even on the frame structure makes the military network unavailable or nonoperational, since it keeps the receiver radio set from recognizing the adopted communication protocol.

3. Case Studies of Attacks for General Tactical SDRs

In this section, we describe several cases of vulnerabilities that a tactical radio is typically exposed to. Our goal in this section is to include case studies that we consider the most relevant for military applications, considering expected losses to legitimate users of the tactical radio network, based on the taxonomy presented in Section 2. Based on that, we present several case studies in which the radio sets are enabled with adaptive modulation features.

Adaptive modulation techniques have been widely studied for use in mobile scenarios due to their excellent performance characteristics in relation to conventional modulation strategies in typical mobile radio communication scenarios. Due to that fact, adaptive modulation techniques implementation is suitable for SDR and cognitive radios, since the functional core of such radios is software based, thus supporting adaptive modulation techniques changing pattern. Moreover, adaptive modulation techniques present secrecy capacity, bringing within a remarkable contribution to the transmission security over wireless communications links.

Therefore, due to the above, adaptive modulation techniques are a promising strategy in the context of strategic and tactical military communications, which justifies its choice as the physical layer technology in this paper.

3.1. Military Scenario Description. We present in Figure 1 an illustration of a point-to-point connection between a server and a subscriber, through a wireless link with two radio channels, representing forward and backward communication between stations, as typical in several military communication scenarios.

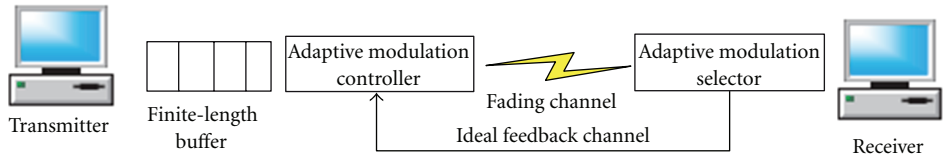

Figure 1: Typical point-to-point tactical wireless link.

The transmitter station has a finite-length queue (buffer), which operates in a first-in-first-out (FIFO) mode and feeds an adaptive modulation controller, in order to match transmission parameters (e.g., modulation schemes) to time-varying channel conditions and ensure a maximum performance and/or an agreed quality-of-service (QoS) level. The adaptive modulation selector is implemented at the receiver to make an on-the-fly performance evaluation, giving the acquired results back to the transmitter through the feedback channel. The processing unit at the data-link layer is a packet, which comprises multiple information bits. On the other hand, the processing unit at the physical layer is a frame, which consists of multiple transmitted symbols transmitted deterministically in a fixed rate pattern.

We assume that multiple transmission modes are available, with each mode representing a specific modulation format. Based on the channel state information (CSI) estimated at the receiver, the adaptive modulation selector determines the more adequate modulation scheme to be used by the transmitter at the following packet transmission.

There are several design strategies to perform modulation selection. According to some of the most suggested approaches, the adaptive modulation scheme is selected to guarantee a physical layer-driven QoS level, since based on the instantaneous SNR on wireless channels characterized by flat-fading effect. As presented in [34], the last approach is suboptimal when compared to a data link layer oriented QoS provision, in which the choice of modulation seeks to keep the total packet loss rate (due to both physical-layer packet transmission errors and data-link layer buffer overflow events) at an appropriate level while maximizing the spectral efficiency, while taking application-layer traffic model into account.

In spite of the adopted modulation selection scheme, CSI data with the proper modulation scheme is sent back to the transmitter through a feedback channel, for the adaptive modulation controller to update the transmission mode. It is worthwhile noting that coherent demodulation and maximum-likelihood (ML) decoding are employed at the receiver and that the decoded bit streams are mapped to packets, which are pushed upwards to layers above the physical layer [35].

The objective of adaptive modulation is to maximize the achieved data rate by adjusting the modulation scheme usage to the present channel state, being subject to prescribed QoS constraints (e.g., a maximum physical layer packet error rate). In order to achieve that, the entire signal-to-noise (SNR) ratio is partitioned into $N + 1$ consecutive nonoverlapping intervals, with boundary points denoted by (L_i), $0 \le i \le N+1$, which means that mode j is used when the instantaneous SNR (L) is such that $L_j \le L \le L_{j+1}$. Moreover, we state that no transmission occurs when $L \le L_1$, which corresponds to mode 0.

Considering several practical operational assumptions, such as the existence of flat-fading effects over the wireless channel, a finite-length buffer at the data-link layer, and the availability of a limited number of modulation schemes, there are important imperfections on the system performance. The most important drawbacks are the packet error rate (PER) at the physical layer, the packet dropping probability (PDP) to indicate the ratio of dropped packets at the data-link finite-length buffer, and the average spectral efficiency (ASE), which stands for the average number of transmitted packets at a single frame and depends on the channel state, the queue occupancy discipline, and the traffic data rate that comes from the application layer.

Based on such assumptions, we consider an adaptive modulation transmitter with five available modulation schemes (BPSK, QPSK, 8-QAM, 16-QAM, and 64-QAM) to perform data transmission, a fixed packet length of 1080 bytes, and a fixed frame transmission duration (time unit) of 2 ms. Besides that, we assume a queue length of 50 packets, an application traffic pattern modeled by a Poisson process with an arrival rate of 2 packets/time-unit, and a Doppler frequency (which measures the wireless channel fading behavior) of 10 Hz. Based on the method proposed by [36], we can evaluate the best suited SNR intervals to maximize ASE given a prescribed maximum PER for different average signal-to-noise ratio (SNR_{av}) scenarios.

3.2. Radio Control Attack. In the first case study, we evaluate a radio control attack, in which an adversary injects malicious code exploiting, for instance, a buffer overflow vulnerability. Here, we analyze the case where system performance is deviated due to an attacker which alters the proposed SNR intervals to maximize ASE given a PER of 0.01. Among several options of possibly available vulnerabilities to achieve his goal, the adversary may exploit SDR adaptive modulation scheme reconfiguration during post-waveform download phase, after discovering a breach either in code authenticity security policy or in software version control policy.

After identifying an available vulnerability, the imposed attack strategy described here provides an unwittingly 1-dB augmentation for all elements into the SNR adaptive modulation interval—for instance, the evaluated SNR interval for $\text{SNR}_{\text{av}} = 20$ dB is $L = [8.5971\ 10.9598\ 16.5522\ 18.2111\ 21.9357]$ dB, while the under-attack SNR interval is $L =$

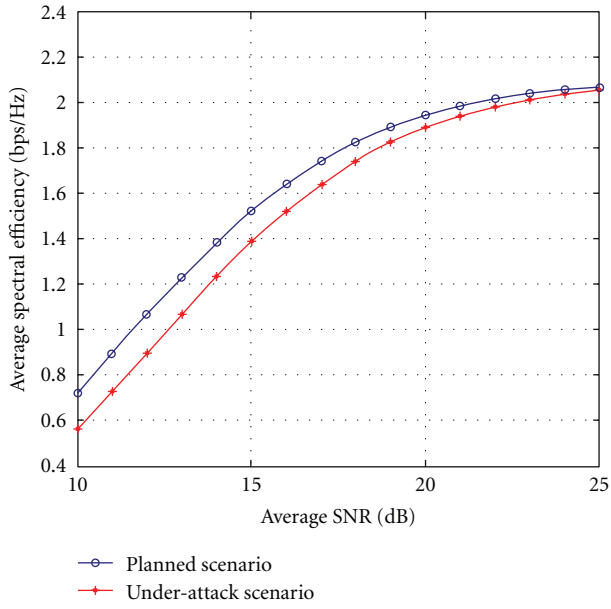

Figure 2: ASE in different scenarios.

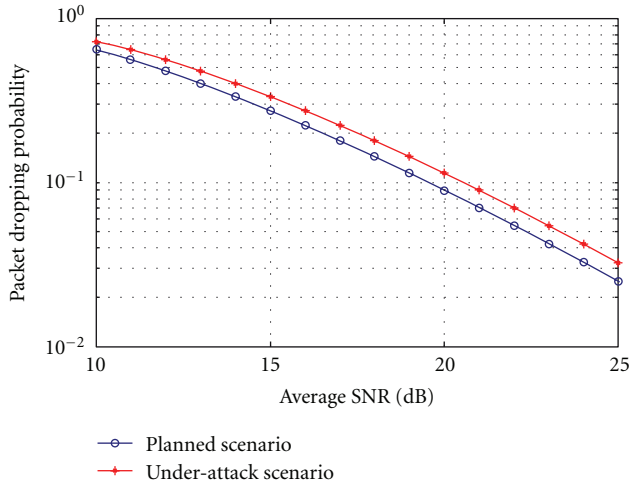

Figure 3: Packet dropping probability in different scenarios.

[9.5971 11.9598 17.5522 19.2111 22.9357] dB. So, Figures 2, 3, and 4 describe, respectively, the average spectral efficiency, the packet dropping probability, and the global packet loss rate (encompassing both physical- and data-link layer errors) for the currently planned and the under-attack scenarios.

Based on that, we can state that the proposed system keeps operational, since both scenarios achieve a PER of 1%, as required by the prescribed constraint. However, the resulting breach exploited by the adversary intrusion brings an overall drawback in system performance, since it lowers ASE (as much as 0.1643 bps/Hz at 12 dB), while it increases PDP (i.e., the dropping probability increases 30.36% at 25 dB) and, as a consequence, the overall PLR (e.g., the global losses in both physical- and data-link layer are 24.06% higher at 20 dB), even with such a slightly different adaptive modulation vector, which could easily pass unnoticed.

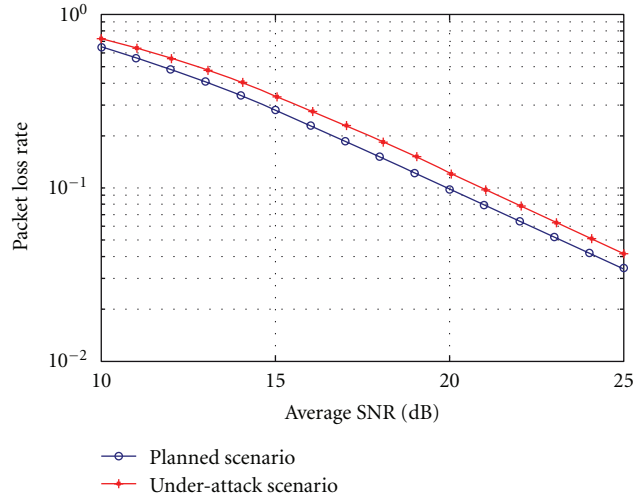

Figure 4: Global packet loss rate in different scenarios.

The reason for that performance is the SNR interval translation to higher levels. Due to that upper shift, it is less probable to adopt modulation schemes with higher spectral efficiency rates, lowering the average number of packets transmitted at a given time slot. Since the prescribed application data rate remains the same (it is worthwhile noting that the authorized user is unaware of the attack), the lower the number of transmitted packets per time slot is, the higher the average buffer occupancy is, increasing the packet dropping probability and the overall packet loss rate as well, degrading overall system performance [28], in spite of frame structure preservation.

Since the threshold increases, the physical layer QoS (namely, the bit error rate) is satisfied with an increasing slack, but the spectral efficiency tends to decrease, which increases the average queue occupancy in the link layer. Such a scenario can therefore increase the packet loss and dramatically reduce the spectral efficiency.

Thus, in an extreme case, we could face a DoS (denial of Service) attack, since a malicious tampering that promotes a very high level of L_1 can interrupt the data transmission. Moreover, by reducing the thresholds, the data rate increases, but the useful rate (goodput) gets reduced, due to the increase in physical layer error rate.

In a previous work [5], the authors provide a description of how attack mitigation strategies can impact the development of an SCA-compliant software infrastructure. Thus, among several options to harden tactical SDR security against radio control attacks, the usage of separation kernels is appropriate, since the adoption of several logical partitions limits the damage caused by a code injection attack.

The separation kernel concept is tightly related to MILS (Multiple Independent Levels of Security) capable systems [29, 37], which resolves the difficulty of certification of MLS systems by separating out the security mechanisms and concerns into manageable components. Besides that, an MILS verifiable system reduces the number of vulnerabilities that can be exploited by an adversary, since MILS

approach makes mathematical verification possible for the core systems software by reducing the security functionality to four key security policies, namely, information flow, data isolation, periods processing, and damage limitation, to assure data and process separation. An MILS RTOS system is designed to minimize the size of the kernel in order to make it verifiable by formal analysis and proof-of-correctness methods. The price related to this approach is more context switch overhead. However, this cost has been made more tolerable by hardware advances and careful design of the interpartition communication services.

3.3. Personification Attack. In the second case study, we evaluate a personification attack, having unauthorized data modification as a side effect. In this study, we consider that a transmitter adopts a modified adaptive modulation vector, instead of using the prescribed SNR interval to communicate with an authorized receiver station. Moreover, the modified SNR vector ensures an optimal system performance with an attacker radio station.

For instance, we consider that the average SNR between transmitter and attacker stations (SNR_{TR}) is 10 dB, with a data-link queue length of 20 packets, while the average SNR between the transmitter and the authorized receiver (SNR_{TR}) is 25 dB, with a data-link queue length of 10 packets.

The attacker may exploit a data transmission protocol vulnerability that allows replay attacks—for instance, relaying a copy of previously transmitted information onto a SCA-compliant waveform that does not implement challenge scheme to update adaptive modulation scheme vector. So, instead of using the evaluated adaptive modulation vector for $SNR_{AV} = 25$ dB, the transmitter adopts the evaluated adaptive modulation vector for $SNR_{AV} = 10$ dB, due to a personification attack under which the attacker is considered to be an authorized user and informs his average signal-to-noise ratio during the data transmission establishment phase.

Based on that, Table 2 describes the achieved performance at the two receiver stations after the breach exploitation, namely, the authorized user (AU) and the spoofer user (SU), according to several performance metrics. Moreover, the AU is evaluated under two scenarios, namely, the expected and the actually received ones. The presented results indicate system performance degradation due to the personification attack, especially on data-link packet dropping events.

Thus, among several options to harden tactical SDR security against personification attacks mixed with data modification drawbacks, the implementation of sequence numbers, challenges, or freshness schemes present simple, but effective, countermeasures to overcome such threats [23].

4. Conclusion

In this paper, we identify several case studies of attacks aimed at tactical software defined radios after presenting taxonomy with the most common classes of attacks on military scenarios. By using such approach, we identify several possible sources of vulnerabilities, attacks, intrusions, and mitigation strategies, especially in SCA-based operating environments. Concerning attack classes, it should be noted that the set of attacks and threads that are relevant to a radio set depend on its particular architecture, and therefore they are precisely defined during the execution of the radio-specific security engineering process.

Many recent studies highlight the inherent ability of secrecy in adaptive modulation techniques. For this reason, it is possible that military radios explore the use of this type of modulation in the near future, not only for their good performance characteristics in flat-fading and time-variant channels, but especially for the security aspect. The presented case studies showed that if the radio has vulnerabilities, it is possible to modify modulation parameters to keep the transmission, but with poor system performance. Thus, not only the information regarding the physical layer communication standard must be well protected, but also the adaptive modulation scheme threshold values.

As new research directions, we state that the definition of security requirements and the identification of new threats, when designing military-oriented security architecture, require the development of novel case studies focused on military scenarios. Thus, we consider that the vulnerabilities, attacks, intrusions, and mitigation strategies identified in this study define a point of departure not only for the threat analysis or even novel mitigation approaches, which are out of the scope of this work, but also for the requirements definition related to the security engineering process of a military software defined radio.

Acknowledgments

The authors acknowledge Fundação de Apoio à Pesquisa do Estado do Rio de Janeiro (FAPERJ) role in this work for the provided financial support (Process E-26/102.269/2009).

References

[1] "Interoperability and Performance Standards for Data Modems," United States Department of Defense Interface Standard, MIL-STD-188-110B, 2000.

[2] D. F. C. Moura, R. M. Salles, and J. F. Galdino, "A Joint method for cross-layer design over tactical wireless networks," in *Proceedings of the 8th International Information and Telecommunication Technologies Symposium (I2TS '09)*, Florianopolis, Brazil, December 2009.

[3] D. F. C. Moura, R. M. Salles, and J. F. Galdino, "Generalized input deterministic service queue model: analysis and performance issues for wireless tactical networks," *IEEE Communications Letters*, vol. 13, no. 12, pp. 965–967, 2009.

[4] X. Fu, B. Graham, Bettati, and R. Zhao W, "Active traffic analysis attacks and countermeasures," in *Proceedings of the International Conference on Computer Networks and Mobile Computing (ICCNMC '03)*, 2003.

[5] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS '05)*, 2005.

[6] J. Bonneau and I. Mironov, "Cache-collision timing attacks against AES," in *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES '06)*, 2006.

[7] J. F. Galdino, E. L. Pinto, and M. S. de Alencar, "Analytical performance of the LMS algorithm on the estimation of wide sense stationary channels," *IEEE Transactions on Communications*, vol. 52, no. 6, pp. 982–990, 2004.

[8] E. M. Gallery and C. J. Mitchell, "Trusted computing technologies and their use in the provision of high assurance SDR platform," in *Proceedings of the Software Defined Radio Technical Conference*, Orlando, Fla, USA, November 2006.

[9] D. Murotake and A. Martin, "A high assurance wireless computing system architecture for software defined radios and wireless mobile platforms," in *Proceedings of the Software Defined Radio Technical Conference and Product Exposition (SDR '09)*, 2009.

[10] A. M. A. Filho, E. L. Pinto, and J. F. Galdino, "Simple and robust analytically derived variable step-size least mean squares algorithm for channel estimation," *IET Communications*, vol. 3, no. 12, pp. 1832–1842, 2009.

[11] R. Gallo, H. Kawakami, and R. Dahab, "On device establishment and verification," in *Proceedings of the 6th European Workshop on Public Key Services, Applications and Infrastructure (EuroPKI '09)*, September 2009.

[12] R. Riley, X. Jiang, and D. Xu, "An architectural approach to preventing code injection attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 4, pp. 351–365, 2010.

[13] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr., "Assessing the spoofing threat: development of a portable gps civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08)*, pp. 1198–1209, September 2008.

[14] 3GPP, *Security Threats and Requirements (Release 4)*, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project, 2001.

[15] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, Article ID 1290968, pp. 94–100, 2007.

[16] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, Article ID 5604161, pp. 39–46, 2010.

[17] D. F. C. Moura, R. M. Salles, and J. F. Galdino, "Multimedia traffic robustness and performance evaluation on a cross-layer design for tactical wireless wetworks," in *Proceedings of the 9th International Information and Telecommunication Technologies Symposium (I2TS '10)*, Rio de Janeiro, Brazil, December 2010.

[18] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 154–163, May 1997.

[19] A. A. Pereira Junior and J. F. Galdino, "Secrecy rate of adaptive modulation techniques in flat-fading channels," *Revista IEEE América Latina*, vol. 8, pp. 332–339, 2010.

[20] D. Murotake and A. Martin, "System threat analysis for high assurance software radio," in *Proceedings of the Software Defined Radio Technical Conference and Product Exposition (SDR '04)*, Phoenix, Ariz, USA, November 2004, SDR Forum.

[21] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: leaking secrets," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (Crypto '99)*, vol. 1666 of *Lecture Notes in Computer Science*, pp. 388–397, Springer.

[22] A. J. Goldsmith and S. G. Chua, "Adaptive coded modulation for fading channels," *IEEE Transactions on Communications*, vol. 46, no. 5, pp. 595–602, 1998.

[23] A. Pellegrini, V. Bertacco, and T. Austin, "Fault-based attack of RSA authentication," in *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE '10)*, pp. 855–860, March 2010.

[24] R. W. Beckwith, W. M. Vanfleet, and L. MacLaren, "High assurance security/safety for deeply embedded, real-time systems," in *Proceedings of the Embedded Systems Conference*, 2004.

[25] M. P. Correia and P. J. Sousa, *Segurança No Software*, FCA Editora de Informática, 2010.

[26] F.-X. Standaert, T. G. Malkin, and M. A. Yung, "Unified framework for the analysis of side-channel key recovery attacks," in *Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques (Eurocrypt '09)*, vol. 5479 of *Lecture Notes in Computer Science*, pp. 443–461.

[27] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity," *IEEE Transactions on Computers*, vol. 53, no. 6, pp. 760–768, 2004.

[28] P. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS and other systems," in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (Crypto '96)*, vol. 1109 of *Lecture Notes in Computer Science*, pp. 104–113, August 1996.

[29] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES '02)*, vol. 2523 of *Lecture Notes in Computer Science*, pp. 29–45, August 2002.

[30] J. Goodchild, Social engineering: the basics, 2010, http://www.csoonline.com/article/514063/social-engineering-the-basics.

[31] A. J. Ferguson, "Fostering e-mail security awareness: the west point carronade," *Educause Quarterly*, vol. 28, no. 1, 2005.

[32] H. Berghel and J. Uecker, "WiFi attack vectors," *Communications of the ACM*, vol. 48, no. 8, pp. 21–28, 2005.

[33] T. X. Brown and A. Sethi, "Potential cognitive radio denial of service attacks and remedies," in *Proceedings of the International Symposium on Advanced Radio Technologies (ISART '07)*, 2007.

[34] A. González, R. Carlos, C. B. Dietrich, and J. H. Reed, "Understanding the software communications architecture," *IEEE Communications Magazine*, vol. 47, no. 9, pp. 50–57, 2009.

[35] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide To IEEE 802.11i—Recommendations of the National Institute of Standards and Technology*, 2007, NIST Special Publication 800-97.

[36] F. H. Hsu, F. Guo, and T. C. Chiueh, "Scalable network-based buffer overflow attack detection," in *Proceedings of the 2nd ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS '06)*, pp. 163–171, December 2006.

[37] J. Alves-Foss, W. S. Harrison, P. Oman, and C. Taylor, "The MILS architecture for high assurance embedded systems," *International Journal of Embedded Systems*, vol. 2, no. 3-4, pp. 239–247, 2006.