Secure Wireless Transmissions with Truly Random Noise Source Data Encryption

Encryption is a technique used to safeguard sensitive information over a communications network, meant for the eyes of only the intended recipient. The encrypted information appears unintelligible to intercepting parties but can be deciphered by those who have access to the specific decryption key, such as an algorithmically generated, pseudo-random sequence. Interception is possible; however, this feat typically demands vast computational resources.

Although the output from a pseudo-random algorithm appears patternless, it isn't a truly random sequence, as the term "pseudo" suggests. Instruments that generate noise waveforms provide an alternative path toward data encryption – one that attains complete randomness to strengthen viability against interception. This article will explore the basic concept of securing data with noise, as well as provide insight into the possible design of these encryption systems by reviewing relevant noise applications.

Noise Source Encryption Systems

Used in lieu of a pseudo-random generated key, noise offers an effective means to camouflage data of interest due to its truly random nature. In this process, the transmission appears as a noise-like signal while in transit. Although it appears as a random signal, the transmission actually contains a combination of the coveted data plus a noise waveform. Therefore, noise source encryption heightens the difficulty of data identification and decryption for unauthorized entities. In addition to producing a random signal, noise sources also provide a simpler, more efficient way to generate signals when compared to systems that utilize complicated algorithms for data encryption.

Noise sources, such as the NC3000 Series Calibrated Coaxial AWGN Modules and NC1000 Series Amplified Noise Modules from Noisecom, are potential devices that can be used for this type of application. The NC3000 Series generates additive white Gaussian noise (AWGN) from 10 MHz to 110 GHz and is available in standard coaxial RF connectors, such as N type, SMA, 2.92 mm, 1.85 mm, and 1.0 mm. The high-power, compact NC1000 Series can produce AWGN up to +13 dBm and has bandwidths up to 18 GHz. When utilized in a system, TTL-controlled attenuation allows power output control for external operation.

Within noise source encryption systems, only one NC3000 Series module, NC1000 Series module, or other physical noise generating device is embedded into the design. Two noise sources cannot be utilized, even if they are the same make and model. Encryption systems

only use one physical noise source since these devices are random and not coherent, meaning the signals will not have the same timing and voltage characteristics. The single noise source, for instance, can be physically implemented into the transmit side of the encryption circuit to mask the data of interest, while the receiver will employ techniques to decode the noise from the transmitted data.

Specific design details of encryption systems taking advantage of noise waveforms are kept under wraps, however, we can gather a bit more insight into possible setups by exploring two related concepts – the polarization of RF signals and noise-encrypted radar.

RF Signal Polarization

RF signals are comprised of electric and magnetic waves that are perpendicular in respect to each other as well as to the propagation direction. The polarization of a radio wave refers to the electric field's direction of oscillation. Many antennas are linearly polarized, meaning the electric fields oscillate in just one direction, including horizontally (horizontal polarization) and vertically (vertical polarization).

Since radio waves are polarized in various ways, antennas are generally designed and developed to handle a single type of polarization for transmit/receive operations. However, two signals in the same frequency band can be polarized in opposite directions, which avoids signal interference and increases channel capacity by a factor of two. Applications that utilize this technique, such as satellite television, can modify receive antennas to successfully capture both polarizations.

Oppositely polarized RF signals can play an important role in encrypting and decrypting wireless transmissions. For instance, a transmission may contain a noise signal plus the transmit signal that is vertically polarized, and just a noise signal that is horizontally polarized. In transit, the encrypted waveform would appear as a random signal of no interest to interceptors.

The receiving side, which is equipped to handle both polarizations, can use the noise-only signal to decrypt the desired information from the vertical polarization. This is achieved by first combining both received signals and adding the two noise signals out of phase, which effectively cancels out the noise waveforms. The receiver is then left with the decrypted and securely sent information. In order to successfully intercept a message of this kind, attackers would need to know the exact transmit frequency as well as which polarization contains the encrypted transmission.

Noise Radar Encryption

In primary radar systems, like those used in air traffic control (ATC) applications, signals are transmitted from a ground-based antenna at an intended target (e.g., an aircraft). The signals reflect off the target and are then recaptured by the ground-based radar antenna. Analyzing the reflected signal can determine various pieces of information about the object of interest, such as distance, angle, and velocity.

While ATC applications must easily detect and process radar signals, more stealth-focused operations require the use of radar signals with a low probability of interception and exploitation. Noise radar technology adds random noise to the transmit signal, typically generated from high-frequency noise sources. The transmission appears as background noise as it travels to its intended target, when in actuality it is an encrypted signal hiding in plain sight.

After receiving the reflected waveform, the signal can be analyzed to uncover its changes from the initial transmission, which determines the desired information about the target of interest. While noise radar reduces the signal's visibility from adversaries, it also limits mutual interference from other radar signals when operating in crowded environments.

Preserving Data Security with Noise

Encryption maintains the privacy and security of confidential information as it embarks on potentially high-risk travel to reach its intended parties. While there are various ways to protect sensitive data, noise sources provide a truly random, simply generated means to disguise transmissions. Noisecom, a leader in RF and microwave noise sources such as the NC3000 Series and NC1000 Series, safely mask wireless transmissions behind the generation of noise waveforms, increasing defensive capabilities against would-be interceptors. To learn more about noise source solutions, visit www.noisecom.com/.