Description of Videofied RF technology

Videofied uses advanced RF (radio frequency) communications between the control panel (hub) and the peripheral devices. The RF used is not the standard 802.11 typical WiFi operating at 2.4 GHz used in home and office environments. Instead of WiFi, Videofied operates in the 868, 915 or 925 MHz band (depending upon geographic market) for maximum penetration of building materials and maximum range in harsh environments. While WiFi is designed to transmit large amounts of data it does a poor job of penetrating common building materials like plasterboard, brick and concrete. Instead of going through walls, 2.4 GHz mostly bounces around solid objects, which is why there are often "dead zones" in office buildings or homes – not ideal for a security system. 900 MHz is an ideal compromise with a frequency that carries enough data for small 200K Videofied files as well as being able to penetrate building materials for maximum coverage and range inside commercial buildings, homes and outdoor structures.

In addition to using the optimal frequency, Videofied RF is based upon military grade enhancements for maximum security and performance:

- 25 channel spread spectrum (frequency hopping)
- AES encryption of the signal

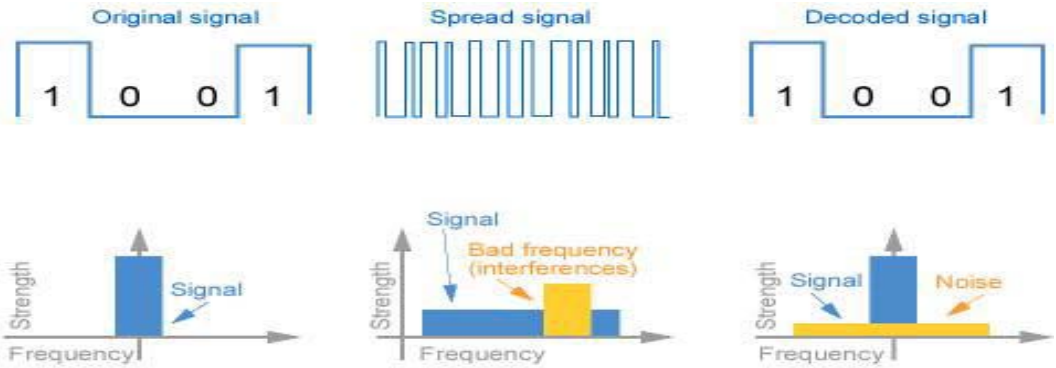
These enhancements mean that Videofied operates in noisy harsh RF environments such as electrical substations, overcoming interference. It also means that the system is secure from unauthorized access and hacking. The following summaries describe these features in greater detail.

Frequency Hopping Spread Spectrum

Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. It is utilized as a multiple access method in the frequency-hopping code division multiple access (FH-CDMA) scheme.

A spread-spectrum transmission offers three main advantages over a fixed-frequency transmission:
Spread-spectrum signals are highly resistant to narrowband interference. The process of re-collecting a spread signal spreads out the interfering signal, causing it to recede into the background. Spread-spectrum signals are difficult to intercept. An FHSS signal simply appears as

an increase in the background noise to a narrowband receiver. An eavesdropper would only be able to intercept the transmission if they knew the pseudorandom sequence. Spread-spectrum transmissions can share a frequency band with many types of conventional transmissions with minimal interference. The spread-spectrum signals add minimal noise to the narrow-frequency communications, and vice versa. As a result, bandwidth can be utilized more efficiently.



Spread Spectrum uses wide band signals that are more difficult to jam and less subject to interference than narrow band signals.

AES Encryption

In cryptography, the Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor,[3] the Data Encryption Standard (DES).

AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. It became effective as a standard May 26, 2002. As of 2009, AES is one of the most popular algorithms used in symmetric key cryptography.[citation needed] It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information.

In June 2003, the US Government announced that AES may be used to protect classified information. The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in

products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

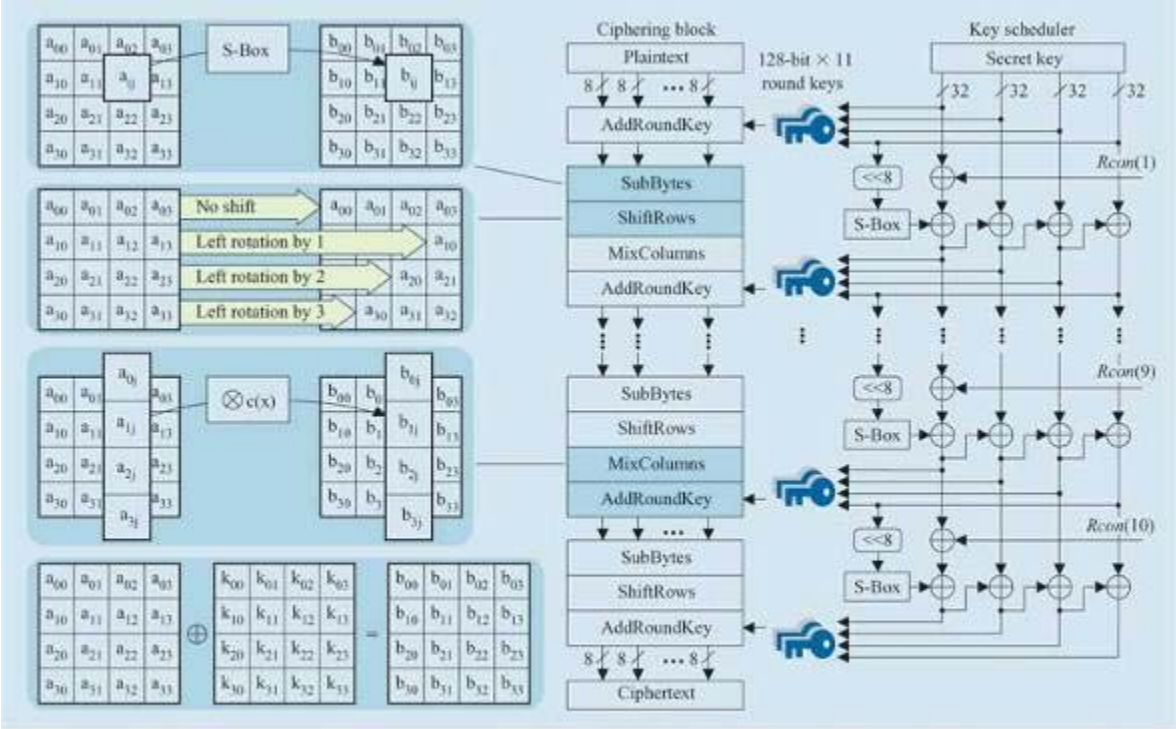


Figure 2

AES encryption process under a 128-bit secret key.

This figure shows an advanced Encryption Standard (AES) encryption process under a 128-bit secret key. Eleven sets of round keys are generated from the secret key and fed to each round of the ciphering block. The round operation is a combination of four primitive functions: SubBytes (sixteen 8-bit S-Boxes), ShiftRows (byte boundary rotations), MixColumns (4-byte x 4-byte matrix operation), and AddRoundKeys (bit-wise XOR). In decryption, the inverse functions (InvSubBytes, InvShiftRows, and InvMixColumns, with AddRoundKey as its own inverse) are executed in reverse order. The key scheduler uses four S-Boxes and 4-byte constant values *Rcon(i)* (1/10). In decryption, these sets of keys are used in reverse order.