PowerG®

Technology for life

Technology Overview

Visonic®

For a secure way of life

CONTENTS

INTRODUCTION 3
FREQUENCY HOPPING SPREAD SPECTRUM 4
FULL TWO-WAY SYNCHRONIZED TDMA COMMUNICATION 5
SECURED WIRELESS COMMUNICATION WITH AES ENCRYPTION 6
UNMATCHED BENEFITS WITH A BREAKTHROUGH TECHNOLOGY 7
SUMMARY 8

© 2010 Visonic Ltd. All rights reserved. Information subject to change without notice.

Visonic®
For a secure way of life

INTRODUCTION

Today, wireless communication is part of daily life - it is everywhere we turn and it affects everything in multiple ways. The use of wireless communication systems and devices is increasing at an exponential pace. In parallel, users have gained full confidence in wireless performance and rely on numerous wireless devices.

With intrusion alarm systems, this trend is no different. The shift from hard-wired to wireless alarm systems has been rapid. In a 2009 report, IMS Research estimated that shipments of wireless alarm products will double in volume in the next five years—the main reason being the high penetration of wireless alarm equipment. Security installers are standing behind wireless alarm systems, allowing for consumer adoption and insurance companies' acceptance of technologies that had once been considered not trustworthy enough for security.

The rapid adoption of wireless communication is making our environment noisy and dense with radio energy. As a result, the performance of wireless security systems is hindered by collisions, interferences, and jamming. Furthermore, security standards are becoming more stringent and demanding. They require higher immunity to interferences and to message substitution, correct message identification and very fast supervision. Security standards are also now stricter with regards to the alarm systems' ability to withstand intruder attempts to hack the system.

As labor costs increase worldwide, central monitoring stations are looking for ways to save on installation cost and time. The need for reduced on-site maintenance demands technological tools that enable intrusion systems to be managed remotely.

Until now, wireless alarm systems were based on technologies that could not fully answer the needs nor solve the problems described above. The facts called for an entirely new technology that would bring the industry improved reliability and robustness.

Visonic's PowerG technology introduces a new era in alarm systems that literally redefines wireless intrusion security and reliability. PowerG provides the answers and solutions to the demanding requirements facing the security industry today as well as the challenges of tomorrow.

FREQUENCY HOPPING SPREAD SPECTRUM

Frequency Hopping Spread Spectrum (FHSS) derives from military radio technology where it was designed to be secure and reliable under adverse battle conditions. FHSS changes the frequency of a transmission at intervals faster than an intruder can retune a jamming device. With FHSS, the bandwidth is divided into multiple frequency channels. Once a wireless connection is established and time-synchronization is gained, the receiver and transmitter agree on one of practically infinite frequency hopping sequences. These sequences are both encrypted and time-dependant. Based on the current time and a mathematical calculation, both the receiver and transmitter hop to the next frequency channel in the sequence at the same time. Unless the system time, the system encryption key and the proper calculation are all known, the communication cannot be tracked. As a result, unauthorized interception of, or eavesdropping on, a communication is virtually impossible.

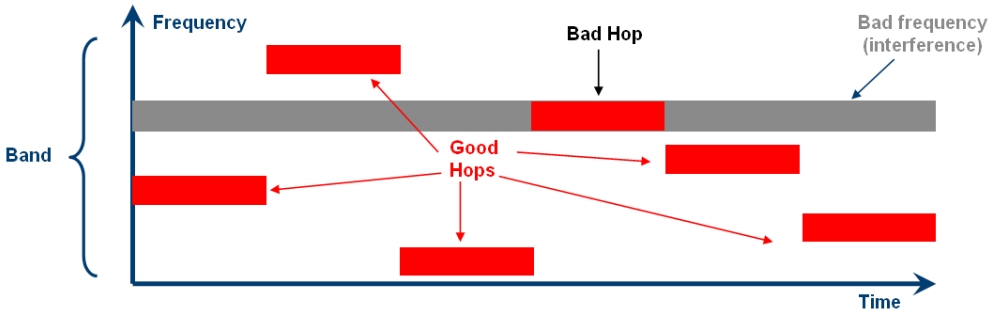
The PowerG network uses Frequency Hopping Spread Spectrum technology. The network continuously hops between multiple frequencies spread over the entire assigned frequency band: 8 hopping frequencies in the 433-434MHz bands, 4 hopping frequencies in the 868-869MHz bands, and 50 hopping frequencies in the 912-918MHz bands.

The network does not remain in a single frequency but switches frequencies 64 times a second, using an encrypted unique pseudo-random sequence known only to devices enrolled to the PowerG panel. The pseudo-random sequence differs from one PowerG panel to another.

By using FHSS technology, the PowerG network successfully overcomes intentional and un-intentional interferences and jamming. Multiple Visonic PowerG-based alarm systems can operate in the same vicinity without interfering with each other. Robustness and reliability of the wireless network increases dramatically.

An analogy to FHSS is as follows: Imagine a car driven in a multi-lane highway. As a strategy, the driver continuously and rapidly changes lanes. If one of the lanes is blocked (by road-works or a road accident) the car will avoid the disturbance because it is changing lanes continuously. The following figure illustrates the FHSS concept.

Frequency hopping avoids blocking and interferences

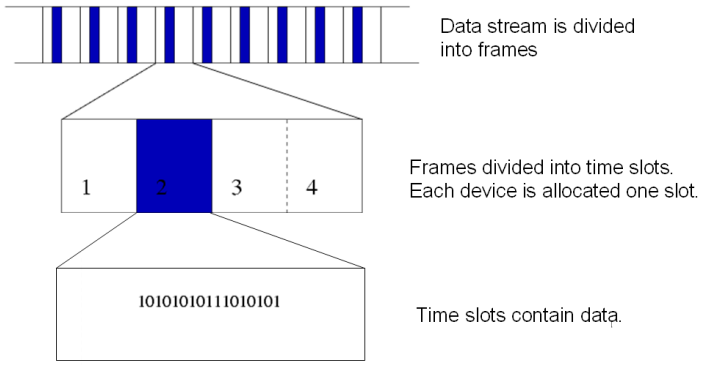


Visonic®
For a secure way of life

FULL TWO-WAY SYNCHRONIZED TDMA COMMUNICATION

TDMA (Time Division Multiple Access) is a digital transmission technology that allows a number of users to access a single radio-frequency (RF) channel without interference by allocating unique time slots to each user within each channel.

TDMA Frame Structure



The users transmit in rapid succession, one after the other, each using their own time slot. This allows multiple users to share the same transmission medium (e.g. radio frequency channel) while using only part of its channel capacity. Multiple users, therefore, can share the same frequency channel without causing interference because the signal is divided into multiple timeslots, where each timeslot acts as a separate communication path. TDMA relies upon the fact that the signal has been digitized - divided into milliseconds-long packets. It allocates a single frequency channel for a short time and then moves to another channel. TDMA is used in digital cellular systems such as GSM.

Similar to the GSM cellular network, each device in the PowerG network is allocated unique timeslots for full two-way data transmission with the panel, streamlining communication and increasing channel efficiency. This eliminates RF collisions and assures that no alarm or supervision message is lost. TDMA technology provides the devices with extended battery life since the device is only transmitting a portion of the time. Repeated transmissions are also avoided, resulting in an energy-saving network.

An analogy to the PowerG synchronized TDMA communication is as follows: imagine a meeting attended by several people. When communication is not synchronized, participants speak simultaneously, creating interferences and communication blocks. On the other hand, if the meeting is managed by a moderator who controls who speaks by a complex set of rules and a rigid clock, each participant restricts his or her speaking to a specific timeslot during which everyone else remains silent. The meeting is then conducted effectively.

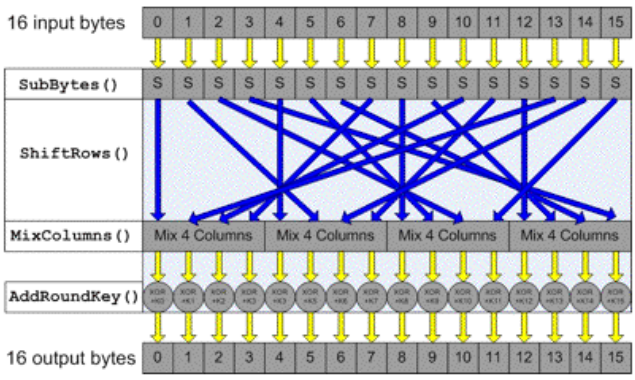
SECURED WIRELESS COMMUNICATION WITH AES ENCRYPTION

AES (Advanced Encryption Standard) is a symmetric (private key) encryption standard originally published as Rijndael (after its inventors Rijmen and Daemen) in 1998 and adopted by the U.S. government in 2000. In 2001, AES was chosen by NIST (National Institute of Standards and Technology) as the Federal Information Processing Standard (FIPS), also known as FIPS197. In 2003, the National Security Agency (NSA) stated that AES was secure enough to protect its information at the secret and top-secret levels.

AES consist of three block ciphers. Each cipher has a 128-bit block size with three different key sizes of 128, 192, and 256 bits. The algorithm is based on permutations and substitutions. Permutations are rearrangements of data, and substitutions replace one unit of data with another. AES performs permutations and substitutions using several different techniques. The AES cipher repetitively performs a number of transformation rounds, thus converting the input plain data into an output of cipher data. There are several processing steps for each round, with one round that relies exclusively on the encryption key. Then, a set of reverse rounds are applied to convert the cipher data back into plain data. The AES encryption uses a single key which is a shared secret between the sender and receiver to encrypt and decrypt data. An analogy is a locked mailbox without a mail slot. Anybody who wants to leave or read a message needs to have a key to the mailbox.

The PowerG network employs the proven AES-128 (128 bit key) advanced encryption algorithm for correct message identification and for protecting the alarm system from code grabbing and from message substitution by hackers and other attackers. AES-128 uses 10 rounds with each round performing several transformations.

AES Transformations Round



AES is a well-proven encryption algorithm that guarantees strong authentication and encryption security for the PowerG wireless network.

Visonic®
For a secure way of life

UNMATCHED BENEFITS WITH A BREAKTHROUGH TECHNOLOGY

The combination of technologies—Frequency Hopping Spread Spectrum (FHSS), synchronized TDMA communication, and AES—gives PowerG immense strength to delivver a new, advanced alarm system that provides unmatched advantages for professional installers, central monitoring stations and end-users alike. In fact, PowerG provides the convenience of a wireless network with reliability closer than ever to that of a hard-wired one.

Energy-saving network:

- Each device continuously measures communication quality and automatically sets its transmission power to the minimum required for reliable communication with the panel. Full, two-way synchronized communication ensures minimum, short transmissions. These significantly extend the battery life of PowerG devices to exceed 8 years. Furthermore, on-site maintenance visits are reduced due to the system's capability to support numerous functions remotely.

Unmatched robustness and reliability:

- Signals continuously hop between channels in a random sequence, avoiding interferences and jamming. TDMA communication ensures RF collisions are eliminated.

Surpasses most industry security standards:

- The PowerG network employs the proven AES-128 encryption algorithm, protecting the system from code grabbing and message substitution by hackers and other attackers.

Huge transmission range:

- PowerG employs advanced radio and diversity antenna technologies that, when combined with frequency hopping and synchronized TDMA communication, result in an extremely large range—far greater than the industry standard. This enables repeater-free installations even on very large premises. Tests reveal a line of sight communication range greater than 2km (6,000ft)*. By adding a PowerG repeater the range can be doubled.

Support for advanced applications

- PowerG was designed to handle a substantially high bandwidth, enabling the network to transmit large amounts of data in a short time. This provides the infrastructure for future solutions, such as installations with numerous devices, audio and video applications.

New and advanced toolset saves time and money:

- The PowerG full two-way uplink and downlink data communication provides installers with powerful tools, never seen before in our industry, that can save time and money on a daily basis. The toolsets include: quick and easy installation with built-in link quality indicators on the devices; on-site and remote configurations of devices and peripherals; cost-saving advanced on-site and remote diagnostics—the system continuously diagnoses the RF environment and interferences at the site and provides (locally and remotely) meaningful information to help understand and resolve problems; remote real time testing and walk testing of the system.

* In actual installations, the range is reduced due to construction signal attenuation.

SUMMARY

While Frequency Hopping Spread Spectrum, TDMA communication and AES are not new technologies, it is the implementation of all three within PowerG that makes this system so innovative and revolutionary. This combination in Visonic's new intrusion alarm systems fully answers the urgent needs of our industry.

ABOUT VISONIC

The Visonic Group (TASE:VSC.TA), founded in 1973, is a leading developer and manufacturer of cutting-edge home security systems and components that provide people around the world with peace of mind and safety in their homes. Building on its decades-long position at the forefront of home security innovation, Visonic is today leading the drive to expand the boundaries of security, offering advanced solutions to the full range of residential safety needs, from securing the house and contents to safeguarding the health and comfort of the people who live there.

Visonic's offerings include a wide variety of home security systems, personal emergency response and safety systems, and a market-leading variety of peripherals. Visonic is headquartered in Israel, where it operates a development center and manufacturing plant. Its sales and marketing subsidiaries in the USA, Germany, UK, Poland, Spain and Hong Kong are supplemented by a worldwide network of distributors, serving a growing installed based that spans more than 70 countries. Please visit www.visonic.com.

© 2010 Visonic Ltd., Ltd. All rights reserved. Visonic and PowerMax are registered trademarks of Visonic Ltd. All other trademarks, trade names, and images mentioned herein belong to their respective owners. Visonic reserves the right to change information or specifications without notice.