

Security Industry Communications in the Internet Age

The onslaught of mobile phones, Voice over IP and Instant Messaging has changed the way we communicate. GSM and fixed & wireless Internet is becoming more widespread and less expensive each year and this will have an effect on the way security systems might communicate in the future. Consumers are ever keener to take advantage of new technologies and it is important that the security industry adapts quickly and does not get left behind.

Author: Steve Nutt (IP Alarms)



Steve started out as an alarm installer in 1983 and ran his own UK based company for 15 years. In that time he installed hundreds of digital communicators on behalf of his clients. He progressed into writing software for the security industry full time and spent 4 years in Australia on a joint venture with another software company before settling in Thailand to develop IP & GPRS solutions for alarm monitoring.

Demise of the Public Switched Telephone Network

For decades, PSTN has been the chosen communication platform for the transmission of alarm signals. Today, many are predicting its days are numbered.

Two transmission paths have emerged as the preferred methods of communication between an alarm panel and Monitoring Centre – IP (the Internet) and GSM. This article will examine the pros and cons of each.

GSM Wireless Networks

In today's high tech world, almost everybody owns a mobile phone. The perception is that GSM networks are very reliable and rarely suffer from network outages. This makes GSM a viable platform for alarm

communications and three different technologies can be employed for signal transmission – SMS, Voice and Data.

The reliability of SMS varies greatly from country to country and delays in message delivery rule it out from being considered a serious option in countries where messages can often be delayed for many hours.

In countries that do not experience such delays, SMS can be a good low cost method of alarm communication, however, it is often not popular with alarm monitoring companies as it opens up the possibility of self monitoring where messages can be sent directly to the end users mobile phone.

The use of a GSM Dialer/Communicator allows an alarm panel modem to dial out and make a phone call to the Monitoring Centre over the GSM network. When a conventional analogue alarm receiver answers the call, an audio/voice channel is opened up and the alarm panel can communicate with the receiver just as it would over a PSTN line. This technology benefits from being alarm protocol independent and industry experts claim a transmission success rate of somewhere between 80% and 100%.

Both SMS and Voice benefit from low equipment costs and low network rates.

CONS: SMS and Voice technologies do not allow for the cost efficient supervision of a connection to the Monitoring Centre and often the first anyone gets to know about sabotage or network failure is when a scheduled signal, or worse, an emergency signal fails to arrive.

GPRS Wireless Networks

The use of a GPRS data plan overcomes this problem and allows constant supervision of the connection between the protected premises and the Monitoring Centre.

A GPRS device uses the GSM network to achieve an “always on” wireless connection to the Internet. Once connected, it can communicate using Internet Protocols (IP) just like any other Internet enabled device. This allows the sending of regular heartbeats to the monitoring server so that any equipment failure, sabotage or loss of network can be detected within seconds.

GPRS devices do not support audio/voice communications, so any alarm signals using standard protocols such as Ademco Contact ID or Fast Format have to be converted from analogue to digital within the device itself. This is referred to as Dialer Capture.



GPRS enabled devices are more expensive than SMS and Voice devices and the cost of data plans vary widely from country to country. Asian countries tend to have very reasonable rates whereas rates in North America are very restrictive.

CONS: All of the GSM technologies are vulnerable to sabotage from a GSM Jammer which can be used to prevent devices from connecting to the network.

IP Networks (the Internet)

Due to the widespread availability of the Internet, a large number of consumers are turning to voice over IP for voice service. For the continuity of clear telephone calls from human to human it's a simple case of unplugging your analogue telephone handset from the PSTN line and plugging it into an analogue terminal adapter to make and receive calls over the Internet. The human ear is very forgiving and even though delays and echo in voice conversations can sometimes be off-putting, both parties are usually able to understand each other.



Unfortunately, this is not the case with alarm communications. Somewhere between converting analogue into digital, traveling over the wire and converting digital back to analogue, things like noise and latency are introduced and along with other problems with VoIP networks, can cause alarm communications to fail.

An in depth knowledge of alarm panel protocols, alarm receivers and Internet protocols has made it possible for some solutions providers to allow the use of regular low cost "off the shelf" VoIP ATA's for the reliable transmission of alarm signals over the Internet. This obviously provides huge cost benefits to both installers and end users as devices can be sourced locally and existing Internet connections can be utilized as the transmission path.

It should be noted that these solutions do not use or rely on the services of a VoIP service provider. A fully controlled connection direct from the VoIP ATA device to the monitoring server effectively creates a private network.

CONS: All fixed wire IP solutions are subject to sabotage from "line cut" which prevent devices connecting to the network.

Dual Path Signaling

Even trusty old PSTN was not immune from network failure and was definitely prone to line cut attacks. The line cut vulnerability has been removed with the supervised connections incorporated by IP and GPRS solutions but it is clear that even they cannot guarantee 100% network uptime.

With this in mind, many consumers refuse to rely 100% on a single transmission path and insist on a secondary backup path. There are several combinations that can be used to provide a dual path solution with different levels of security.

The lowest level dual path solution is provided by using a combination of PSTN and GSM. As PSTN continues to decline and neither path allows for cost efficient network supervision, this is not a future-proof option.

A more popular combination for cost sensitive applications is the use of the Internet as the primary path and GSM Voice as the secondary path. The Internet path benefits from network supervision and the GSM path can take over if the primary path fails. Certain model VoIP ATA's used in conjunction with GSM dialer have the ability to send signals over the Internet when a panel dials the primary telephone number and over the GSM network when it dials the secondary telephone number.

A similar level of security can be provided by using GPRS as the primary path and PSTN as the secondary path. Some solutions providers claim a dual path capability by using GPRS as the primary path and GSM Voice or SMS as a secondary path. Others claim dual path capability by using two GPRS SIM cards. These claims are somewhat misguided as a GSM jammer will effectively prevent all communications over the GSM network regardless of which method is used. GSM can only ever be treated as a single path even though it allows for 3 different methods (SMS, Voice & GPRS) of transmission.

High security applications demand two independently supervised transmission paths and this is usually achieved by using the Internet as the primary path and GPRS as the secondary path. Both are fully supervised, so even if the primary Internet path fails the system is left with a supervised alternative path.

Some solutions providers claim that by using a combination of broadband Internet, GPRS, GSM, PSTN and Dialup Internet their product supports 5 paths. As both broadband and Dialup Internet generally depend on the availability of a PSTN line and GPRS depends on a GSM connection a more accurate claim would be that such a solution can use 5 different methods of communication over two independent transmission paths. A dual path solution with "bells and whistles".

Remote Programming and Audio Verification

If it is important for your company to retain the ability to remotely program control panels or to open up a two way audio connection to the monitored site then you should carefully consider which of the above mentioned solutions you chose.

It is not possible to open up an audio path using GPRS. It is possible using GSM voice and PSTN, however, both usually attract call charges. You should check that the solutions provider supports both client and server initiated remote programming connections to the panel.

Some control panel manufacturers allow remote programming over the Internet but this method is proprietary and restricted to their particular brand. The preferred universal method is to use an audio connection over the Internet from a solution that incorporates a VoIP ATA as the primary transmission device. Such devices have the ability to reliably transmit alarm signals, allow operators to have two way

voice conversations and allow Alarm Companies to remotely program any make of alarm panel over the Internet.

Summary

The cost and availability of the various networks, existing equipment and infrastructure, insurance requirements and other concerns may ultimately determine which solutions you chose to migrate from the analogue to digital world.

My hope is that this article has helped cover some of the more technical aspects of the decision making process and makes your transition as smooth as possible.