Trolley Scan (Pty) Ltd

P.O.Box 59227
Kengray
2100 South Africa
Tel (+27) 10 237 0675
Fax (+27) 86 617 8002
Email:info@trolleyscan.com
Web:http://trolleyscan.com

TROLLEYPONDER/ECOTAG/RADAR RFID Newsletter #96

27 March 2013

Your latest copy of our regular newsletter keeping you up to date with developments.

Contents

1. Different operation frequencies allocated to RFID

The most important criteria to select in choosing an RFID system is its operating frequency. The choice of frequency determines the performance that can be expected from the system.

The world is divided into three regions for frequency plans which are then accepted or modified by the individual countries in the region.The regions are - Europe & Africa, North & South America, and Asia(excl Russia) with Australia.

The regions draw up the masterplans for the management of the radio spectrum and these are then adapted and accepted by the individual countries in those regions. This means that for major issues there are blocks of frequencies allocated in the different regions, such as for example cell phones. Minor applications, such as RFID, are fitted in by the individual countries between the big blocks and as a result there are nearly 177 different plans for RFID globally.

Because different frequencies will give different performance, there are five groups of frequencies allocated for RFID by the individual countries.
These are typically

1) 125kHz
2) 13.56Mhz
3) approx 900MHz
4) approx 2.45GHz
5) approx 5.8Ghz

There are two modes of sending energy through space, namely magnetic and electric fields. Magnetic systems use coils to couple the energy into space and these coils can be quite small, but operating range is short. Electric field use antenna systems that are usually operating wavelength related - for example half wave dipole.

The wavelength is the speed of light divided by operating frequency. The wavelength at 100MHz is 3 meters, 900Mhz is 33cms, 2.45Ghz is 12cms, and 5.8Ghz is 5cms.

The electric field antenna collects energy passing and its collecting area is proportional to the wavelength squared. So a 900 Mhz system with a 16cm antenna size collects 7 times the energy that a 2.45GHz system can collect or 33 times the amount of energy a 5.8GHz system will collect. This reduction in energy collection with frequency means that a 900 Mhz is almost the ideal RFID frequency for passive systems having consideration for antenna size and operating range.
Lower frequencies would give more performance but would have much larger antenna systems.

For passive systems (that is where the transponder extracts its operating power from the energising field), typical ranges for the different operating frequencies are - 125KHz (2 centimetres), 13.56Mhz (1 metre), 900MHz (10 metres), 2.45GHz(1.2 metres) and 5.8Ghz (25 centimetres).

The 125Khz and 13.56MHz systems are magnetic coupled which allow them to operate in situations where electric field systems cannot operate, such as underwater, inside the bodies of humans and animals, and even inside blocks of metal. The 125khz transponder can be made very small, the most common being a coil 1 millimetre in diameter and 11 millimetres long.

In 1990 when the staff of Trolley Scan were involved in the development of a transponder that could be used for the labelling of items in a supermarket trolley, 900MHz as a frequency was only available in a few parts of the globe with many countries preferring that development happened at 2.45GHz, a frequency that was already allocated to microwave ovens which had very poor frequency stability.

After Supertag(tm) was developed and demonstrated in South Africa(1994), the interest globally in RFID took off and countries slowly realised that they needed to allocate a frequency for RFID in the 900MHz region in order for their countries to stay competitive. By 2013 virtually every country in the world has finally allocated part of the spectrum at 900Mhz for RFID.

Trolley Scan have a technical paper explaining these choices which can be requested Interested? - Use this link to be sent the white paper.
mailto:info@trolleyscan.com?subject=Send_Frequency_performance_RFID_white_paper

2. Server attacks
This section relates to some observations that would be of interest to readers who operate internet servers and please skip if not of interest.

For the past 16 years Trolley Scan have been serving information from a stand alone webserver running a linux operating system. The server supplies about 2.5 million documents per annum in the form of HTML, PDF and JPG files. In the whole 16 years, on only about five occasions has it stopped and needed a reboot. Two of these stoppages have happened in the past three months and as a result we have been investigating the cause. Usually nobody looks at logfiles as everything is running smoothly until there is a problem.

Particularly with what has recently happened with attacks in South Korea in the past weeks, internet security is becoming an issue.

We found that the reason the machine had stopped was due to simultaneous attacks from about 300 machines distributed all over the globe on our server at virtually the same instant. This

overloaded a stack causing the machine to stop.

What was interesting about the attack was the distribution of the attacking servers and their time coordination. We have since limited the number of child processes that can be started at any time and made the machine bullet proof.

On further analysis of the historical logfiles, we found that our machine was being probed by very many servers continuously. This takes the form of sending the server an email to a fictitious user on our server to see if our machine would acknowledge that the user is UNKNOWN.
Once again the probing is coming from no single source but is routed through 3000 different slave servers around the world, but particularly from Russia, Belarus, Kazakistan and Vietnam. We have recorded about 100 000 of these attempts over the past 4 weeks.

Because we have the logfiles and are experts at data processing and analysis, we find so far that about 3000 slave servers are being used to do this probing. They are connected as all the probing messages are the same with just part of the destination address changing. What is interesting is the use of individual slave servers is kept to once or so per week so that unless you have a long data set you will not notice the pattern. One can find the more important machines in the probing as they often use multiple IP addresses from the same server or group of servers.

We then started blocking the probing from the more noticeable servers by listing them in the access.db file. This sent them an ACCESS DENIED message and they immediately knew that we knew who they were. This brought upon us a major storm, like hitting a bee hive. Whereas when we started this we were getting 1000 probes a day, we are now getting 8000 a day but have identified and blocked 85% of all probes. However new slave servers are being added all the time and whereas initially almost all the attacks were from Russia and Belarus, now many parts of the Western World are also involved in the attacks. These attacks are coordinated as at times all is very quiet and then the messages start coming fast and furious from all parts for an hour or so and then stop.

In the past when we have had attacks, there were a few machines and you could see a coordination that might be with many people in a club all agreeing to do something at some time. We tracked these and blocked them and weathered the storm.

This time we are convinced that the slave servers have been infected with a virus that allows some controlling body to coordinate and route targeted messages on their command and receive the feedback without the owners knowing. As the slave servers are only occasionally used for these messages, the existence of the virus is undetected.

This whole exercise has become a James Bond like scenario. This server is really unimportant in the commercial sense as it has no commercial value and is just a repository for documents - i.e. it is not a bank server and it does not hold confidential information. It is only operating at 1% usage, it has a lot of spare resources and is a long way from being overloaded and is bulletproof after we closed the last loophole. Every time we get sent a probe, it is collected and added to a database that allows us to reverse understand the attacking structure and to see our impact on the probing.

At present we are blocking 2984 servers that have been involved in multiple attacks on our server in the past four weeks, but we suspect this number might grow to 10000 when some of the servers that have only been used once are reused - unless someone discovers the virus in the client servers.

Want more info such as a list of attacking servers?

mailto:info@trolleyscan.com?subject=Server_attack_send_more_info

3. Product range

Trolley Scan are a manufacturer of UHF RFID systems. Trolley Scan manufacture fixed readers, portable readers and RFID-radar systems (Real Time Locating systems that give accurate position information) as well as a variety of transponders for different applications. Transponders come in the form of passive transponders with operating ranges up to 20 metres and battery assisted transponders with an operating range up to 40 metres. Trolley Scan also combine some of these components into packages for end users which are supplied with the appropriate software. Typical applications are asset management, notebook tracking, equipment barriers, store control, sheep and cattle tracking, event logging and sports timing systems.

Trolley Scan have been delivering their RFID solutions for the past 15 years and offer full support for all their equipment.

4. Getting your own complete RFID/radar system

You can order RFID systems or RFID-radar systems from Trolleyscan.com

Trolley Scan provide small RFID reader systems which give new users the ability to evaluate UHF RFID and their applications without needing specialised skills.

Trolley Scan provide a variety of easy starter systems for first time users who have an application that needs a solution. Typical packages are :

- Standard UHF long range readers with antennas and 100 transponders
- RFID-radar system comprising long range reader, antennas and a variety of different transponders.
- RFID-asset tracking systems comprising portable reader, antenna and a variety of transponders with software.
- RFID-notebook/laptop tracking system comprising reader, antennas, transponders and software

In addition components such as readers and transponders are available

These systems are already operating in 52 countries.

To find out details of the systems and to order see http://trolleyscan.com/