Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Emergency Alert Systems over Private Network Using Message Broadcasting

B.Venkata Phani Raja Rao[1], K.R.K.Sateesh[2]
Department Of Computer Science and Engineering,
Madanapalle Institute of Technology and Science, Madanapalli,
Chittoor, Andhra Pradesh, India-517 325.

Abstract: -SMS is a superior approach for transmission of EAS messages i.e.broadcasting critical information during emergency situationos to protect lives and properties of people. Several departments has joined with third-party providers to provide efficient solutions, regrettably they do not work efficiently due to the limitations in cellular communication system. To provide an alternative approach in this paper we have described about message broad casting over private networks. And also we describes about security issues and limitations with this approach. And finally we analyze cell broadcasting as a means of current approaches to third-party EAS. In doing sowe demonstrated that this progressively implemented security infrastructure does not accomplish its acknowledged requirements for large populations.

Index Terms: SMS, broadcasting, security, private networks.

I. Introduction

Text messaging is the act of typing and sending a brief electronic message between two or more mobile phones. This is used for wide verity of applications like chatting, to coordinate meetings, vicious circle up on gossip, put forward reminders of an event or even vote for a participator on a television game show, this discreet form of communication is now the dominant service offered by cellular networks. In some countries text messaging can be used to contact emergency services. In UK, text messages are used to call emergency services this can be only after registering with the emergency SMS service. This emergency service is primarily aimed at people who by reason of disability, are not capable to make a voice calls. Accordingly we can implement an emergency alert mechanism to send an emergency message during emergency situations like earth quakes, storms, fire accidents in a particular location etc. However, with voice-based phone services being almost completely unavailable, SMS messages were still effectively received in even the most crammed regions because the control channels responsible for their delivery remains available.

With a huge number of cellular towers damaged by the storms text messaging allowed the communication lines to remain open for a lot of individuals in need, in malice of their inability to complete voice calls in areas where the equipment was not spoiled and power was available. Consequently, SMS messaging is now viewed by many as a reliable method of communication when all other means appear unavailable. As response to this acuity, a number of companies offered SMS-based emergency messaging services. Boasted as able to deliver critical information organizations like colleges, universities and even municipalities hoping to coordinate and protect the physical security of the general public have spent tens of millions of dollars to install such systems. Regrettably they do not work efficiently due to the limitations in cellular communication system. In this paper we demonstrated an alternative approach to this problem. By constructing awireless environment as location oriented we can transmit the message to the nodes present in that location. In this paper we have demonstrated the approach by using Bluetooth. At last we analyzed the limitations during this approach.

II. Background Work

The Bluetooth technology is divided into two specifications: the core and the profile specifications. Core specification discusses how the technology works while the profile specification focuses on how to build interoperating devices using the core technologies. This paper deals with the core technology, and focuses on the lower layers of the Bluetooth architecture (up to the link manager).

The Radio Frequency Layer

The Bluetooth interface is based on a regular antenna power of 0dBm (1mW) with extensions for operating at up to 20dBm (100mW). The interfaces comply with most countries' ISM band rules up to 20dBm. The radio uses Frequency Hopping to spread the energy across the ISM spectrum in 79 hops displaced by 1MHz, with the range of 2.402GHz - 2.480GHz. The nominal link range is 10 centimeters to 10 meters, but the range can be extended to more than 100 meters by increasing the transmit power.

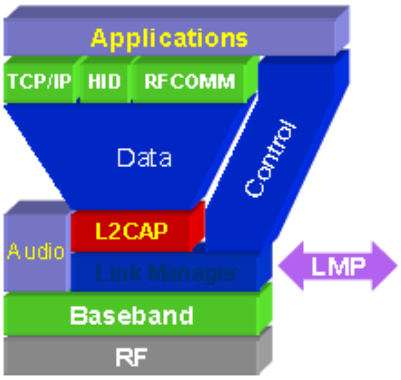

Figure 1: Bluetooth Architecture

As mentioned previously, the basic radio is a hybrid spread spectrum radio. Usually the radio operates in a frequency-hopping manner in which the 2.4GHz ISM band is broken into 79 1MHzbchannels that the radio randomly hops through while transmitting and receiving data. Piconet is formed when one Bluetooth radio connects to another Bluetooth radio. The both radios then hop together through the 79 channels. Bluetooth radio system supports a large number of piconets by providing each piconet with its own set of random hopping patterns. Some times Piconets will end up on the same channel. When this situation occurs the radios will hop to a free channel and the data are retransmitted. The Bluetooth frame consists of a transmit packet followed by a receive packet each packet can be composed of multiple slots (1, 3, or 5) of 625us. Multi-slot frames allow higher data rates because of the elimination of the turn-around time between packets and the reduction in header overhead. The eventual goal of this investigate is to examine the feasibility of a scalable system that is able to dispense context-aware content to possibly large mobile groups via the Bluetooth wireless communication. In order to attain this we need:

- A server with a Bluetooth Access Point,
- A group of people with Bluetooth-enabled devices, and
- An external database storing the content that needs to be distributed.

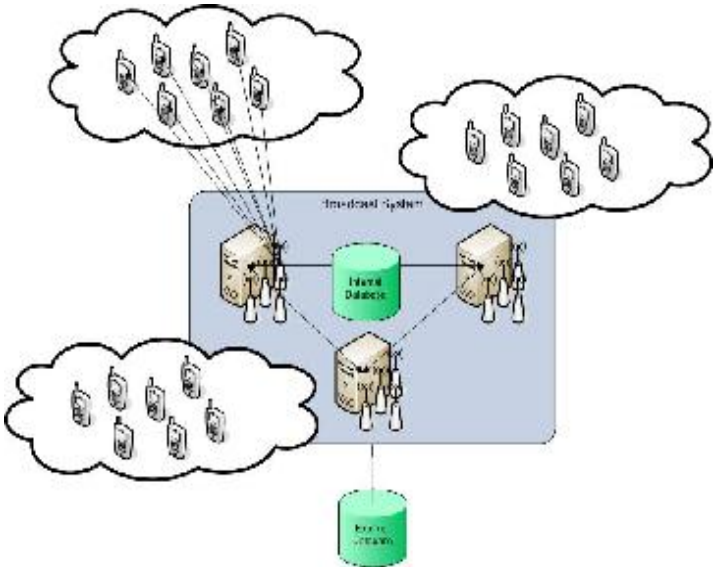

Figure 2: Global Architecture

Figure2 shows how the different components are working together. Those servers equipped with Bluetooth Access Points retrieve the content they distribute from the external database. Bluetooth Access Point is responsible for discovering Bluetooth enabled devices in range and establishing a connection over which the content may be distributed. An each access point may have connections with multiple Bluetooth-enabled devices and the internal database stores the logs and overhead for the Access Points to work together successfully.

IV. Related Work

Broadcasting with Bluetooth did work with a few devices and at the same time since Bluetooth allows up to seven connections to one Bluetooth radio at the same time. By building a passive system where the user is the one which requests information it also will not affect users' privacy. Nevertheless, my research also found a few issues with the Bluetooth which might affect a broadcast, the most obvious of them being the somewhat low transfer rate, an issue with device detection not always working when a lot of users are doing device discovery at the same time. Basically, while it is possible to use Bluetooth for broadcasting, it might be problematical to use it for targeting a large audience.

Passive and Active Broadcasting

Broadcasting from a central point is known as passive broadcasting. In this approach a central point is selected to broadcast the message and Bluetooth hardware called transmitter is installed. This equipment is handled by a monitor or a pc. This is a process of carrying one or more Bluetooth broadcasting units and roaming around different places finally collects the overall delivery reports of message.

Alterwave

Alterwave means Bluetooth access points as 'hot spots', which are maintained by a central server like most other companies. As Alterwave supports the features, they follow their competitors in given that support for the distribution of MP3, applications, video and Java games. Alterwave doesn't provide any details concerning to the class of the Bluetooth transceiver used and the number of simultaneous connections those are takes place.

Scalability of Bluetooth Broadcasting

An important part of thesis is about the scalability of Bluetooth broadcasting technique. Since scalability can sometimes be a fuzzy concept, we give a small explanation of the term. A significant aspect of software products is how they are able to deal with development. For example, how does the system handle an increase in data traffic or users? This property of a software system is usually referred to as scalability. A more detailed specification can be given as: 'Scalability is a desirable attribute of system or a network, or process. The concept connotes the ability of a system to accommodate an increasing number of objects or elements, to process growing volumes of work elegantly, and/or to be vulnerable to enlargement'. Any system that meets these requirements one can say that the system scales. In this thesis scalability comes downwards to the issue if the system is capable of dealing with large groups of users with Bluetooth enabled devices capable of receiving simple text messages.

V. Proposed System

As a short-range wireless protocol, Bluetooth was initially proposed as a cable replacement. These days, Bluetooth has outgrown its original purpose and is now also used for a variety of other applications. A mounting domain is its use for proximity marketing, i.e. the localized wireless circulation of advertising content associated with a choosy place. Content, changing from simple text messages to MP3, business cards, video or pictures are broadcasted to passing clients. How do these systems handle with large groups of mobile users? In this thesis we investigate what the hardware and software requirements are to set up a scalable message distribution network to distribute location-based information. Broadcasting is of mainly two types one is

A. Baseband

Bluetooth operates in the Industrial Scientific Medical (ISM) frequency band, centered around 2.4GHz. It uses a binary Gaussian–shaped Frequency Shift Keying (GFSK) modulation, with a bit period of 1 ¹s, achieving a raw bit rate of 1 Mbit/s. A fast frequency hopping spread spectrum scheme is used to limit interference from and to other radio devices operating in the same band. The frequency band is partitioned in a set of 79 RF channels, 1 MHz wide each. The carrier frequency jumps in this set, on the basis of a pseudo–random hopping sequence, with a nominal hop rate of 1600 hops/s (1 hop every 625*¹s*). In order to communicate, Bluetooth units have to be organized in a small network, called *piconet.* A piconet can host up to eight active units, one of which assumes the role of master, while the others become slaves. All the units in the same piconet are time and frequency synchronized to a Frequency Hopping channel. The frequency hopping sequence can be uniquely derived from the Bluetooth address and clock of the master unit. Transmissions can directly occur between master and slaves only. Duplex communication is obtained by a slot–based Time Division Duplex scheme. Time is divided into consecutive slots that are used for downlink (master-toslave) and uplink (slave-to-master) transmissions, alternatively. Each slot has a duration of *T*slot = 625 *¹s*. In general, the carrier frequency is changed at each time slot. However, the carrier frequency cannot be changed during the transmission of a packet, so that multi–slot packets are transmitted on the same frequency. In order to prevent collisions among units in a piconet, the master employs a simple polling technique to enable each slave unit to transmit. On the basis of this scheme, only the slave addressed by a downlink packet is allowed (and required) to transmit a packet to the master in the following uplink slot. The master can poll the slave implicitly, by using a useful data packet (if any), or explicitly, with a short control packet (POLL) that does not contain the payload field. The receiver slave is required to reply immediately to the master by transmitting a data packet or a special control packet (NULL) with no payload.

Application prototype

Figure 3: Login page of application

B. Data packet formats & Reception Mechanism

Bluetooth supports both synchronous connection oriented (SCO) and asynchronous connectionless (ACL) links. SCO links are used for voice traffic, while ACL links provide a basic point–to–point connection for asynchronous data traffic. In the following of this paper, we will consider ACL links only. An ACL packet can extend over an odd number of consecutive slots, namely, one, three or five slots. The transmission of a new packet is preceded by an idle period of 220 ^{1}s. This period is used by units for processing the previous packet and synchronizing on the new carrier frequency. Each baseband packet contains three main fields: Access Code (AC), Packet Header (HEAD) and, optionally, Payload (PAYL), as depicted in Fig. 1. The AC field is used for synchronization and piconet identification. All the packets exchanged within the same piconet have the same AC field. The AC is 72–bit long and contains a synchronization word that assures a minimum Hamming distance of 14 between ACs of different piconets. At the beginning of each receive slot, the Bluetooth receiver correlates the incoming bit stream against the expected synchronization word. For an incoming packet to be recognized, the correlate output has to exceed a given threshold. The receiver–correlated margin, denoted by *S*, is the distance between the maximum correlated output (perfect matching between incoming and expected AC words) and the correlate threshold. Hence, an incoming packet is recognized only whether the gap between actual and maximum correlated outputs falls within the correlated margin *S*. In this case, the HEAD field is also received and decoded; otherwise, reception stops

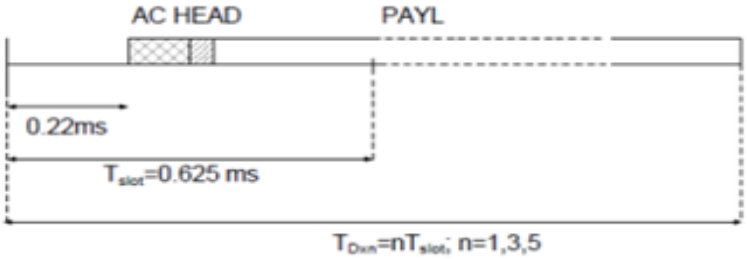

Figure 4: Bluetooth data packet format

And the units sleep until the successive receive slot (approximately two slots later). Note that, the value of the correlated margin *S* is not specified by the standard. The access code field is followed by the packet header (HEAD). It contains 18 bits, coded with a 1/3 forward error correction code (two–time repetition of every bit), resulting in a total field length of 54 bits. HEAD contains link control information, including packet type, destination address, sequence number and acknowledgment flag (ARQN). HEAD includes also an 8 bit Header Checksum field (HEC) that is used to check the integrity of the HEAD information after decoding. If the HEC test fails, the receiver switches off until the following receive slot (approx two slots later). Otherwise, the unit checks the 3–bit destination address field in HEAD. If the unit is not the intended recipient of the packet, then it switches off the transceiver and sleeps until the first receive slot *after the end* of the incoming packet. In this case, indeed, the unit can determine the packet type from the appropriate field in the packet header. Hence, it will not wake up before the packet has been completely transmitted by the sender. In general, AC and HEAD fields are followed by the payload field. However, POLL and NULL packet types contain no payload. Such packets are used whenever a unit is required to send a packet, e.g., for polling a slave or acknowledging the reception of a packet, and there is no data available to the designed destination. Except for POLL and NULL, the other ACL data packet types include a data part (PAYL) that can extend over one, three or five consecutive slots. The PAYL field can optionally be protected by a (15, 10) shortened Hamming code, which is able to correct all single errors and detect all double error in each codeword. Unprotected packet formats are usually denoted by DH5, DH3 and DH1, for the 5, 3 and 1-slot long types, respectively. Analogously, DM5, DM3 and DM1 are used to denote the corresponding protected formats. The main characteristics of the six different data packet formats provided by Bluetooth are summarized in following table.

Table1: Data packet formats

	Number of slots	PAYL FEC	PAYL-data length (bit)	Total packet length (bit)
DM1	1	Yes	136	366
DH1	1	No	216	366
DM3	3	Yes	968	1626
DH3	3	No	1464	1622
DM5	5	Yes	1792	2870
DH5	5	No	2712	2870

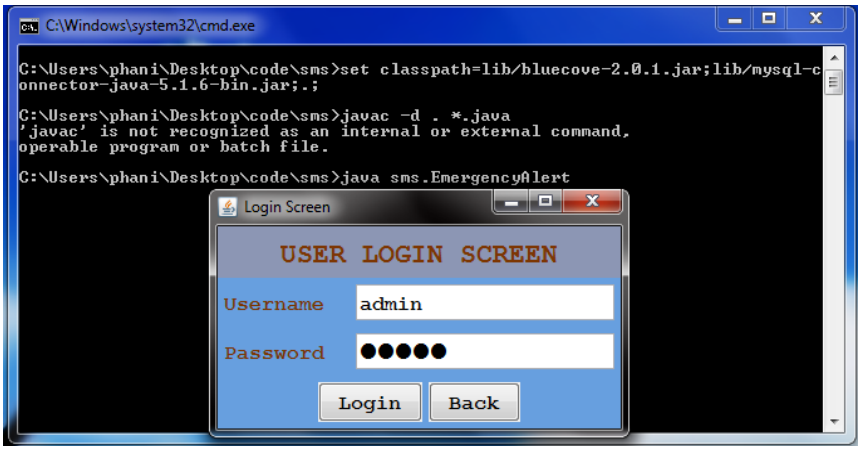

Figure 5: Authorized Login

This is a java based application intended to transmit more specifically broadcasting message to all Bluetooth enabled devices. Application will prompts for authentication, on successful login one can type the EAS message and prompt for transmission. Following figure describes the receiving of testing EAS message.

Figure 6: EAS message receiving

V. Performance

About JAVA

Java technology is both a programming language and a platform. With most programming languages you either compile or interpret a program so that you can run it on your PC. The Java language is unusual in that a program is both compiled and interpreted. Using the compiler first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java platform. Interpreter parses and runs each Java byte code instruction on the computer.

Performance:

Devices with Bluetooth, having various types of accessing methods and limited accessing to the devices that makes less capabilities of transmission. And also having less transmission ranges of Bluetooth makes limited transmission. Using multiple hot-spots we can able to cover small area like a college campus only. The fact that it only supports seven connections is also a limitation.

VI. Conclusion and Future Work

Bluetooth broadcasting might not be quite as flexible as it was hoped to be in the beginning of this project. It is not possible to simply set up a broadcast to send a EAS messages and hope that "everyone" will be able to access them. Without the user test, the conclusion will have to be that Bluetooth broadcasting is not quite as flexible as expected, due to the variations in how Bluetooth devices handle incoming files. This inflexibility makes the usage areas for Bluetooth broadcasting somewhat limited. Still, even using just the most supported files it should be quite possible to set up a quite functional Bluetooth broadcast. A Bluetooth broadcast can be quite a useful addition to the traditional information brochures! And with devices continuously evolving and the Bluetooth technology being improved, it is possible that Bluetooth broadcasting can be used for delivering a wider range of information in the near future at higher speeds than now. Therefore, Bluetooth broadcasting as a channel for delivering information definitely has potential as a technological solution. Accordingly, it is critical that technologists, legislators, and the general public understand the fundamental

limitations of this mechanism to safeguard physical security and public safety and those future solutions are thoroughly evaluated before they are deployed.

References

[1] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial of Service with Capabilities," Proc. ACM Workshop Hot Topics in Networking (HotNets), 2003.

[2] K. Argyraki and D.R. Cheriton, "Scalable Network-Layer Defense against Internet Bandwidth-Flooding Attacks," ACM/IEEE Trans. Networking, vol. 17, no. 4, pp. 1284-1297, Aug. 2009.

[3] Associated Press, "Man Admits Sending 'Monkey Out of Cage' Message," http://www.google.com/hostednews/ap/article/ ALeqM5gjBi_YGzVmUqV0YDKifMv, 2009.

[4] S. Blons, "Emergency Team Aids Efforts," http://graphic. pepperdine.edu/special/2007-10-24-emergencyteam.htm, 2007.

[5] M. Casado, P. Cao, A. Akella, and N. Provos, "Flow Cookies: Using Bandwidth Amplification to Defend against DDoS Flooding Attacks," Proc. Int'l Workshop Quality of Service (IWQoS), 2006.

[6] Cellular-News, "Malaysian Operators Dismiss Hoax SMS," http://www.cellular-news.com/story/31247.php, 2008.

[7] T. Christensen, "Ga. Tech Building Cleared After Blast," http:// www.11alive.com/life/pets/story.aspx?storyid=106112, 2007.

[8] CollegeSafetyNet.com, http://www.collegesafetynet.com, 2008. [14] Courant.com, "University Emergency SMS Service Doesn't Deliver," http://www.courant.com, Nov. 2007.

[9] B.K. Daly, "Wireless Alert & Warning Workshop," http://www.oes.ca.gov/ WebPage/ oeswebsite.nsf/ClientOESFileLibrary/ Wirel, 2011.

[10] e2Campus, "Mass Notification Systems for College, University & Higher Education Schools by e2Campus: Info on the Go!" http:// www.e2campus.com, 2008. P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 40-53, Feb. 2009.

[11] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. La Porta, and P. McDaniel, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," Proc. ACM Conf. Computer and Comm. Security (CCS), 2009.

[12] P. Traynor, P. McDaniel, and T. La Porta, "On Attack Causality in Internet-Connected Cellular Networks," Proc. USENIX Security Symp., 2007.

[13] Bluetooth Specifications, Bluetooth SIG at http://www.bluetooth.com/.

[14] Reverse 911, "Reverse 911 - The Only COMPLETE Notification System for Public Safety," http://www.reverse911.com/index.php, 2008.

[15] Roam Secure, "Roam Secure," http://www.roamsecure.net, 2008.

[43] shelbinator.com, "Evacuate! or Not," http://shelbinator.com/2007/11/08/evacuate-or-not, 2007.

[16] Simon Fraser Univ., "Special Report on the Apr. 9th Test of SFU Alerts," http://www.sfu.ca/sfualerts/april08_report.html, 2008.

