An Internet Public Alerting System: A Canadian Experience

Nabil Seddigh
Solana Networks
nseddigh@solananetworks.com

Biswajit Nandy
Solana Networks
bnandy@solananetworks.com

John Lambadaris
Systems and Computer Engineering Dept., Carleton University
ioannis@sce.carleton.ca

ABSTRACT

Public officials have the responsibility of giving public directions and issuing warnings in the event of an emergency. Traditionally, siren systems, radio and television have been used as the primary means for issuing public alerts. Recently, there has been increased interest in evaluating the Internet's suitability for issuing public alerts during times of emergency. This paper presents a Canadian experience with the design and trials of an Internet-based emergency public alerting system (IPAS). We discuss a proposed set of requirements and system architecture. We also include a discussion of the challenges to be overcome in developing such systems and report on experiments and field trials using the IPAS system developed during this project. Our objective is to provide motivation for future research and industry work in this area..

Keywords

Internet Public Alerting Canada Early Warning

INTRODUCTION

Disaster and emergency situations can arise at any time or place with the potential of endangering public lives and damaging community infrastructure. Public officials have the responsibility of giving public directions and issuing public alerts in the event of such emergencies. Diverse sets of approaches are required in order to expeditiously distribute public alerts related to potential hazards and emergencies. These approaches should harness the large variety of communication technologies at our disposal, including television, radio, public telephony system (satellite, land-line and wireless), electronic billboards and the Internet.

Traditionally, sirens, radio and television have been the primary means for emergency alerting of the public. In recent years, satellite-based receivers as well as automated phone dialers have also been utilized for emergency public alerting and warning. Recently, the interest in utilizing the Internet to issue public warnings and alerts has increased. With the convergence of voice and video over the Internet as well as emergence of wireless data devices, the Internet holds much promise as a viable complementary means to facilitate alerting of the public – especially during work hours.

This paper reports the results of a Canadian project in the area of Internet-based emergency public alerting. The project is the result of continuous collaboration between researchers, developers, and officials from the industry, academia, and Industry Canada. The work started in early 2003 with an initial investigation of using the Internet for emergency public alerting [5]. At that time, there were no strong Canadian efforts in this area. Since then, research and industry efforts have begun towards defining the software/networking infrastructure that would make such a system feasible for different levels of the Canadian government.

Through an Industry Canada sponsored program, the project undertook a detailed study of the requirements and architecture for an Internet-based Emergency Public Alerting System (IPAS). A system was developed using this design and deployed in 3 rounds of field trials (late 2004/early 2005) with a number of Canadian municipalities including Guelph, Ottawa, Brandon, Cornwall, Charlottetown and Sarnia. Other trial participants include Holland

College (Prince Edward Island), University of Saskatchewan IT Security services, Carleton University, North Carolina State University and Stevens Institute of Technology.

Potential users for an IPAS can include Municipal Emergency Planning departments and/or similar departments at the provincial or federal government. In addition, multi-site organizations and corporations with requirements for widespread real-time notification may have an interest in the results of this investigation.

The project included a detailed study of open issues related to developing a secure, scalable, robust IPAS system. A number of novel approaches were utilized when developing the proof-of-concept system and architecture. This included a new scalable high-performance transport protocol, multi-server protocols and architecture as well as a hierarchical scheme for issuing alerts.

The rest of this paper presents an overview of the requirements, challenges and architecture for an IPAS system. As well as a brief summary of field trials executed with a prototype IPAS system.

Related Work

This section reviews some of the relevant ongoing work in the area of emergency public alerting.

One existing alert system utilized by the United States Government is the Emergency Alert System (EAS) - a hierarchical, trickle down distribution system. The primary method of delivering alerts to state and local areas is over-the-air broadcast signals and cable systems. Research has shown [1] that stations "down the chain" may miss important messages. Stations sometimes decide not to air messages or delay the message. Traditional media such as EAS have a limited daytime audience as many people who are at work do not have access to radio or television. There are recommendations to use modern technologies such as the Internet and cellular networks to deliver alerts to workstations and mobile handsets of wireless subscribers directly [2].

Satellite-based systems have also been utilized for emergency public alerting. ComLabs EMnet messaging system [6] allows the user to send messages and warnings to individual stations or thousands of stations, simultaneously and instantaneously in a secure environment. It is an excellent mechanism for disseminating alert messages from a primary station to secondary stations for broadcast. It is not clear if this technology can suitably be utilized as an effective mechanism for alerting a large number of end users.

More recently, Internet-based systems are being utilized for some form of emergency public alerting. One such system has been developed by MyStateUSA. MyStateUSA provides an Internet-based communication system with secure, real-time alerting. The software can be integrated with existing information systems and databases via HTTP and XML, including the Common Alerting Protocol (CAP) [3].

A number of messaging systems have been adapted for use in dissemination of public alerts to end-users. This includes systems such as [9] and [10]. These systems were originally designed as chat clients and thus, do not include a number of must-have capabilities for mission-critical emergency public alerting systems. e.g. classes of users with security clearance permissions.

IPAS: REQUIREMENTS, CHALLENGES AND ARCHITECTURE

For a number of reasons, we designed the Internet Public Alerting System (IPAS) around the publish-subscribe architecture. Public Officials issue alerts to the system. Users receive published alerts that meet their subscription criteria. The system would comprise three components: end-user client, IPAS server, and web interface. In[5], we studied the possibility of an IPAS system where public officials sent alerts to end-users without the end-user having to subscribe. This approach was not pursued due to challenges with the current Internet architecture and netiquette. This includes challenges such as the following:

- Firstly, many end-users have dynamic IP addresses and so the system would not know which users to send alerts to.
- Secondly, most alerts need to be sent with some geographic scope. The area of mapping IP addresses to geographic regions is not mature enough at the present to pursue this option.
- Finally, since spam and unsolicited emails have caused many legal concerns, it is unclear if Governments would wish to become embroiled in such an approach until such time as clear policies and regulations are in place.

The end-user client software must be installed on the user's computer and allows the user to manage their subscription criteria, account information, and retrieve alerts. Public Officials and System Administrators use the web interface to publish alerts and manage the system. The back-end for IPAS must be robust, scalable and secure.

Figure 1 illustrates IPAS operation. The IPAS architecture should provide support for transmission of voice or video alert messages if required as well as disseminating the alerts to a variety of end-client terminals including cell-phones and wireless PDAs. Though the Internet does not have widespread current support for Differentiated Services [4], the widespread interest in VoIP leads us to believe that any viable IPAS system will need to include support for voice-based alert messages. Our initial studies in the project [5] lead us to believe however that the current Internet cannot viably support voice-based alert messages with high volumes.

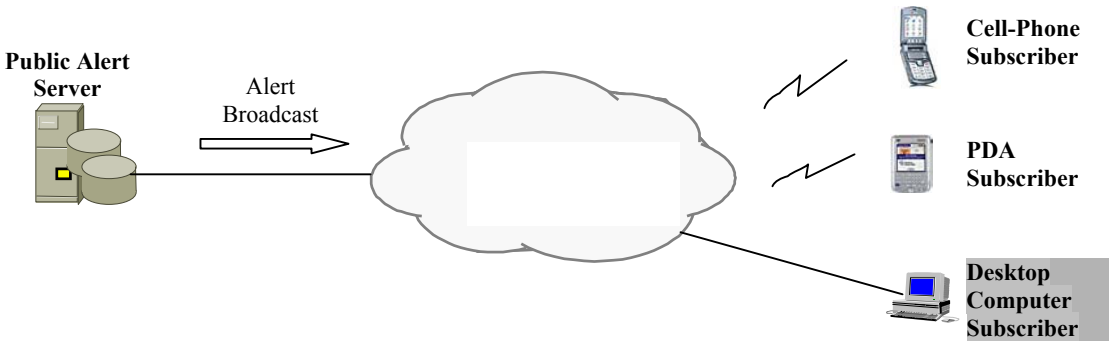

Figure 1. Alert Dissemination to a Variety of Devices

Requirements

Through detailed study, we have identified a series of requirements which we believe are essential for a viable IPAS system. These requirements include:

- **Security** - The system should have elaborate security access measures built in. One aspect of such security ensures that only the appropriate officials with requisite authorization can issue public alerts. This can be achieved through a database of users in the form of access-lists. Another aspect of security ensures that there is privacy of information for those who issue or receive the alerts. There should be support for a variety of authentication and authorization mechanisms. Such security measures are extremely important for a national, provincial and regional alerting system. Various alerts have different scope (e.g., weather alerts may have a local scope while terrorism alerts may have a national scope) and will be issued/received by people at different levels. The proposed system should be designed with a built-in security infrastructure that would ensure requisite authorization or authentication and data encryption for various types of notification. In addition, the system must be able to operate successfully in the presence of firewalls, pop-up blockers and other defensive security systems commonly deployed on the Internet.
- **Remote Alerting** - The system should support remote issuing of alerts. Officials should be able to initiate a public alert broadcast from any remote location. e.g. if an Ottawa-based official is visiting Vancouver, he/she should be able to access a server in Ottawa to issue a Nation-wide alert (assuming the official has the requisite authority to do so).
- **Real-Time Notification** - The system should utilize a pop-up window approach for disseminating information. Users should be required to register for emergency alert notification with the server. In the event of an emergency alert broadcast, the alert message will pop-up in a small window on the subscribed user's computer. The email approach to public alerting was considered but not selected since many people may have their computer turned on but not retrieve their email. Email is useful for non-real-time public alerting.

- **Portability** - The public alert client should be portable across a variety of common operating systems such as Windows, Linux, Sun OS, Palm, WinCE etc.
- **Scalable, Fault-Tolerant & Reliable** - The system should be implemented using a distributed client-server architecture. Such an architecture provides a basis for incremental system development and deployment. Deployment at a regional, provincial or national level can be undertaken incrementally (in a cost efficient manner) without affecting other parts of the Public Alerting System. For example, regional infrastructure can be added to provincial infrastructure with a minor configuration update. Scalability is another attribute that emerges from a distributed architecture through the use of multiple servers and an innovative server discovery mechanism. The system must also be fault-tolerant to failure especially at the time of disasters when the network is most likely to be under severe stress in terms of availability and traffic load. IPAS was designed to scale to support millions of users.
- **Efficient Transport protocol & Data Representation** – The system should be capable of disseminating large numbers of alerts to Internet users without unduly loading the network. In this regard, the project team developed IPAP (Internet Public Alerting Protocol) - an innovative transport protocol developed to meet the stringent performance requirements of IPAS) [7]. IPAP is a reliable transport protocol like TCP but is designed to yield high performance for small alert messages. Data representation for alerts should conform to CAP (Common Alerting Protocol) [3] which has recently been standardized.

Architecture

From the requirements of the previous section, it is possible to determine the broad elements of an architecture for IPAS. Figure 2 illustrates such an architecture within the Canadian context.

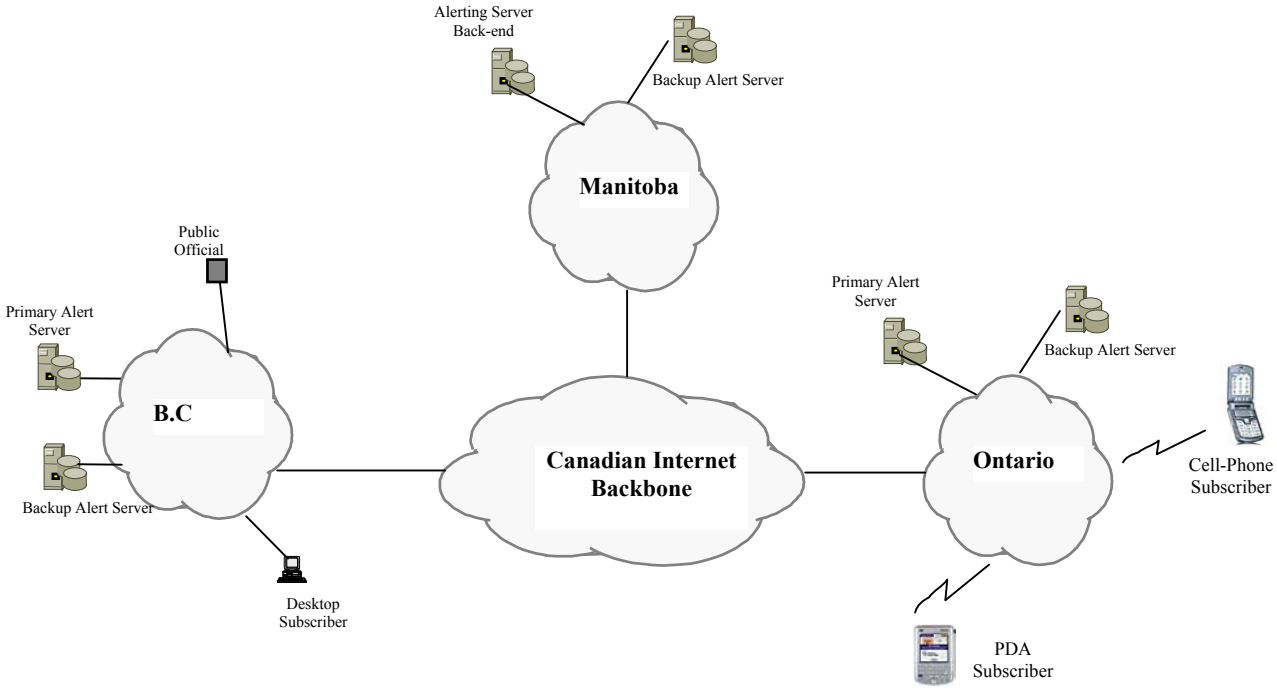

Figure 2. Alert Dissemination to a Variety of Devices

The public alerting infrastructure would consist of a set of alerting servers and clients. The alerting server can be deployed at the desired granularity based on the needs of the officials and the number of users. It is possible to have a single server serving an entire province. However, in time, due to the sheer volume of subscribers, it is expected that the server will be unable to serve the many different cities across the province. It is not difficult to envisage a time in the near future where each city will have its own server and in the case of larger cities, possibly a cluster of

servers. The figure also depicts a backup alert server. This is to ensure redundancy in the case of unexpected failures related to the primary server. Synchronization mechanisms will be in place to ensure that the backup server can take over from the primary server seamlessly should this be required.

Subscriptions would be stored in a distributed fashion at local servers without replication. This would distribute load across all servers, thus improving performance. The system should also be less complex in terms of managing the volume of data. Alerts would be sent to all the servers. Each server would then find the local users whose subscription matches the scope of the alert.

EXPERIMENTS AND FIELD TRIALS

The IPAS system was developed in 2004. The server was developed on a Linux platform using C++. The client software was developed in JAVA and was tested on Windows XP, Windows 2000, Windows 98 and Linux platforms.

A single IPAS server was deployed live on the Internet in June 2004. The first round of field trials was held in July 2004 with users from the cities of Ottawa and Guelph. A number of issues were understood and learnt from this field trial. An enhanced IPAS system was then developed and tested.

The enhanced distributed server version of the IPAS system was deployed live on the Internet in October with 2 servers hosted by different ISPs. The second round of field trials was held in November 2004 with a larger number of users including the Emergency Management officials for the municipalities of Guelph, Ottawa, Brandon, Cornwall, Charlottetown and Sarnia. Other trial participants included Holland College (Prince Edward Island) and the University of Saskatchewan IT Security services. A 3rd round of field trials was successfully held in February 2005.

Analysis of Results

The Field trials provided an opportunity to validate and test some of the assumptions behind the IPAS system. It also provided a vehicle for learning about deployment and design issues of such a system. Key learnings and conclusions as a result of the trials included:

- Reliability of Alerts - Due to packet losses on the current best-effort Internet, it is important for the alerts to be transmitted over a reliable protocol. In the case of IPAS, we ran experiments using two types of transport protocols: (i) a proprietary efficient transport protocol developed for this project (IPAP) and (ii) traditional TCP-based transport protocol. Use of a proprietary protocol could cause problems for users that sit behind a firewall in an enterprise network – a few such cases were encountered during the trial. The Internet Standards body, the IETF over a number of years has had periodic discussion about a reliable transport protocol that is tailored for small data transmissions and performs better than TCP. It may be timely for work to be initiated in this area.
- Alert Acknowledgement – After the first set of trials, some officials wanted the ability to determine how many end users actually read their alerts. It was not difficult to include the capability for the IPAS server to keep track of alerts that were delivered to IPAS clients reliably and the time that the alert was delivered. However, this was not sufficient for some of the officials. They wanted the users to click on the received alerts and an acknowledgement to be sent back to the server. Although this is not a particularly difficult scheme to build into the system, we had concerns about large numbers of users potentially sending acknowledgements to the same server around the same time. While this was not a concern for the size of trials that we held, we remain uncertain if this should be a built-in feature of the system.
- Alert Message standardization – At present there is no Canadian standard for the form and format of alert messages in a variety of mediums. For the purposes of this project, we defined a clear format for the various fields in an alert message. However, to avoid each public alerting system defining their own set of fields, there needs to be a clear standard. There are strong indications that Industry Canada is leaning towards adopting the CAP [3] protocol as the data inter-change format. This is clearly an important step forward. We started work on the integration of the CAP protocol into the IPAS system. This work is currently ongoing.
- Use of Client Application vs Email – One of the key points of discussion at the onset of the project was whether to utilize email as the medium for users to receive IPAS alerts or whether to develop a pop-up

window based application for the client. It was decided that email would not meet some of the requirements of real-time, security and reliability. Hence, the IPAS client was developed which displayed incoming alerts on user computers using a pop-up window. The application was designed to be light-weight and easy to install. Nonetheless, during trials, it appeared that some users would prefer not to install yet another application on their computer. However, for the great majority of users, this was a non-issue and they preferred the IPAS client application over email as it was a distinct public alerting application whereas email was a general purpose tool for communications of all kinds.

CONCLUSION

This paper presents a summary of preliminary results from our work on IPAS (Internet-based Emergency Public Alert System). This class of applications is expected to be widespread due the growing use of the Internet. We briefly discuss some of the issues associated with developing such a system, describe the architecture that is based on the publish-subscribe model and report on field trials utilizing the prototype system.

ACKNOWLEDGMENTS

We acknowledge the key contributions of Leo Paoletti, Don Bennett, Rupinder Makkar, and Nader Yared in relation to various aspects of the project. We are grateful to Kathleen McCrae and Wendy Wu of Industry Canada for their diligent review and input particularly during the trial phases of the project. We also acknowledge the helpful feedback from the various IT departments, Emergency Management departments and users from the municipalities of Brandon, Charlottetown, Cornwall, Guelph, Ottawa and Sarnia.

REFERENCES

[1] "The Emergency Alert System (EAS): An Assessment", February 2004 (PPW Report 2004-1)

[2] FCC Notice of Proposed Rulemaking on improving the Emergency Alert System August 2004, (EB Docket No. 04-296)

[3] Common Alerting Protocol v1.0. (2004) http://www.oasis-open.org/committees/download.php/6334/oasis-200402-cap-core-1.0.pdf

[4] Blake S et al, "An Architecture for Differentiated Services", RFC 2475, IETF Internet Informational RFC

[5] Lambadaris I et al. (2003) "A study and proposal for a Public Alert System using the Internet", Technical Report, May 2003

[6] ComLabs, http://www.comlabs.com/emnet.html

[7] Nandy B et al, "Detailed Design: An Internet-based Emergency Public Alerting System", Technical Report, March 2004

[8] http://mystateusa.net/pres5.cfm

[9] http://www.solvetech.com/products.aspx

[10] http://www.wiredred.com/active-alert-software/