Wireless Emergency Alerts

Computer Model and Simulation Results

July 2013

Homeland Security

Science and Technology

WIRELESS EMERGENCY ALERTS

COMPUTER MODEL AND SIMULATION RESULTS

Homeland Security

Science and Technology

July 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document describes work undertaken as part of the Wireless Emergency Alerts (WEA) Program, formerly known as Commercial Mobile Alert Service (CMAS), at The Johns Hopkins University Applied Physics Laboratory for the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T). A computer model was developed for the purposes of investigating WEA system performance under specific scenarios and to identify recommended enhancements. This report presents the modeling approach and the results of the simulations performed using the model. The results highlight potential improvements that should be considered by DHS and the Federal Emergency Management Agency (FEMA) in future iterations of WEA.

A public alert and warning system like WEA has to be able to operate continuously despite possible extreme conditions (e.g., massive infrastructure damage, heavy network traffic, cyber attacks). Because it is not possible to generate these conditions for testing in a controlled environment, a WEA computer model was developed to simulate the transmission of alert messages from alert origination through delivery to a citizen's mobile device. This report presents an analysis of simulated system performance under a variety of conditions, including scenarios with extreme conditions.

The WEA computer model was built using a discrete event simulation software package. The model employs a "black-box" approach because detailed design information about WEA system components was not available to the project team. With this approach, the model describes only the external behavior of the WEA components without detailed information about their specific internal design. The model employs numerous configurable equipment attributes, which can be tuned to reflect specific knowledge of these elements should additional design or performance information become available in the future. The model uses alert delivery latency as the main performance metric. In WEA, different handsets will in general receive an alert at different times. This variability is caused by several factors such as different service providers, different locations, interference and transmission errors, handset state, and so forth. The study described in this document simulated the effects of various delay factors on alert delivery latency.

The main finding of the study is that under normal operating conditions, WEA can alert the public with latencies under 5 seconds. A five-second latency is expected to be adequate for many types of alerts and warnings. On the other hand, WEA latency can exceed 20 seconds under certain extreme conditions, such as high levels of Internet delay that can be encountered during a major disaster, or high levels of cell broadcast traffic. The WEA alert delivery success rate is also strongly dependent on phone call volume because alerts are not received by mobile handsets during active phone calls. High levels of phone call volume can cause a significant portion of the target population to receive an alert delayed by several tens of minutes. Finally, target populations that have poor cellular reception may also have alerts delayed for several tens of minutes.

The project team evaluated numerous disaster scenarios as simulation scenarios. A representative subset of the scenarios was selected to study the potential effect of each major delay factor. The first scenario employed a series of weather alerts to investigate WEA performance as a function of background (non-alert) cell broadcast traffic load. WEA shares the same channel with other cell broadcast traffic. Therefore, alerts can potentially be delayed if a Commercial Mobile Service Provider (CMSP) sends substantial commercial broadcast to its subscribers. The simulation results revealed that WEA latency can exceed 20 seconds when the cell broadcast load is greater than 80%. Therefore, the study recommends that CMSPs planning to offer commercial cell broadcast services to their customers should assign a higher priority level to WEA alerts to reduce this latency.

The second and third scenarios, a chemical attack and a major earthquake, respectively, were employed to analyze the impact of extremely high levels of Internet delays (e.g., 1 second) and public alert traffic load on WEA performance. The simulation results revealed that WEA latency again exceeded 20 seconds under such extreme conditions. Most of the latency was due to the protocol overhead associated with a Hypertext Transfer Protocol Secure setup. The study recommends that Alert Originators (AO) who are expected to generate alerts with high delay sensitivity, such as earthquake and tornado warnings, use dedicated secure channels to reduce this latency. It also recommends the use of Internet Service Providers that offer Service-Level Agreements (SLAs) with guaranteed minimum bandwidth and maximum delay to reduce delays during extreme conditions. Services with such SLAs are typically more expensive, but can maintain a baseline service quality despite high network traffic.

The fourth scenario analyzed the impact of a denial-of-service attack on the alert Aggregator during a series of weather alerts. The findings reveal the need for strong defenses against this type of attack. The study recommends a distributed architecture for future enhancements to WEA. The existing centralized architecture would be unable to operate if the data centers were disabled by a cyber attack or other means.

The fifth scenario was a nuclear detonation. The study analyzed the impact of very high levels of transmission errors that can result from electromagnetic noise in order to gauge the delays in WEA messages caused by such transmission errors. WEA relies on multiple repeat transmissions of alerts to reach handsets that do not receive an alert during the first transmission. A variety of causes can increase the need for retransmission, including poor reception and active phone calls. Simulation results indicated that if 10% of the handsets cannot receive an alert due to transmission errors, three or more transmissions may be needed to alert at least 90% of a target population.

Lastly, the sixth scenario was another series of weather alerts, this time to analyze the impact of high levels of phone call volume. Similar to the fifth scenario, simulation results revealed that when there was heavy phone call volume (exceeding 50% load), four or more transmissions were needed to alert at least 90% of the target population.

The results in the fifth and sixth scenarios demonstrate the need for optimizing the alert transmission period. It must be tuned for the expected level of transmission errors and the expected phone call volume in an area. Selecting a large transmission period increases alert delivery latency for some portion of the target population; selecting a small transmission period consumes more network resources. Also, a small transmission period may lead to complaints and opt-outs by an over-alerted public.

The results presented in this document can affect a number of important technical, programmatic, and policy decisions that must be made or endorsed by the Federal Communications

Commission, FEMA, DHS, CMSPs, the AO community, and state and local first responders. WEA service is most critical in the very same circumstances when it is most susceptible to unacceptable degradations of service. The evolution of the WEA system must be coordinated in light of the consequences—for the public, for first responders, and for federal disaster response—of the degradation of service predicted by the WEA simulation results. AOs need to be aware of the worst-case consequences of alert initiation under extreme circumstances.

a. Alert Origination Systems (AOS) at the local, state, and Federal levels generate emergency alert messages for WEA using a data standard called the Common Alerting Protocol (CAP). These messages are transmitted to the Alert Aggregator via Interface A.

b. The Alert Aggregator receives, authenticates, and aggregates emergency alerts from the AOS's and forwards them to the Federal Alert Gateway.

c. The Federal Alert Gateway generates a Commercial Mobile Alert Message (CMAM).

d. Based on Commercial Mobile Service Provider (CMSP) profiles maintained in the Federal Alert Gateway, the Federal Alert Gateway delivers the CMAM over Interface C to Gateways maintained by the appropriate CMSPs.

e. The CMSP Gateway is responsible for formulating the alert in a manner consistent with the individual CMSP's available delivery technologies, and handling congestion within the CMSP infrastructure. WEA messages are mapped to an associated set of cell site transceivers and transmitted using Cell Broadcast Service (CBS) over the air interfaces.

f. Lastly, the alert is received on a customer's mobile device. The major functions of the mobile device are to authenticate interactions with the CMSP infrastructure, monitor for WEA alerts, maintain customer options (such as the subscriber's opt-out selections), and activate the associated visual, audio, and mechanical (e.g., vibration) indicators that the subscriber has chosen as alert options.

The WEA Reference Architecture forms the basis of the computer model architecture explained in Section 4.

their internal dynamics. This approach captured the external behavior of WEA components in the model, without internal details.

It is not feasible to simulate tens of thousands of cellular devices directly in OPNET Modeler or any other discrete event simulator. For this reason, the numbers of cell towers and cellular devices have to be scaled down during the simulation runs. In this case the results should be extrapolated to reflect the actual system performance.

The simulation of each scenario requires a schedule of WEA alerts relevant for that scenario to drive the model. Furthermore, each scenario may contain various external events that could be examined as part of the model. Therefore, events such as changes in equipment characteristics (e.g., being non-operational) or network characteristics (e.g., delays across Interface A or Interface C) are also inputs to a simulation analysis. To make the simulation configuration easy for the analyst to create and easy for the alert community of interest to review, all these events were expressed in a simple text scenario file ingested by the model.

The ability to examine the effects of equipment outages is a key element in the assessment of the effectiveness of WEA in response to certain types of events. This was accomplished by disabling the nodes and links that represent the failed equipment in OPNET Modeler. When re-enabled, most of these equipment models continue from the internal state they were in before being disabled. They do not support a more realistic recovery that represents the behavior of equipment in the process of coming back online. This was not a significant issue for the simulation scenarios selected in this study because the scenarios had durations that were too short to see any recovery after failure. For this reason, the disable feature was used without any need for creating custom code for recovery.

After an initial examination of the cellular system models available with OPNET Modeler, it was decided to customize two of them with the addition of CBS modeling:

a. A basic GSM model formerly developed for the Department of Defense (DoD)

b. The built-in LTE model in OPNET Modeler

The models of these two cellular systems were different enough that rather than trying to create a common capability used in both, a distinct, custom CBS model was made for each one.

OPNET Modeler also has a built-in UMTS network model. Adding CBS support to this model was considered as an option in the early stages of WEA model design, but because cell broadcast over UMTS networks is expected to show similar performance to cell broadcast over GSM networks, it was decided that the GSM and LTE models would be sufficient for the purpose of this work. If there is specific need to simulate UMTS cell broadcast, this can be accomplished by using a generic wireless broadcast model based on the built-in Worldwide Interoperability for Microwave Access model with radio characteristics made similar to UMTS. Future addition of CBS support to the built-in UMTS model is also possible, if desired.

Table 3-1 lists all WEA functional components and networks that have been modeled. Communication link models and models used for simulation configuration are not listed. The table also shows the base model used for each WEA component and added functionality to the base model to simulate the WEA system. A detailed description of each model is provided in Section 4.

Table 3-1 List of WEA Models

Modeled Functional Component	Base Model	Modification
Alert Origination		
AOS	Built-in workstation model	Added AOS functionality
IPAWS-OPEN		
Alert Aggregator	Built-in server model	Added alert Aggregator functionality
Federal Alert Gateway	Built-in server model	Added Federal Alert Gateway functionality
Networks		
Internet	Built-in Internet Protocol (IP) cloud model	None
CMSP Backbone Network	Built-in IP cloud model	None
CMSP (all)		
CMSP Gateway and CBE	Built-in Gateway model	Added CMSP Gateway and CBE functionality
CBC	Built-in Ethernet server model	Added CBC functionality
CMSP (GSM)		
Base Station Controller (BSC)	DoD GSM model	Added CBS functionality
Base Transceiver Station (BTS)	DoD GSM model	Added CBS functionality
Mobile Station (MS)	DoD GSM model	Added CBS functionality
CMSP (LTE)		
Evolved Packet Core (EPC)	Built-in LTE model	None
Enhanced Node B (eNodeB)	Built-in LTE model	Added CBS functionality
User Equipment (UE)	Built-in LTE model	Added CBS functionality

Table 5-2 Assumptions and Configuration Settings

Parameter	Value	Description
IPAWS-OPEN processing capacity	60 messages per minute	Each alert was assumed to take 1 second to process. This capacity matches well to the result in the IPAWS-OPEN Performance Test and Evaluation Report,[7] which states that an experiment to post 1000 alerts took 17 minutes to complete.
IPAWS-OPEN traffic load (normal conditions)	Negligible	Normal alert volume is assumed to be very small compared to IPAWS-OPEN capacity. Two additional stressed conditions are defined in Section 5.3 with significantly higher load levels.
Average Internet delay (normal conditions)	50 ms	The average latency for normal conditions was picked based on latency values reported by various service providers and Internet traffic measurements.[8] [9] [10] [11] The AOS's and IPAWS-OPEN were assumed to be connected to the Internet by different service providers. Two additional stress conditions are defined in Section 5.3 with significantly larger delay.
Alert message priority	Normal	Alert messages were assumed to be imminent danger messages and to have the same priority as non-alert cell broadcast network traffic.
Alert repetition interval	10 minutes	Each alert broadcast was assumed to be repeated every 10 minutes until the expiration time.
Average phone call duration	2.7 minutes	The average duration for cell phone calls was calculated from a publicly available dataset.
Number of cell towers	9	Alert broadcast was simulated over a small hypothetical region with 9 cell towers.
Number of handsets	45	Alert broadcast was simulated assuming 5 handsets connected to each cell tower.

5.2 CELL BROADCAST NETWORK TRAFFIC

This scenario investigated WEA performance as a function of background (non-alert) cell broadcast network traffic load. Normal levels of Internet delay and IPAWS-OPEN traffic load were assumed, without any simulated infrastructure damage. It was also assumed that WEA alerts are transmitted at the same priority level as background cell broadcast traffic. Prioritization of WEA

[7] "FEMA IPAWS-OPEN Active-Active Release 3.02 Quality Assurance Independent Validation and Verification Performance Test and Evaluation Report," Version 1.0, 29 August 2012.
[8] http://ipnetwork.bgtmo.ip.att.net/pws/network_delay.html
[9] http://www.internetpulse.net/
[10] http://www.internettrafficreport.com/namerica.htm
[11] http://www.cs.helsinki.fi/group/context/data/

alerts is at the discretion of CMSPs, and if some CMSPs elect to treat WEA alerts at a higher priority level than other cell broadcast traffic, then WEA alerts will be relatively unaffected by other cell broadcast traffic. In this case, WEA alerts will experience smaller delays than indicated by the simulation results during high background cell broadcast load.

In this scenario, background cell broadcast traffic was increased from 1% load to 99% load in five increments. The arrival of incoming background cell broadcast requests was assumed to be random with a Poisson distribution. Each background cell broadcast was repeated three times at 1-minute intervals. Three different alerts were transmitted for each load level. The simulation was repeated six times with different seed values for the random number generator.

Figure 5-1 shows the end-to-end delay that different WEA messages experienced in multiple runs of this scenario. Each data point in the figure corresponds to a successful reception of an alert by a different handset during the first transmission of that alert. Several handsets did not receive the alerts during the first transmission due to ongoing phone calls, and had to wait for a subsequent transmission, which introduced much larger delay values than shown in the figure. Such delays due to ongoing phone calls are excluded from the figure and investigated separately in Section 5.6. The figure shows the effect of increasing cell broadcast traffic. Congestion of the cell broadcast channel delays some alerts by as much as 20 to 70 seconds during high and extreme loads of background cell broadcast. Although this delay can be acceptable for some types of public alerts, it can be excessive for others such as earthquake warnings. Assigning a higher-priority level to such alerts (or all WEA alerts) compared to background cell broadcast traffic would reduce this type of delay.

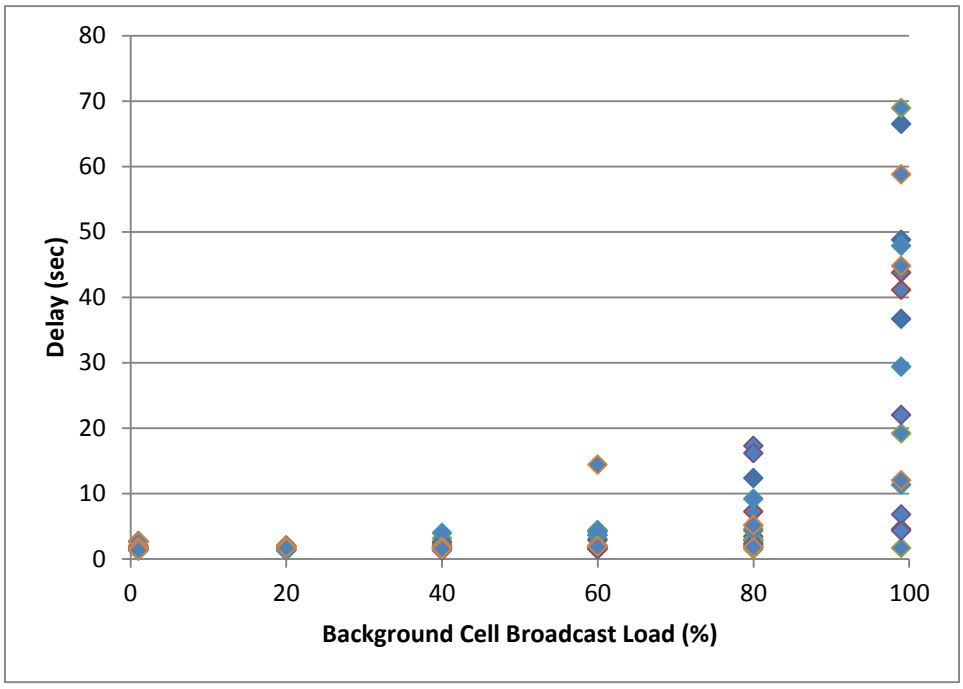

Figure 5-1 End-to-End Delay as a Function of Background Cell Broadcast Traffic

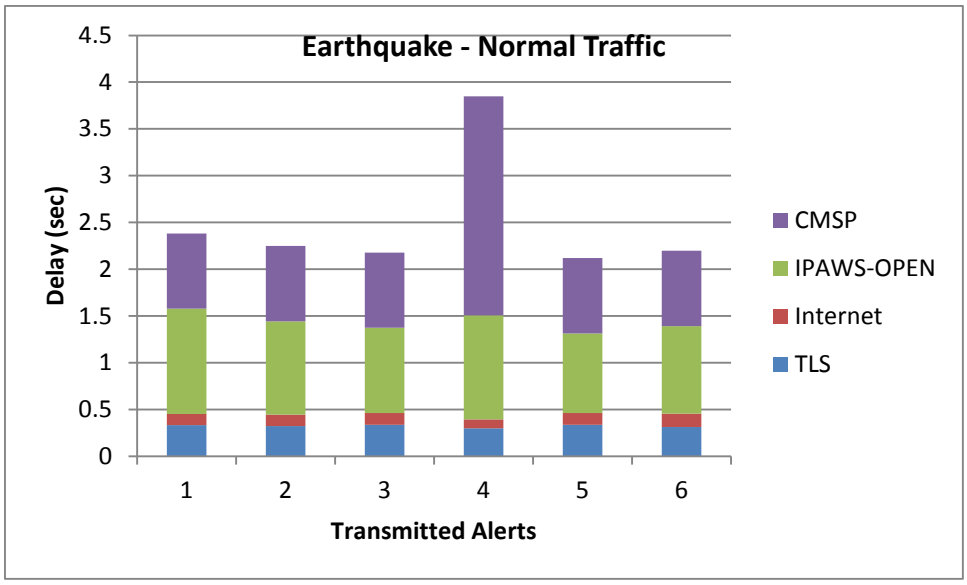

Figure 5-2 End-to-End Delay in Major Earthquake Scenario with Normal Network Traffic

Figure 5-3 and Figure 5-4 show the simulation results with high levels of traffic in the major earthquake and chemical attack scenarios, respectively. In this case, the end-to-end delay was around 6 seconds for most alerts, which may be acceptable for many types of disasters. Comparing this to the results with normal conditions, the increase in delay was mainly caused by increased TLS and Internet delays. The TLS protocol requires the exchange of multiple packets to set up a connection before the actual alert packet is sent, and therefore takes multiple roundtrip times to complete. Increasing the Internet delay directly increases the TLS delay. The TLS protocol also requires some processor time to validate and authenticate received security credentials, so increased IPAWS-OPEN load increases processing delays as TLS packets may have to wait longer until processor time becomes available.

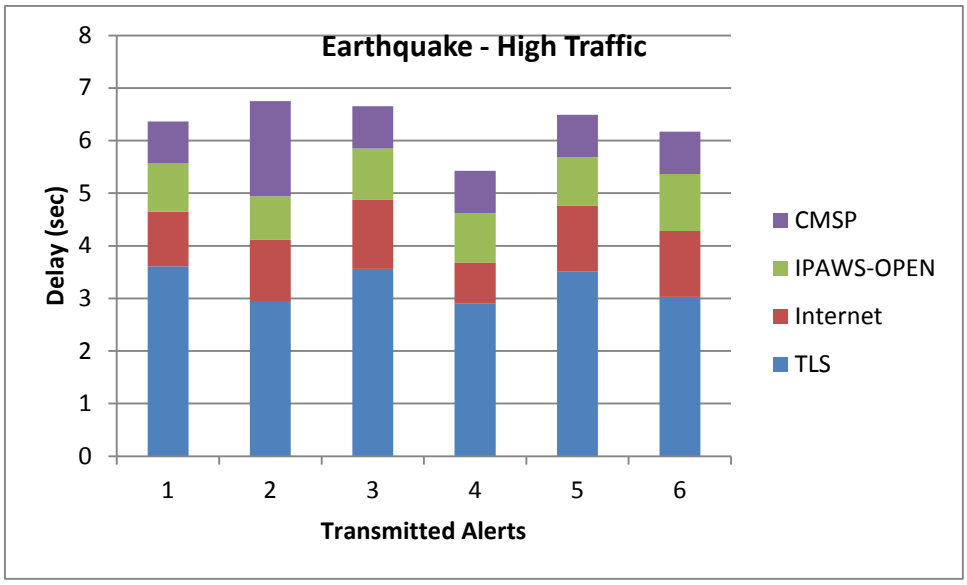

Figure 5-3 End-to-End Delay in Major Earthquake Scenario with High Network Traffic

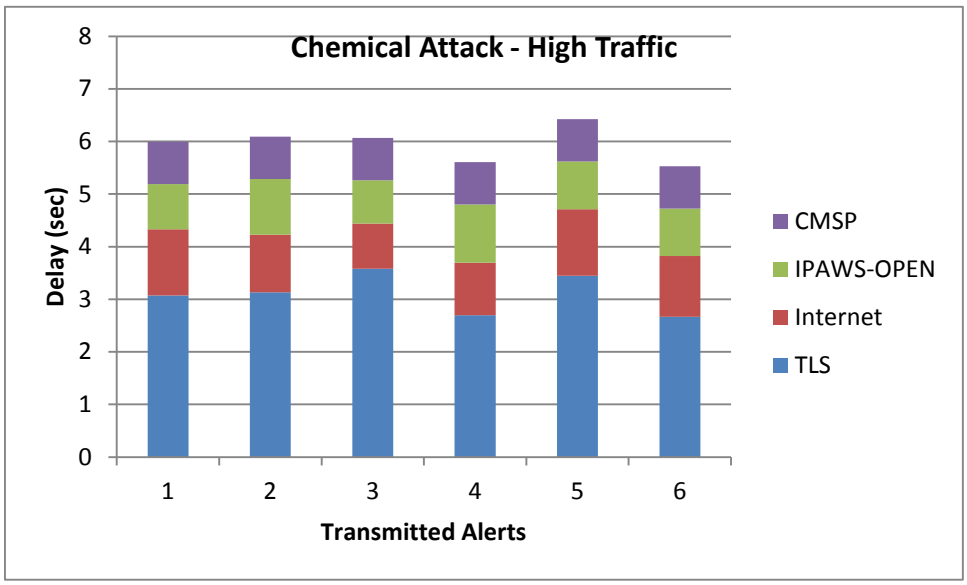

Figure 5-4 End-to-End Delay in Chemical Attack Scenario with High Network Traffic

Figure 5-5 and Figure 5-6 show the simulation results with extreme levels of traffic in scenarios for a major earthquake and a chemical attack, respectively. Most alerts experienced delays between 10 seconds and 20 seconds; however, some of them had larger delays, as high as 57 seconds. Under extreme network traffic conditions, the largest contributor to the overall delay is the TLS delay. Large Internet delays combined with long processor wait times increased TLS delays considerably.

call when a WEA alert is transmitted can receive the alert only during a subsequent repetition, provided it is not engaged in a phone call during that repetition (and provided that other factors such as coverage and interference allow the handset to receive the alert).

The WEA repetition process consists of broadcasting the same WEA message multiple times based on two configurable parameters: the total number of broadcasts and the repetition period. These parameters impact the system performance in terms of the percentage of wireless subscribers that receive the alert and the associated latency.

The impact of active phone calls on WEA alert reception latency and alerted population percentage was investigated during this analysis. It was assumed that each WEA transmission is repeated every 10 minutes. The average call duration was set to 2.7 minutes based on statistical data,[12] and the average time between successive calls (inter-arrival time) was varied between 54 minutes and 3.4 minutes. This resulted in call loading levels between 5% and 80% for each handset. Exponential distribution was assumed for the call inter-arrival times and the call durations.

Figure 5-9 shows the percentage of handsets that received the alerts as a function of time. Different colors correspond to different phone call loads. The horizontal axis is the time elapsed since the origination of the alert messages. At 5% (or less) call load, 95% of the handsets received the alert during the first transmission, and almost all of the remaining 5% received the alert during the second transmission, resulting in a relatively fast alert delivery. In contrast, at 50% call load, only about 48% of the handsets received the alert during the first transmission. In this case, 5% of the handsets still did not receive the alert after five transmissions (i.e., after the 40-minute mark in the figure). The delays become even larger as the call load increases further.

These results illustrate the importance of the repetition period for WEA because it may take a number of repetitions before some handsets receive the alert. Setting the repetition period too large will introduce substantial delays in alerts, whereas setting it too small will consume many cell broadcast resources and may be ineffective beyond some point. An analysis of the optimal repetition period for a given load level is deferred to a future study.

Although transmission errors were not considered in this analysis, it should be noted that in practice some handsets will not receive some alerts due to interference or poor reception. This will increase the required number of repetitions even further.

[12] http://www.cs.helsinki.fi/group/context/data/

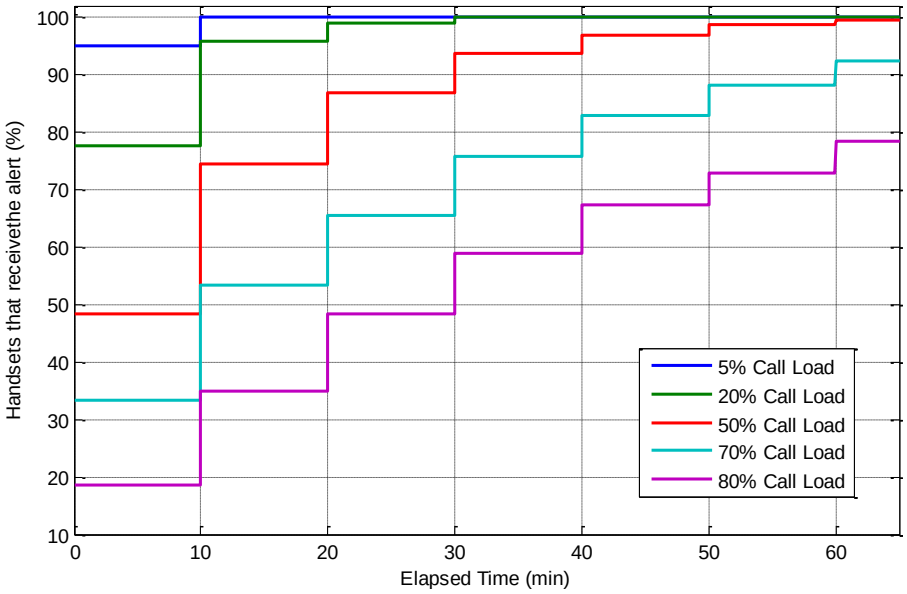

Figure 5-9 WEA Alert Reception at Different Levels of Phone Call Load

Section 6

DISCUSSION OF RESULTS

This document described the WEA computer model and presented simulation results investigating the impact of various factors on WEA performance. More specifically, the study included the impact of background cell broadcast traffic, large Internet delays, high IPAWS-OPEN traffic load, DoS attacks, transmission errors, and active phone call volume. Alert delivery latency was used as the main performance metric. The computer model was developed under the constraints mentioned in Section 3.2, so real world results would be expected to be somewhat different and would vary by CMSP infrastructure.

The results showed that high levels of background cell broadcast traffic (more than 80% loading) can cause excessive delays (larger than 20 seconds) for certain types of alerts. Therefore, CMSPs that plan to offer commercial cell broadcast services to their customers should assign a higher priority level to WEA messages to reduce these delays.

Extremely high Internet delays (e.g., 1 second) combined with high IPAWS-OPEN traffic load also caused excessive delays for certain types of alerts, mainly due to the protocol overhead associated with HTTPS setup. This delay can be reduced by using dedicated secure channels between IPAWS-OPEN and a subset of AOS's that are expected to generate highly delay-sensitive alerts (such as earthquake and tornado warnings). An IPSec option can be considered for such AOS's. With this option, a secure channel between an AOS and IPAWS-OPEN would be opened in advance, and it would remain open. Therefore, there would be no need for a secure channel setup at the time of alert transmission, thus reducing delay. Alternately, the Internet delays during extreme conditions can be reduced by using Internet Service Providers (ISPs) that offer Service-Level Agreements (SLAs) with guaranteed minimum bandwidth and maximum delay. Services with such SLAs are typically more expensive but can maintain a baseline service quality even though the ISP network is congested with high network traffic.

The DoS attack scenario emphasized the need for adequate defenses against this type of attack. Because WEA is a centralized architecture, disabling the IPAWS-OPEN data centers with a cyber attack would make the entire system non-operational. Potential benefits of a distributed architecture should be considered for future enhancements to WEA.

Finally, simulation analysis investigating transmission errors showed that three or more transmissions may be needed to alert at least 90% of a target population, if 10% of the handsets cannot receive an alert due to transmission errors. Similarly, the simulation analysis investigating active phone calls showed that if there is a heavy phone call volume (exceeding 50% load), four or more transmissions would be needed to alert at least 90% of the target population. These results demonstrate that the WEA broadcast repetition interval must be optimized by CMSPs to minimize alert delivery latency without consuming excessive cell broadcast resources or over-alerting the public. The study of cell broadcast patterns with optimal repetitions is deferred to future work.

The results presented in this document could affect a number of important technical, programmatic, and policy decisions that must be made or endorsed by the FCC, FEMA, DHS, CMSPs, the Alert Originator community, and state and local first responders. The evolution of the WEA system must be coordinated in light of the consequences—for the public, for first responders, for federal disaster response—of the degradation of service predicted by the WEA simulation results. Alert Originators need to be aware of the worst-case consequences of alert initiation under adverse circumstances.

Appendix A

CELLULAR NETWORK MODELS

This appendix describes further details of CBS implementation in the GSM and LTE network models. These models were introduced in Sections 4.7 and 4.8, respectively.

A.1 GSM NETWORK MODEL

The GSM network model represents the GSM physical and upper protocol layers (e.g., data link and transport), the application threads (e.g., call setup and delivery), and GSM cell broadcasting. These features were modeled as described in the GSM standards and support the following GSM functions:

a. Cell selection and reselection

b. Registration

c. MS operation in Idle or Dedicated mode

d. Call setup and delivery

e. Handover

f. Cell broadcasting

Cell broadcast messages are generated by the CBC and sent to the appropriate BSCs. Each BSC routes the messages to the target BTSs, and the BTSs broadcast the messages to all MSs (i.e., handsets) within the respective BTS cell range.

In GSM, CBS messages are broadcast on the CBCH in unacknowledged mode. CBCH is supported either by the beacon channel or by the Standalone Dedicated Control Channel (SDCCH). The difference between beacon channel usage and SDCCH usage is in their timeslot assignments to CBCH. Because using the beacon channel or SDCCH for cell broadcast delivery would give similar performance under the vast majority of traffic conditions, for simplicity only beacon channel delivery was modeled in the WEA GSM network model.

A CBS message can be either a Short Message Service Cell Broadcast (SMSCB) message or a schedule message. SMSCB messages carry the actual cell broadcast, whereas the schedule messages contain scheduling information for SMSCB messages that will be sent afterward. The SMSCB message size is equal to one page of data, which is 92 bytes. Messages are broadcast with a repetition period that is a multiple of 1.883 seconds. Each message has one of three priority levels: high, normal, or background. High is the highest priority level, and background is the lowest priority

level. Each message has an absolute expiration time. If the message is received by an MS after the absolute expiration time, the message is considered out of date and is dropped.

A.2 LTE NETWORK MODEL

The LTE network model with CBS support was developed based on three types of nodes from OPNET Modeler's built-in LTE library: UE, eNodeB, and EPC. Adding CBS support did not require any changes to the EPC model.

The eNodeB model was modified to enable discovery by the CBC so that TCP connections can be established directly between the eNodeBs and the CBC in each LTE subnet. The internal structure of the new eNodeB model is shown in Figure A-1. Each plain box represents a different process running inside an eNodeB node. The arrows represent various information flows between different processes. A new *application* process was added to the eNodeB model as identified by the circle in the figure. This *application* process receives cell broadcast messages from the CBC using the direct TCP connections, and it performs three main functions:

a. Delivery of the received cell-broadcast message to the *lte_s1* process

b. Signal retransmissions to the *lte_s1* process

c. Signal end of retransmission when an alert is cancelled or expired

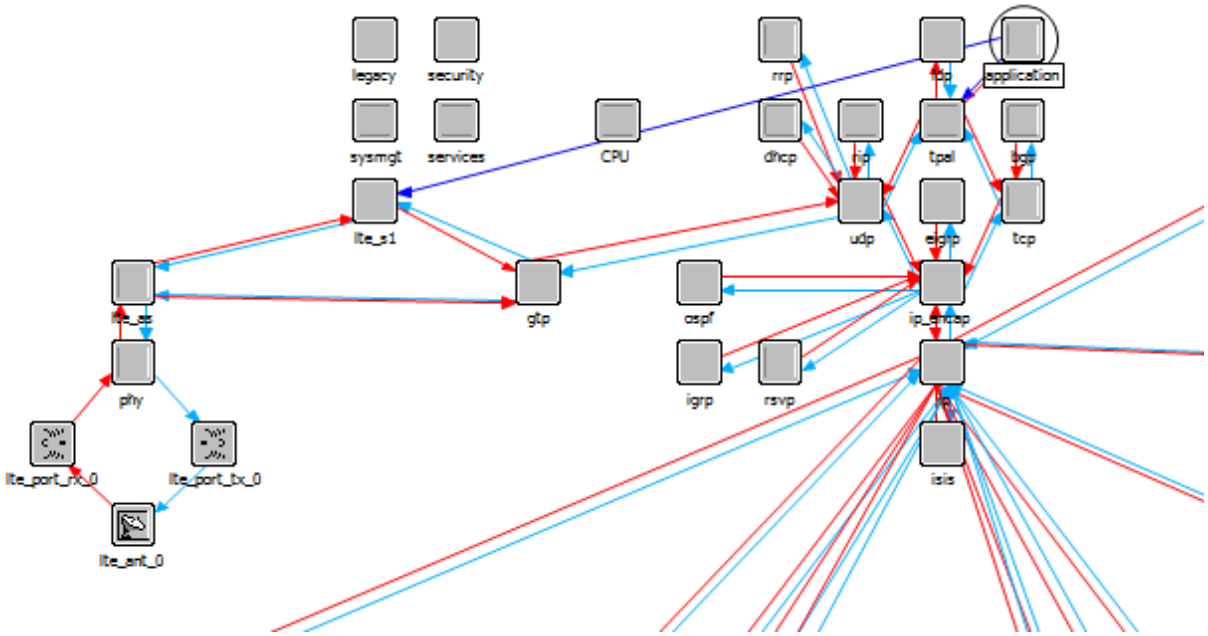

Figure A-1 Portion of Modified eNodeB Node Model for LTE

The *lte_s1* process was modified to treat the cell broadcasts as pass-through messages to be sent to the broadcast International Mobile Subscriber Identity address. This is then incorporated into the combined downlink channel schedule and sent through the physical layer process model.

The UE model for LTE was modified to detect received cell broadcast messages and to process them separately from other applications, as depicted in Figure A-2. All cell broadcast messages are handled by the *lte_CMAS_rcvd* process highlighted by the circle.

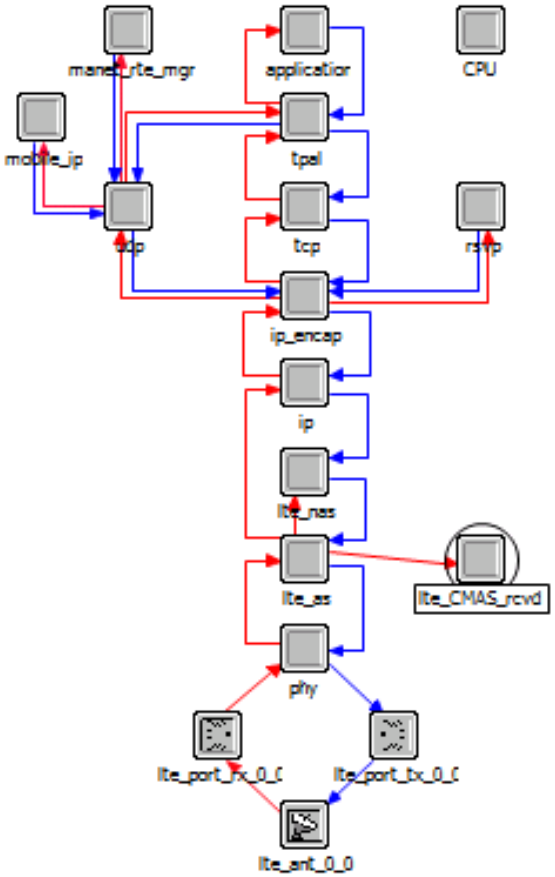

Figure A-2 Modified UE Node Model for LTE

Appendix B

LIST OF ACRONYMS AND ABBREVIATIONS

AO	Alert Originator
AOS	Alert Origination System
BSC	Base Station Controller
BTS	Base Transceiver Station
CAP	Common Alerting Protocol
CBC	Cell Broadcast Center
CBCH	Cell Broadcast Channel
CBE	Cell Broadcast Entity
CBEM	Cell Broadcast Entity Message
CBS	Cell Broadcast Service
CMAM	Commercial Mobile Alert Message
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CMSP	Commercial Mobile Service Provider
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Denial of Service
eNodeB	Evolved Node B
EOC	Emergency Operation Center
EPC	Evolved Packet Core
FCC	Federal Communications Commission

FEMA	Federal Emergency Management Agency
FER	Frame Error Rate
GSM	Global System for Mobile Communications
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
LTE	Long-Term Evolution
M&S	Modeling and Simulation
MS	Mobile Station
OPEN	Open Platform for Emergency Networks
RF	Radio Frequency
SDCCH	Standalone Dedicated Control Channel
SMSCB	Short Message Service Cell Broadcast
S&T	Science and Technology Directorate
SLA	Service-Level Agreement
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
WEA	Wireless Emergency Alerts