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.

Section 1

BACKGROUND

The Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Science and Technology Directorate (S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into tools to help protect the homeland.

The Wireless Emergency Alerts (WEA) Program was established by the Federal Communications Commission (FCC) in response to the Warning, Alert, and Response Act of 2006 to allow wireless service providers to send geographically targeted emergency alerts to their subscribers. Under Executive Order 13407, the Secretary of the DHS, in coordination with the Department of Commerce and the FCC, is responsible for implementing and administering the national public emergency alert system and ensuring that the President can alert and warn the American people in the case of an emergency. Within DHS, the Federal Emergency Management Agency (FEMA) is responsible for the implementation and administration of the Integrated Public Alert and Warnings System (IPAWS). FEMA has established the IPAWS program office to, in critical part, develop and manage technologies and processes capable of accepting and aggregating alerts from the President, the National Weather Service, and state and local emergency operations centers (EOCs), as well as delivering validated, geographically targeted emergency alerts and warnings through WEA.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) has been engaged by the DHS S&T First Responders Group to develop a computer model to simulate WEA and investigate system performance under specific scenarios. The results highlight potential improvements that should be considered by DHS and FEMA in future iterations of WEA.

Section 2

WEA REFERENCE ARCHITECTURE OVERVIEW

In December 2006, the FCC established the Commercial Mobile Service Alert Advisory Committee (CMSAAC) to recommend system-critical protocols and capabilities for WEA. The CMSAAC consisted of representatives from state and local governments, Federally recognized Native American tribes, representatives of the communications industry (including wireless service providers and broadcasters, vendors, and manufacturers), and national organizations representing people with special needs.[1] In its recommendations, CMSAAC proposed the architecture for the WEA as shown in Figure 2-1.[2] The Alert Aggregator and Alert Gateway functionality shown in the figure is currently implemented as part of FEMA's IPAWS Open Platform for Emergency Networks (OPEN).

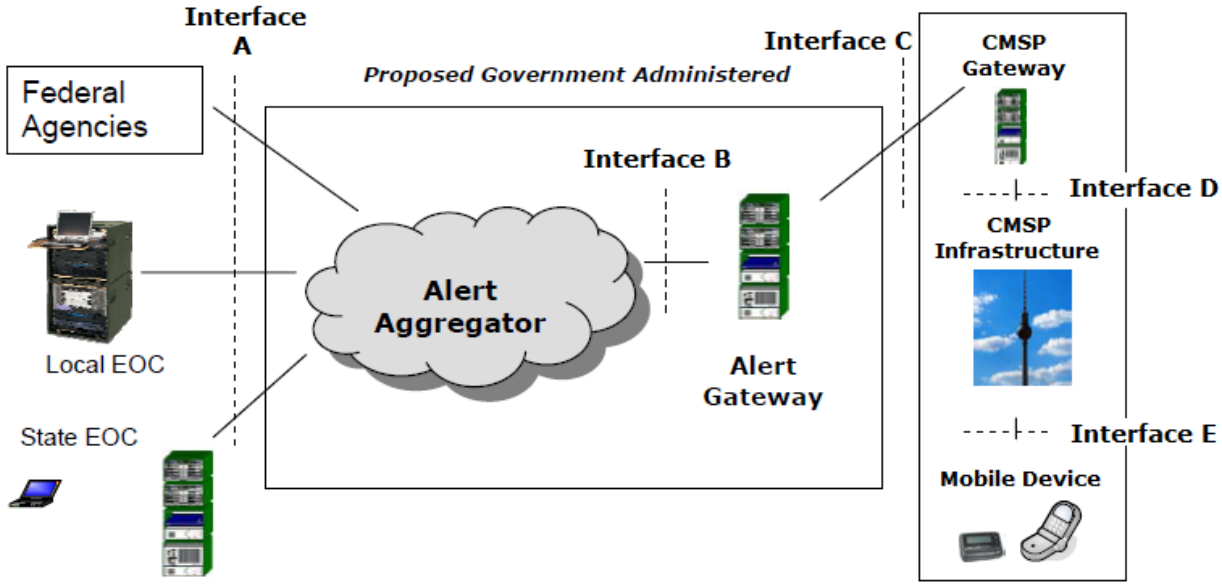

Figure 2-1 WEA Reference Architecture

At a high level, the following actions take place under this reference model:

[1] The full list of CMSAAC members is found in "Notice of Appointment of Members to the Commercial Mobile Service Alert Advisory Committee; Agenda for 12 December 2006 Meeting", Public Notice, 21FCC Rcd 14175 (PSHSB 2006).

[2] "Commercial Mobile Alert Service Architecture and Requirements," 12 October 2007.

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.

Section 3

WEA MODELING AND SIMULATION

A public alert and warning system such as WEA must be able to operate continuously even under 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. This model can simulate the transmission of alert messages from AOS's through delivery to a customer's mobile device and estimate system performance when a variety of conditions are assumed. This includes scenarios with extreme conditions.

There are several factors that can delay or prevent sending alerts to a portion of the target population.[3] These factors include the availability of communication paths between WEA components, transmission delays across various interfaces, and message processing and queuing delays at WEA components. Availability of the WEA service at a given location is also an important factor; a handset cannot receive an alert if it is outside of the provider coverage area or WEA service area, if some infrastructure damage or system failure prevents WEA service at that location, or if the handset is simply inside a poor reception area. Radio frequency (RF) interference can cause transmission errors in over-the-air broadcast and prevent reception of the alerts. Finally, handset status (e.g., on/off, active call) will also affect whether a WEA broadcast can be received by a handset. The WEA computer model was designed with capabilities to simulate the effects of these factors and is explained in detail in Section 4.

3.1 MODELING AND SIMULATION SOFTWARE

The project team evaluated several commercial modeling and simulation (M&S) tools suitable for WEA model development. Based on evaluation criteria such as available features, ease of development, ease of use, customer support, and cost, OPNET Modeler was selected to design and develop the WEA computer model. It includes built-in models for networking devices such as routers and switches, network protocols, wired and wireless communication links, servers, and network clouds. It also allows for the development of custom models and customization of the built-in OPNET models. Built-in models and customization features of OPNET Modeler were used to simulate alert origination, aggregation, Federal and CMSP Gateways, CMSP CBS infrastructure, handsets, and their connectivity.

OPNET Modeler is a discrete event simulator that simulates the transmission of every network packet from its source to its destination. This allows for highly accurate simulations of real systems, but requires a lot of processing cycles and memory utilization for large and complex networked systems. The tool supports different levels of abstraction at the expense of simulation accuracy as a workaround for modeling such complex systems.

[3] In this document the term "target population" refers to the intended recipients of a public alert or warning.

3.2 MODELING CONSTRAINTS

A number of constraints shaped the development of M&S capabilities for WEA. First, the very large number of cell towers and cellular devices that can potentially receive an alert makes it impractical to run simulations at full accuracy. Certain simplifications were used to develop feasible simulations, such as more abstract models of cellular transmission and scaling down the number of cell towers and cellular devices.

Limited information was available about the internal architecture and performance attributes of the AOS's, IPAWS-OPEN, and CMSP network components. For example, IPAWS-OPEN uses Akamai services over Interface A for load balancing and failover switching between two data centers. However, detailed information about these services is sensitive and subsequently restricted.

Validation of the WEA computer model requires WEA performance data, such as processing and transmission delays, network capacity, and cell broadcast reception statistics, obtained by system testing or field measurements. However, the only performance data available to JHU/APL at the time of this study were the results of an IPAWS-OPEN performance test.[4] The test consisted of posting 1000 alert messages to IPAWS-OPEN and retrieving messages from the system while the alerts were being posted. This operation took 17 minutes to complete. These data were used to configure the alert processing capacity of the IPAWS Aggregator model. Other components of the computer model were configured using other sources of information, including relevant system performance requirements.

Generic models of Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) technologies were available in OPNET Modeler and some other commercial software tools, but research uncovered no available commercial or open-source models for CBS delivery over Global System for Mobile Communications (GSM), UMTS, or LTE. Furthermore, existing equipment models generally supported simulating equipment failure, but very few models supported realistic recovery behavior.

Lastly, timelines are required for simulation scenarios, but there is no body of agreed-upon emergency alerting timelines for incidents where WEA might be involved.

3.3 MODELING APPROACH

Given the absence of detailed information about IPAWS-OPEN elements and internal CMSP equipment, the decision was made to use the standard OPNET Modeler network, server, and protocol models. WEA- and CBS-specific extensions were added to these standard models, and they were used to represent alert origination, aggregation, Federal and CMSP Gateways, Cell Broadcast Entity (CBE), and Cell Broadcast Controller (CBC) functions, and their connectivity including the Akamai services. These models have been used successfully by many network analysts to represent general processing and network routing in situations where specific data are lacking. They are configurable by setting equipment attributes so that they can reflect specific knowledge of these elements, should these data become available in the future. Without specific design data, the WEA components were modeled using a "black-box" approach which does not include detailed modeling of

[4] "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.

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

Section 4

COMPUTER MODEL ARCHITECTURE

The WEA computer model uses the same architecture as the WEA network architecture. Figure 4-1 shows representative models for AOS's (labeled as Emergency Operations Center (EOC)), Aggregator and Federal Alert Gateway functionality at two data centers, connections to multiple CMSP networks, and the Internet.

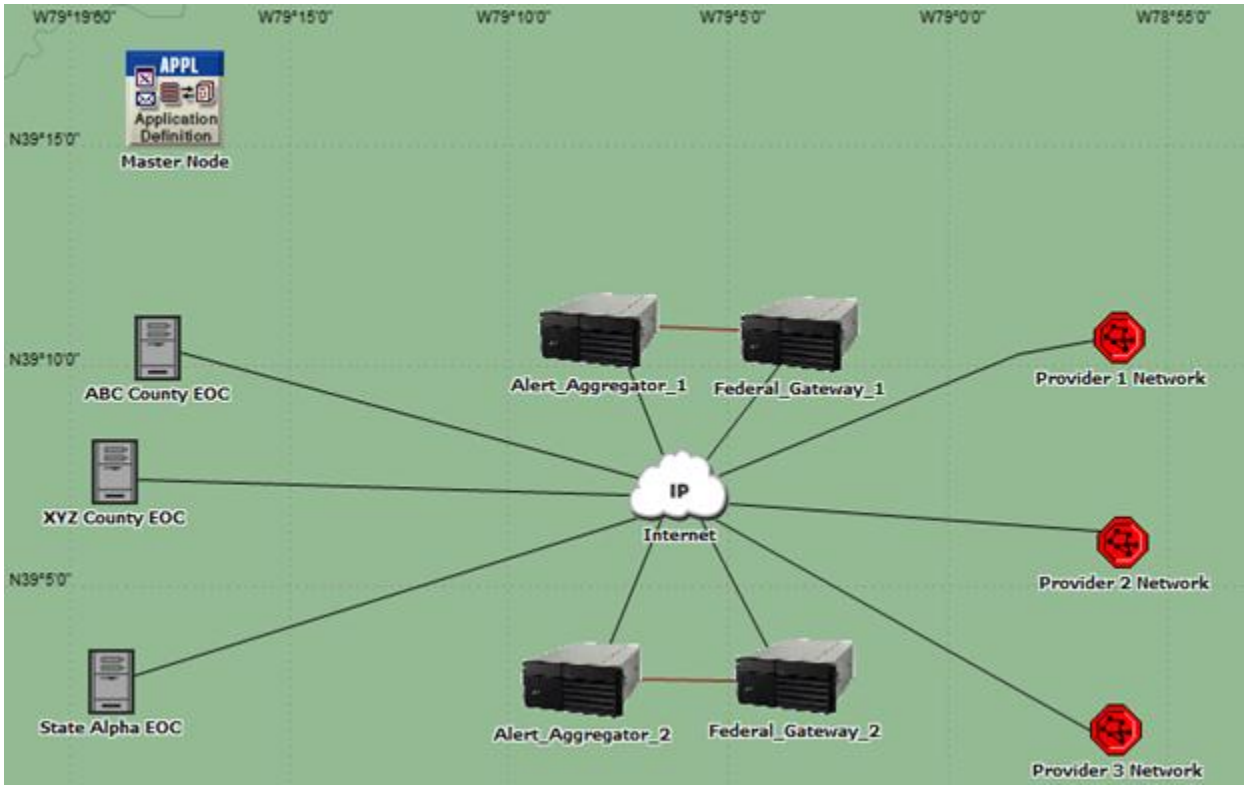

Figure 4-1 WEA Computer Model Architecture

Although only three EOCs and three provider networks are shown in the figure for simplicity, the model supports much larger numbers of instances for each. The Master Node is responsible for the scenario configuration. It reads a text file that describes all events in a scenario—such as alert generation and equipment failure—and orchestrates these events using the appropriate OPNET Modeler methods. Each of the three Provider Network nodes in Figure 4-1 is actually a full CMSP infrastructure, hidden from view for simplicity. Each of these nodes can be a GSM network model or

an LTE network model, based on the scenario being analyzed. These representative elements are explained in subsequent sections of this document.

4.1 SIMULATING NETWORK CONNECTIONS

Three kinds of connections were modeled for the WEA simulation studies: simple wired connections, IP cloud connections, and cell phone RF connections.

4.1.1 WIRED CONNECTIONS

Simple wired connections are used between the Aggregators and Federal Alert Gateways and for connections within the CMSP domain between the CMSP core network and cell towers. They are assigned a capacity and a level of background (non-WEA) traffic. These connections can model point-to-point communication between two nodes with various transmission effects, such as delay and packet loss. They can also model logical interfaces between two functional entities without any transmission delay or loss.

4.1.2 IP CLOUD CONNECTIONS

The Internet connectivity between AOS's, IPAWS data centers, and the CMSP networks was modeled using a single IP cloud. This model supports associating capacity, delay, and packet loss characteristics with multiple interfaces. These characteristics can be adjusted to meet specific scenario conditions. The model also supports simulating network congestion caused by high background traffic, and has the ability to disable interfaces into the cloud for a period of time. The connectivity between AOS's and IPAWS data centers through the cloud model (Interface A) uses Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS). The connectivity between IPAWS data centers and CMSP networks through the cloud model (Interface C) uses Internet Protocol Security (IPSec). The IP backbone inside the CMSP networks was also modeled by a single IP cloud model, but with attributes different from the Internet cloud model.

4.1.3 HANDSET RF CONNECTIONS

The over-the-air connection between the CMSP network (i.e., cell towers) and the handsets is a critical element of the WEA simulation capability. OPNET Modeler uses a series of code modules called *pipeline stages* to model the transmission and reception of RF signals. Some are associated with the radio transmitter in an OPNET model and some are associated with the radio receiver. Each pipeline stage receives certain inputs from the simulation framework and from the previous pipeline stage, and must set values for the next pipeline stage. There are default radio pipeline stages as well as those customized for specialized models such as LTE or UMTS. These standard stages support a selection of radio propagation models. The default propagation model represents the unimpeded spreading of radio waves in vacuum (free space spreading).

Wireless simulation in OPNET Modeler with existing pipeline stages consumes a considerable amount of computational resources because (1) a copy of a transmitted packet is made for many more receivers than those that might receive and decode the packet and (2) propagation models that require terrain or building information can be computationally intensive. This computational burden is worthwhile only if accurate information about the physical environment is available. An appropriate propagation model must have accurate inputs, especially with regard to the transmitters and receivers. For CMSP modeling, this would mean accurate tower information, including location, antenna height, transmit power, antenna pattern(s), and bandwidth(s).

Full-fidelity[5] wireless simulation in OPNET can be accomplished with reasonable computational resources if the number of packets generated is limited and the propagation modeling is relatively simple. The GSM model that was developed has a simplified packet flow, which enables simulations many times faster than real time. On the other hand, the built-in LTE model is very complex, representing many aspects of the LTE system in detail. The LTE model runs several times slower than real time when used with full detail, limiting the simulations to a small number of nodes and only a few hours of simulated time.

4.2 SIMULATING ALERT ORIGINATION

AOS models were developed based on OPNET Modeler's built-in workstation model. They create alert packets when prompted by the Master Node and transmit the alerts to an Aggregator. AOS models mimic the TLS protocol that establishes an HTTPS connection with the Aggregator before sending the alert packet, and they send the alert packet only after the HTTPS setup is successfully completed. If network congestion or other factors prevent the establishment of an HTTPS connection, the alert packet is not sent. Alert transmission uses the built-in Transmission Control Protocol (TCP) model as the transport protocol. AOS models accept messages from the Aggregator acknowledging that an alert was received and keep track of which alerts have and have not been acknowledged.

AOS models have the following attributes:

a. Aggregator Name – The name of the Aggregator to which the AOS model will send alerts.

b. HTTPS Handshake Packet Processing Delay – The delay inserted between receiving a handshake packet and sending the response. This mimics time spent processing the packet within the AOS.

c. HTTPS Handshake Failure Time Limit – If this amount of time elapses without the handshake completing, the handshake is declared failed.

d. HTTPS Connection Retry Delay – A delay inserted between the failure of an HTTPS handshake and the attempt to reestablish it.

e. Unacknowledged Alert Time Limit – If a transmitted alert remains unacknowledged by the Aggregator for more than this amount of time, the alert is retransmitted.

4.3 SIMULATING ALERT AGGREGATION

The Aggregator models were developed using OPNET Modeler's built-in server model. They respond to TLS attempts from any AOS model and accept alerts following a successful HTTPS setup. The processing delays incurred for authenticating and setting up an HTTPS connection are represented in the model. For each alert packet received via a valid HTTPS connection, the Aggregator model sends an acknowledgment message back to the AOS model, delays the packet to account for message processing, and then passes it to the Federal Alert Gateway model. The Aggregator and the Federal Alert Gateway are assumed to be separate functional entities

[5] In this context the term "full-fidelity" refers to detailed modeling and simulation of RF propagation, including various properties of the physical environment.

implemented in the same physical device (server); therefore, no transmission delay or packet loss was modeled for the connectivity between them.[6]

Aggregator models have the following attributes:

a. HTTPS Handshake Packet Processing Delay – The delay inserted between receiving a TLS packet and sending the response. This mimics the time spent processing the packet within the Aggregator.

b. Authentication Delay – A delay included when setting up a new HTTPS connection, to mimic the time spent authenticating the AO.

c. Alert Processing Delay – A delay inserted between receiving an alert and forwarding the alert to the Federal Alert Gateway.

d. Queue Size – The total size of the buffer space that can store messages waiting to be processed.

4.4 SIMULATING THE FEDERAL ALERT GATEWAY

The Federal Alert Gateway models were developed using OPNET Modeler's built-in server model. Each Federal Alert Gateway model accepts and queues alerts from an Aggregator model. It mimics the setup of a persistent IPSec connection to each CMSP Gateway model, generates multiple Interface C alert messages for each received alert, and forwards them to the CMSP Gateways. The Federal Alert Gateway model also sends Link Test messages to CMSP Gateways and directs alerts to a CMSP's secondary Gateway if the primary does not respond.

All messages between the Federal Alert Gateway models and the CMSP Gateway models are sent using the built-in TCP model as the transport protocol.

Federal Alert Gateway models have the following attributes:

a. Message Response Time – If a transmitted message remains unacknowledged by the CMSP Gateway for more than this amount of time, the message is retransmitted.

b. Retransmit Number – The number of times that the Federal Alert Gateway will attempt to transmit a message to the CMSP Gateway when an acknowledgment is not received.

c. Link Test Period – The time interval between successive Link Test messages from the Federal Alert Gateway to CMSP Gateways.

4.5 SIMULATING THE COMBINED CMSP GATEWAY AND CBE

Whereas the RF delivery, mobility management, and radio network control vary significantly with the CMSP technology (i.e., GSM, LTE), the combined CMSP Gateway and CBE model and the CBC model are common to all technologies. The combined CMSP Gateway and CBE model is based

[6] The wired connection model used for the Aggregator to Federal Alert Gateway connection supports non-zero delay and packet loss, but these parameters were set to zero.

on a generic Gateway model supplied by OPNET Modeler that has multiple Layer 1 and Layer 2 interfaces. This model was modified to support WEA messages in the following manner: An application module was added to process WEA messages from the Federal Alert Gateway models and background cell broadcast messages from background CBS generators. The combined CMSP Gateway and CBE model receives WEA messages from the Federal Alert Gateway models, translates alert information into an approximated Cell Broadcast Entity Message (CBEM) format, and sends the CBEM messages to the CBC model.

The combined CMSP Gateway and CBE models have the following attribute:

a. Repetition Period – Sets the repetition period for alert broadcast. The total number of repetitions for each alert is determined by this period and the alert expiration time.

4.6 SIMULATING THE CBC

The CBC is an OPNET Modeler built-in Ethernet server model, modified to support CBS. It is the second model that is common to all CMSP technologies. The CBC model discovers all of the towers for which it is responsible. This includes the BTSs in GSM subnets and eNodeBs in LTE subnets. It also discovers the intermediate nodes (e.g., the BSCs for GSM) that transmit mobility and radio control information to the towers and relay cell broadcast messages. The CBC model enables discovery of its existence in the CMSP network so that the CBEs can find it. It receives cell broadcast packets from the CBE models and determines which towers and intermediate nodes should receive those cell broadcast packets. This is done by referring to a data structure read from a file outside the model, which describes a latitude and longitude region for each geocode in a CBEM message. If a tower is in that region, the tower is added to a list of towers sent along with the alert message to the intermediate nodes. For wireless technology models with no intermediate nodes, these messages are sent to the towers individually. Any non-WEA cell broadcast packets are sent into the CMSP network for transmission from all towers.

4.7 SIMULATING A GSM SUBNETWORK

The GSM-specific models for WEA were designed based on some existing GSM models that were formerly developed for a DoD project. They were used, with permission, for the WEA computer model, after being modified to add CBS support. However, the following aspects of a typical GSM network were not modeled because they do not have significant impact on the cell broadcast performance and would add unnecessary complexity to the WEA model:

a. Time-Division Multiple Access channels (The MS radio channels were modeled only as Frequency-Division Multiple Access channels.)

b. Power control

c. Message processing capacity (All GSM network components were assumed to have unlimited message processing rates.)

The model of a GSM subnet is shown in Figure 4-2. It includes node models for the three types of GSM-specific nodes used by WEA cell broadcast: BSC, BTS, and MS. In GSM terminology, BTSs are cell towers and MSs are the handsets. The figure also shows the combined CMSP Gateway and CBE and the CBC nodes that are used to carry WEA messages, as well as some telephony network

nodes that are not used by WEA but will typically be connected to the BSCs in a GSM subnet. Further details of the GSM network model are described in Appendix A.

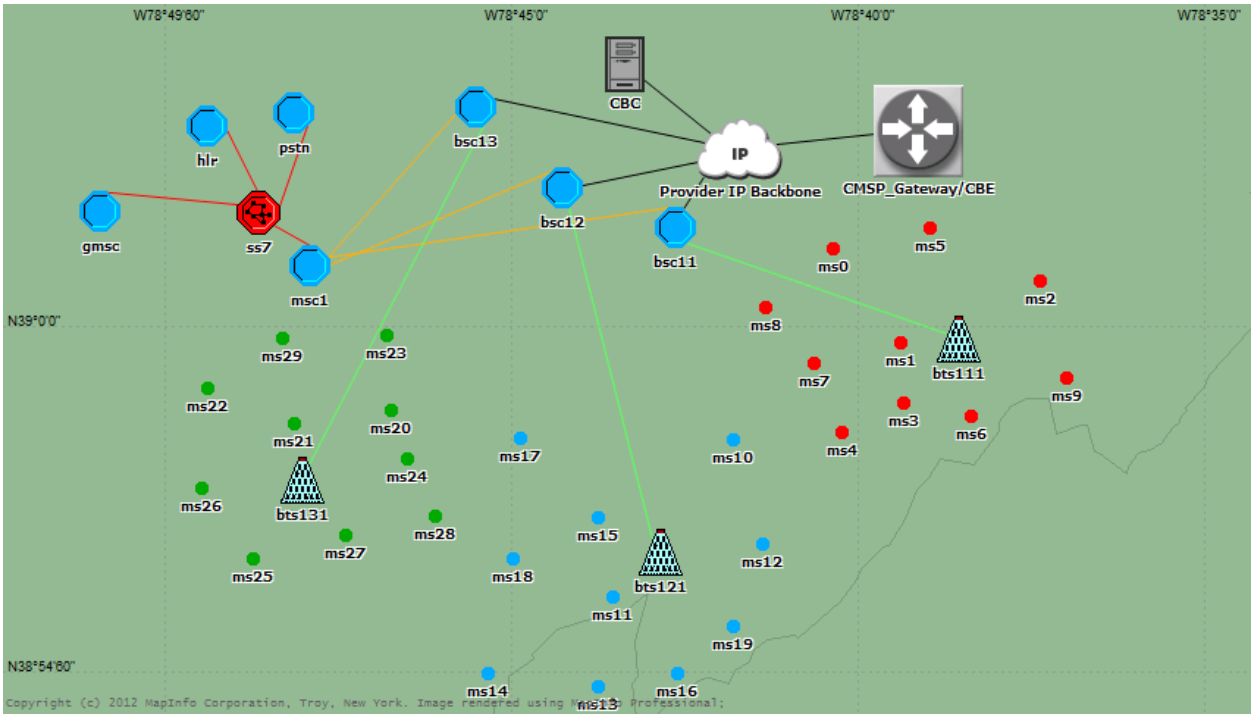

Figure 4-2 WEA GSM Model

4.8 SIMULATING AN LTE SUBNETWORK

The LTE-specific models for WEA were developed based on the built-in OPNET Modeler LTE models. The built-in LTE models do not support CBS; therefore, they were modified to be able to handle cell-broadcast traffic. The overall level of complexity of the LTE-specific models is much higher than that of the GSM-specific models, thus requiring much longer run times for the same simulation timeline.

The model of an LTE subnet is shown in Figure 4-3. OPNET Modeler's built-in LTE model library contains node models for three types of nodes: UE, eNodeB, and EPC. In LTE terminology, UE refers to handsets, eNodeB refers to cell towers, and EPC refers to the core network. In OPNET Modeler, a single EPC node models the entire EPC functionality of an LTE subnet. Further details of the LTE network model are described in Appendix A.

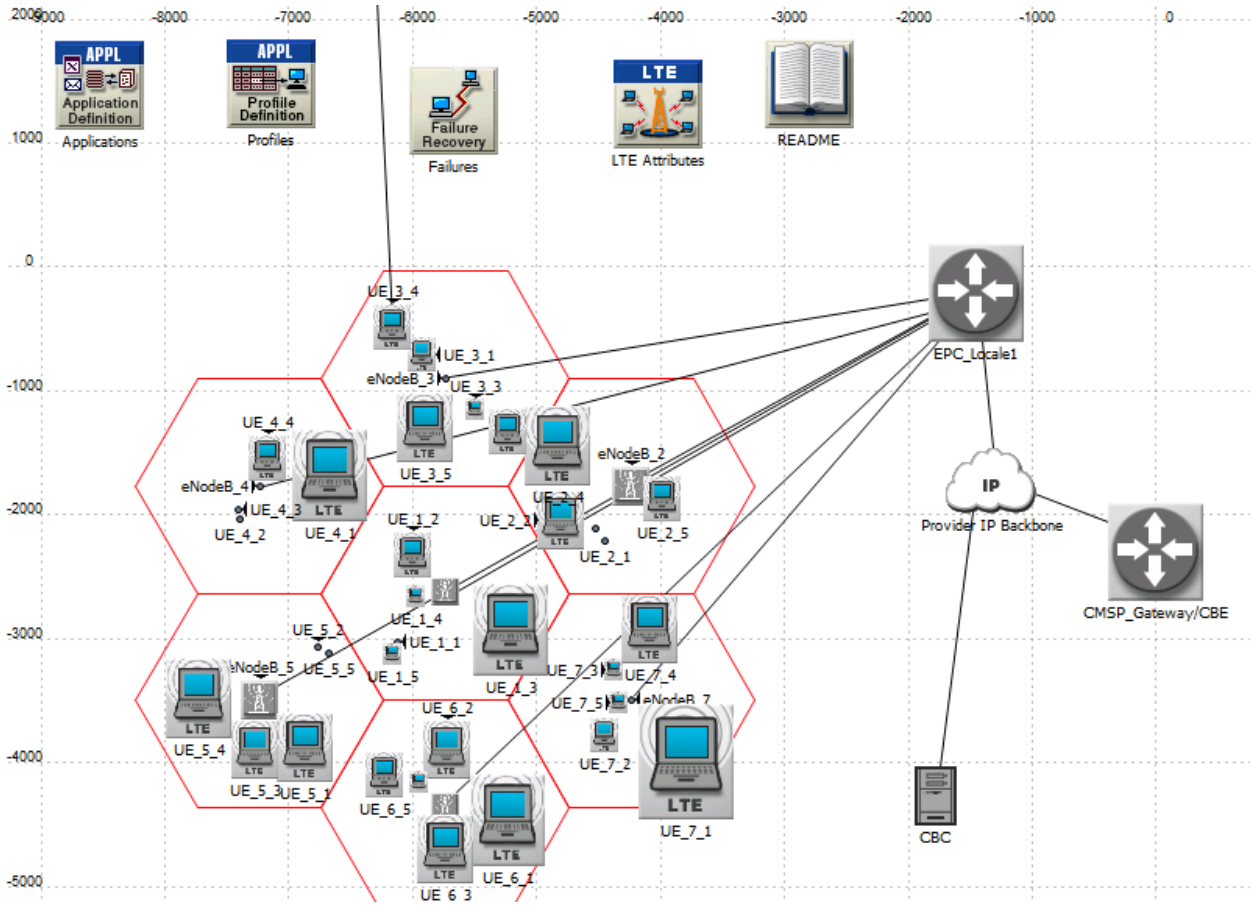

Figure 4-3 WEA LTE Model

4.9 SIMULATING CELLULAR HANDSET DEVICES

The handset model was developed based on OPNET Modeler mobile node models. It represents the behavior of WEA-capable handsets. Each handset node keeps track of several states in line with actual WEA handset features:

a. Handset on/off

b. If an alert message has been received

Animation of the handsets has been implemented to illustrate the arrival of alerts at each handset. All handset nodes also support mobility.

The goal of an alerting system is to make sure alerts reach people; therefore, adding more details such as alert mode (ring, vibrate, silent) and user acknowledgment of an alert will allow simulating the complete alerting process. Additional states for the handset model are planned as future work, to model alerting the user about a new message.

4.10 OUTPUT PERFORMANCE PARAMETERS

The WEA computer model uses alert delivery latency as the main performance metric. End-to-end alert delivery latency is measured from the time a WEA alert is generated at an AOS to the time it is received by an individual handset. Different handsets will in general receive an alert at different times because of several factors such as different service providers, different locations, interference and transmission errors, handset state, and so forth. As a result, a portion of the target population will receive an alert earlier than others, whereas a different portion may receive the alert too late to be useful, or even never receive it. The WEA computer model captures alert message delay and loss statistics at each node in the network from origination to reception. These statistics are then used for post-simulation analysis to infer performance of the end-to-end system and the individual system components.

Section 5

SIMULATION ANALYSIS

The impact of several factors on WEA performance was investigated using the computer model and different simulation scenarios. The analysis used alert delivery latency as the main performance metric, and simulated the impact of the following factors on alert delivery latency:

a. Cell Broadcast Network Traffic

b. Internet Delays

c. IPAWS-OPEN Load

d. Denial-of-Service (DoS) Attack

e. Transmission Errors

f. Active Phone Calls

Some of these factors, such as Internet delays and transmission errors, are at relatively low levels during normal operating conditions, but can potentially rise to extremely high levels following a major disaster. Several disaster scenarios were selected to set a proper context for investigating such high values. For this purpose, more than 20 disaster scenarios were first evaluated as potential simulation scenarios, and a representative subset was selected to cover each major delay factor. Selected scenarios for each delay factor are presented in Table 5-1.

GSM was used as the cellular technology in all of the simulations. Scenarios used in this analysis required long simulated timelines, so using complex LTE models would be infeasible. It is expected that the CMSP community will enforce the same cell broadcast capacity restrictions in LTE as are currently in place for GSM and UMTS. Therefore, simulation results obtained using GSM models should generally be applicable to LTE as well.

Table 5-1 Scenarios and Corresponding Delay Factors Used in the Simulation Analysis

Delay Factor	Disaster Scenario	Purpose
Cell Broadcast Network Traffic	Series of Weather Alerts	Analyze the impact of varying commercial cell broadcast network traffic on WEA during a series of weather alerts.
Internet Delays and IPAWS-OPEN Load	Chemical Attack Major Earthquake	Analyze the impact of extremely high levels of Internet delays and IPAWS-OPEN traffic load, which may happen after a serious disaster of national interest, such as a chemical attack or a major earthquake.
DoS Attack	Series of Weather Alerts	Analyze the impact of a DoS attack to IPAWS-OPEN during a series of weather alerts.
Transmission Errors	Nuclear Attack	Analyze the impact of very high levels of transmission errors, which may happen because of electro-magnetic noise after a nuclear attack.
Active Phone Calls	Series of Weather Alerts	Analyze the impact of high levels of phone call volume on WEA during a series of weather alerts.

5.1 GENERAL ASSUMPTIONS

General assumptions and configuration settings used in the simulation study are listed in Table 5-2.

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.

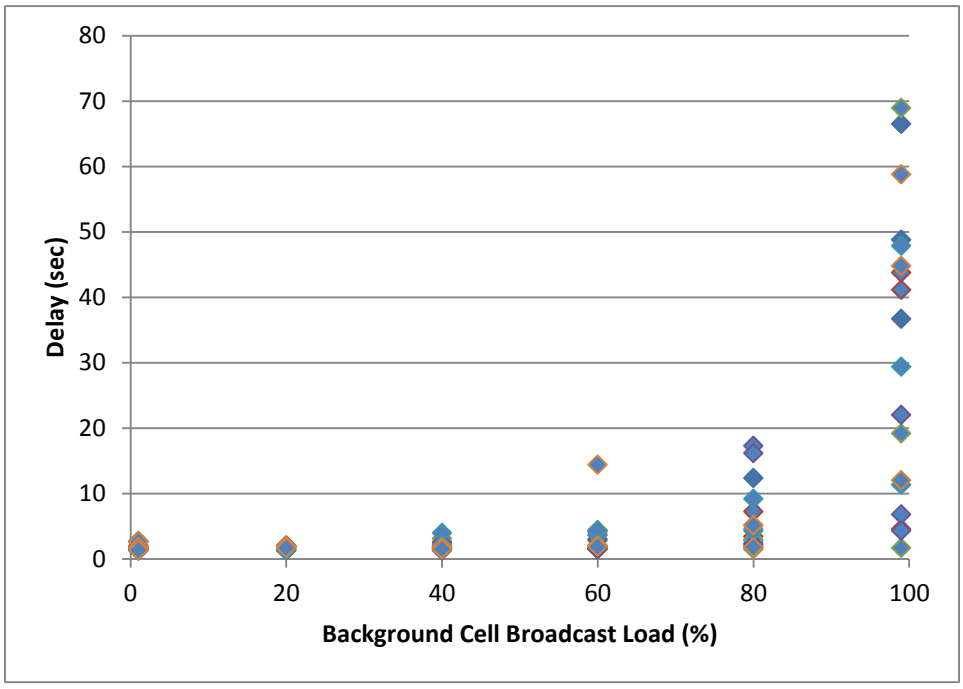

Figure 5-1 End-to-End Delay as a Function of Background Cell Broadcast Traffic

5.3 INTERNET DELAYS AND IPAWS-OPEN LOAD

The effect of Internet delays and excessive IPAWS-OPEN traffic load on WEA performance was investigated in the context of a chemical attack scenario and a major earthquake scenario. Because both scenarios involve disasters that are of high national significance, extremely high Internet delays and extremely high IPAWS-OPEN traffic load are to be expected. More specifically, Internet delays and IPAWS-OPEN traffic load were assumed to be initially at normal levels; they rise to high levels shortly after the event and then to extreme levels as the seriousness of the situation is realized.

The parameter values shown in Table 5-3 were used to model normal, high, and extreme levels. The average latency corresponding to high and extreme Internet traffic was chosen as 10 times and 20 times of normal latency, respectively. The high IPAWS-OPEN load was chosen as one-tenth of the extreme, which is five alerts per minute, and the extreme IPAWS-OPEN load was chosen as 50 alerts per minute, which matches the CMSAAC-recommended rate of 3000 messages per hour.

Table 5-3 Network Parameters for Normal, High, and Extreme Conditions

Network Traffic	Normal	High	Extreme
Average Internet Delay	50 ms	500 ms	1 sec
Average IPAWS-OPEN Load	Negligible	5 alerts per min	50 alerts per min

Figure 5-2 through Figure 5-6 show end-to-end WEA alerting delays in each major disaster scenario and under each network condition, broken down by the sources of delay.

As shown in Figure 5-2, most alerts experienced total delays around 2 seconds with normal levels of traffic conditions in the major earthquake scenario (the chemical attack scenario did not contain any alerts originated during normal levels of traffic conditions). This represents the ideal conditions for alert transmission.

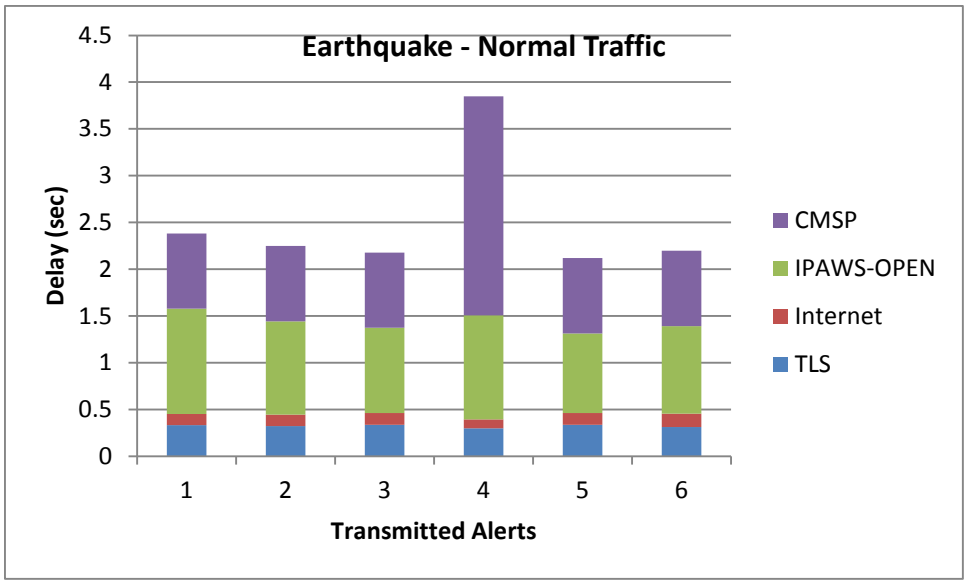

Figure 5-2 End-to-End Delay in Major Earthquake Scenario with Normal Network Traffic

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.

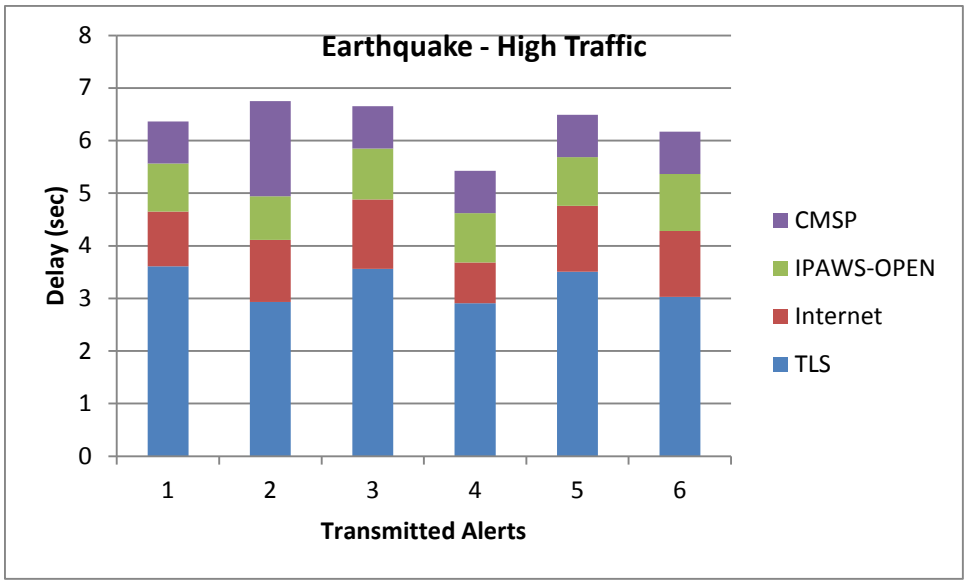

Figure 5-3 End-to-End Delay in Major Earthquake Scenario with High Network Traffic

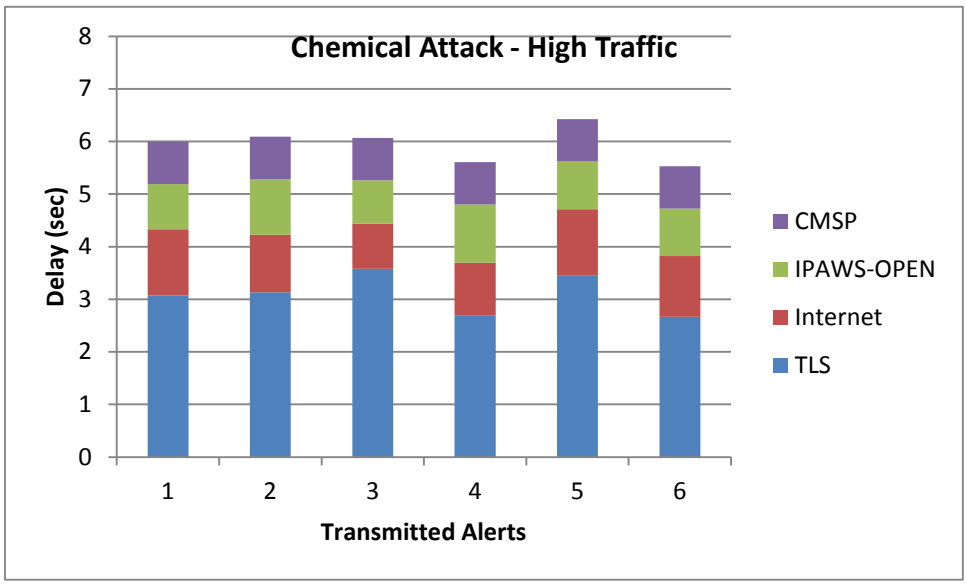

Figure 5-4 End-to-End Delay in Chemical Attack Scenario with High Network Traffic

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.

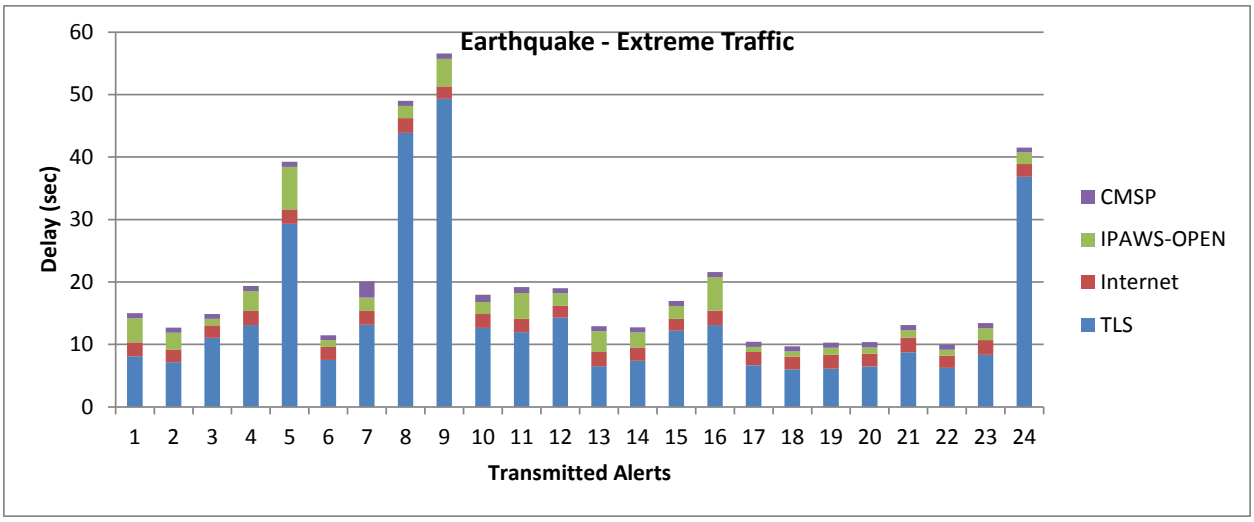

Figure 5-5 End-to-End Delay in Major Earthquake Scenario with Extreme Network Traffic

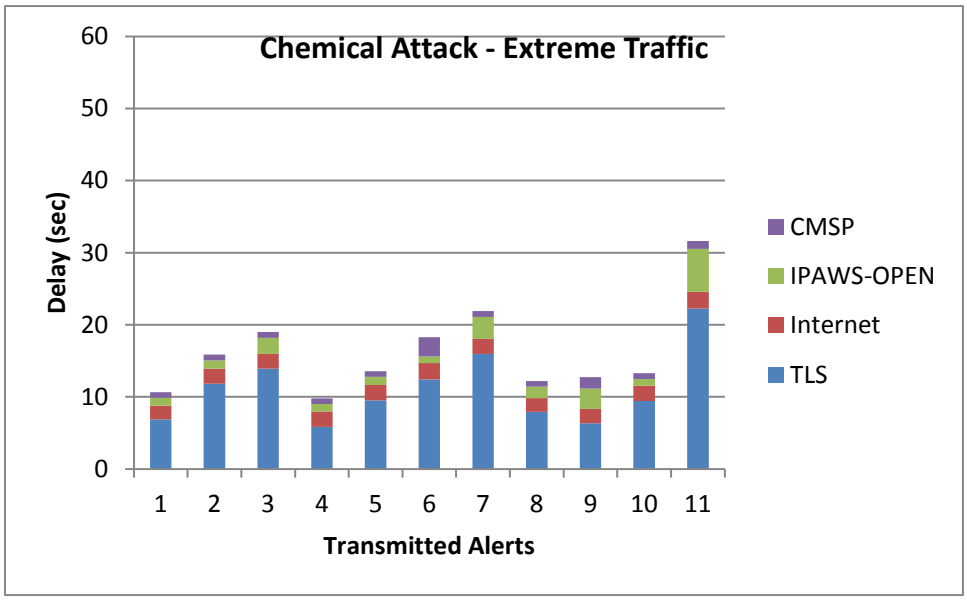

Figure 5-6 End-to-End Delay in Chemical Attack Scenario with Extreme Network Traffic

5.4 DENIAL-OF-SERVICE ATTACK

In the DoS attack scenario, potential delays caused by a generic DoS attack on the IPAWS Aggregator were investigated, assuming normal levels of Internet traffic.

A DoS attack was modeled by flooding the Aggregator model with invalid messages. The Aggregator model had a finite buffer to queue messages waiting for processing, and it dropped any new messages received while the queue was full. The flooding by the DoS attacker rapidly filled the

buffer, which introduced substantial delays in processing TLS packets and actual alert messages. Three different levels of DoS attack intensity were used, where the attack reached 100%, 110%, and 165% of Aggregator capacity. Three WEA alerts were transmitted at each intensity level, for a total of nine alerts. The simulation was repeated multiple times with different seed values.

Figure 5-7 shows the delays experienced by different WEA alerts in multiple runs of the scenario. The red triangles on the x-axis of the graph indicate when the level of DoS attack intensity is increased from 100% to 110%, and then from 110% to 165%. Because the simulated DoS intensity exceeds the IPAWS Aggregator capacity, some alerts are delayed by more than several minutes. At higher simulated DoS intensity levels, delays greater than 10 minutes were observed, and some alerts were never delivered during the simulation.

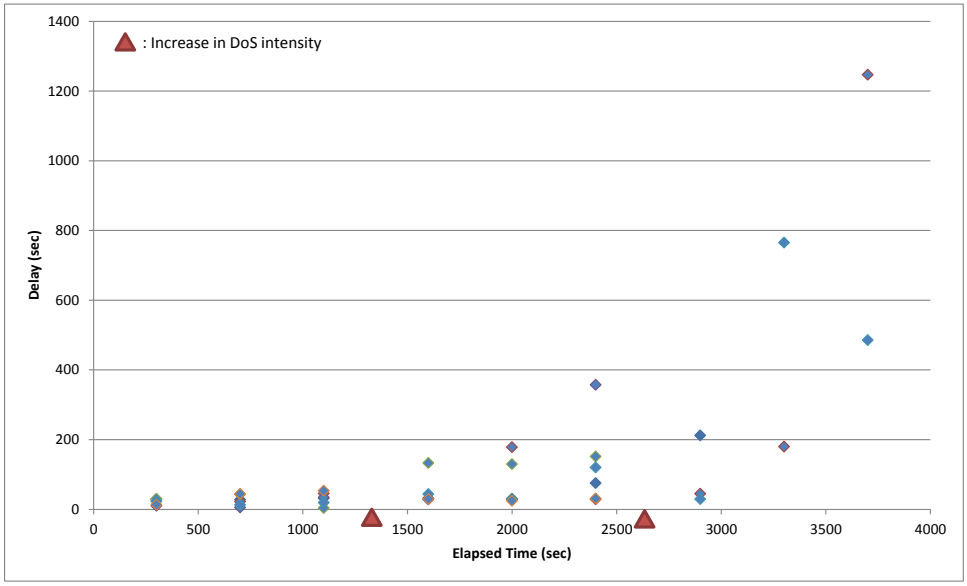

Figure 5-7 End-to-End Delays in Denial of Service Scenario

Although the DoS attack was modeled by message flooding, this model can simulate other types of DoS attacks as well. In particular, many DoS attacks are based on exhausting some limited resource at the target. The limited resource was modeled as buffer capacity, but other resources that can be manipulated by attackers (e.g., concurrently open TCP connections) are also represented by this model.

Results of this scenario emphasize the need for adequate defenses against a DoS type of attack. Details of IPAWS-OPEN security design were not available to JHU/APL, so the level of robustness against this type of attack could not be assessed further.

5.5 TRANSMISSION ERRORS

This analysis investigated the effect of different levels of transmission errors on WEA alerts. A major disaster scenario was used, in which a nuclear device was detonated. In such a scenario there would be total physical damage to portions of the CMSP infrastructure and to most electronic devices in the immediate area and partial damage in the surrounding areas. WEA would not be available in

the immediate area due to physical damage and the presence of electromagnetic noise. In surrounding areas, varying levels of electromagnetic noise would introduce transmission errors that result in frame (message) losses.

In the simulation, alerts were transmitted to four different areas, each with a different noise level but the same transmission power. The frame error rates (FERs) in these areas were chosen to be 0.1%, 1%, 5%, or 10%. Each cell broadcast message consists of four frames; therefore, an error in any one of the four frames resulted in a lost message. Four alert messages were transmitted to each area, and the transmission was repeated every 10 minutes.

Figure 5-8 shows the percentage of the powered handsets in an area that receives the alerts. Different color groups correspond to different areas with different FERs. Different plots with the same color show different alert messages transmitted to the same area, averaged over multiple runs. The horizontal axis is the time elapsed since the origination of each alert message. The results show that more than 90% of the handsets received the alerts during the first transmission for 0.1% and 1% FER. Moreover, the reception reached almost 100% after the second transmission at these FER levels. At 5% and 10% FER, only 60% to 80% of the handsets received the alert during the first transmission. Some of the handsets required four or more transmissions to receive the alert at these FER levels.

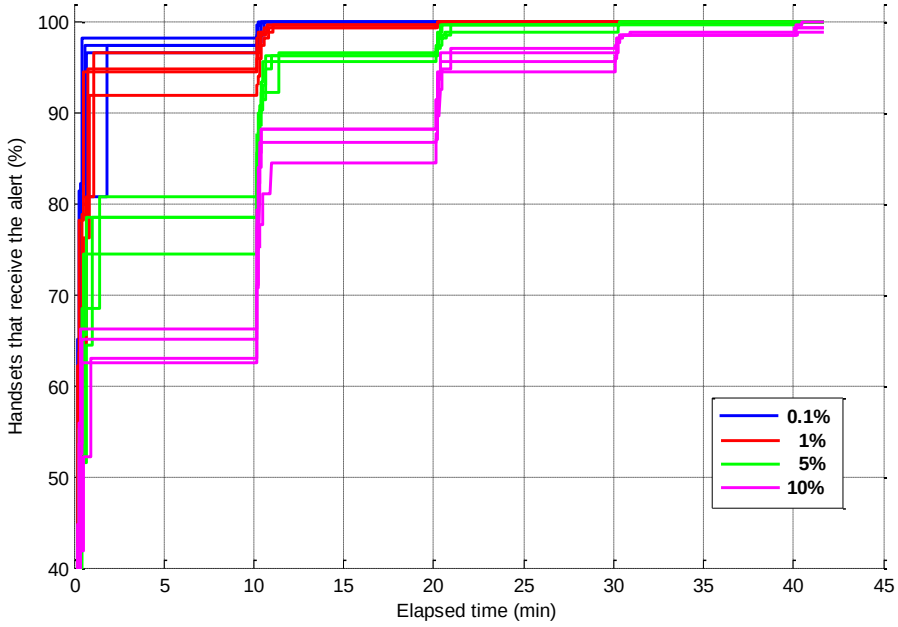

Figure 5-8 Alert Reception Function in Nuclear Detonation Scenario

5.6 ACTIVE PHONE CALLS

In GSM and UMTS networks, when a handset is involved in a phone call, it does not process the cell broadcast channel (CBCH). Consequently, handsets miss any WEA alerts transmitted while the device is engaged in a phone call. WEA relies on broadcasting the message multiple times (repetitions) to reach those handsets that missed previous broadcasts. A handset engaged in a phone

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/

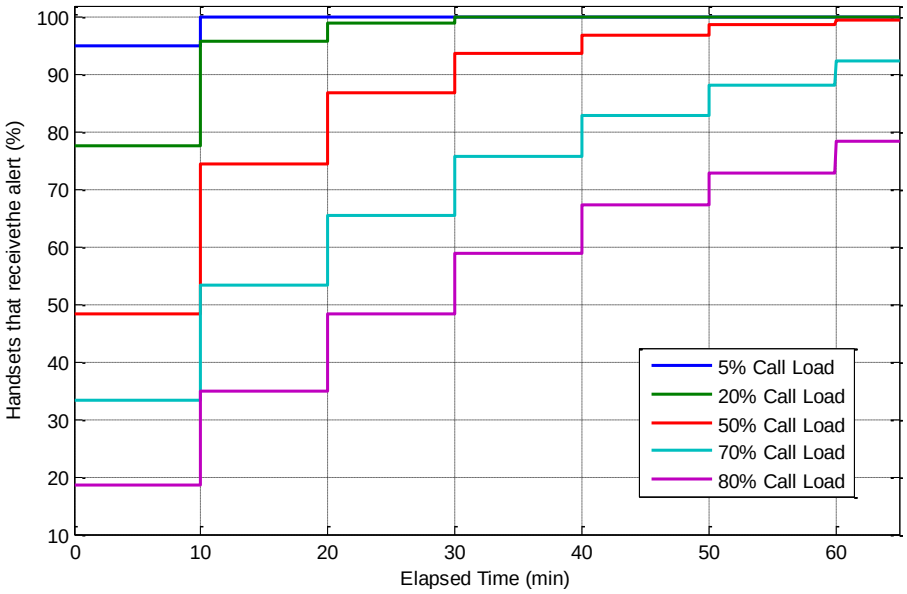

Figure 5-9 WEA Alert Reception at Different Levels of Phone Call Load

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

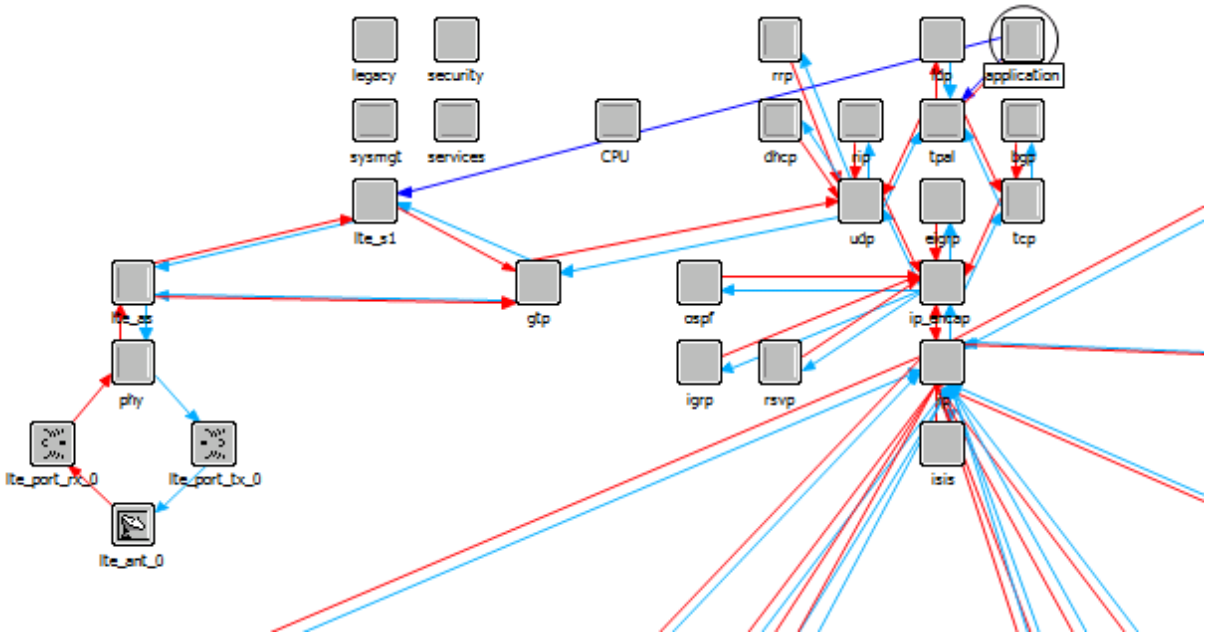

Figure A-1 Portion of Modified eNodeB Node Model for LTE

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.

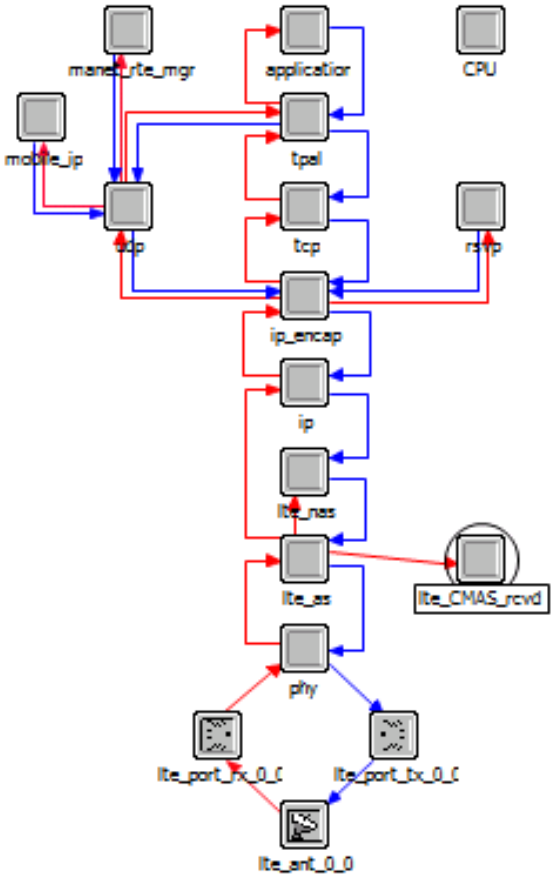

Figure A-2 Modified UE Node Model for LTE

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