NISTIR 8247

Guidelines for Generating Public Safety Benchmark Scenario Set

Richard Rouil
Chunmei Liu
Antonio Izquierdo Manzanares

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8247

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8247

Guidelines for Generating Public Safety Benchmark Scenario Set

Richard Rouil
Chunmei Liu
Antonio Izquierdo Manzanares
Wireless Networks Division
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8247

April 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Interagency or Internal Report 8247
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8247, 15 pages (April 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8247

Table of Contents

List of Figures

1. Disclaimer

Any mention of commercial products within this document is for information only; it does not imply recommendation or endorsement by NIST.

2. Introduction

There is a need to establish well-defined, public safety scenarios for the evaluation of current and future communication technologies for first responders. These scenarios can be based on historical data or hypotheses but need to be realistic. The scenario descriptions must contain enough detail to be considered representative of key public safety operations and their communications needs. The purpose of this document is to provide guidelines for developing these so-called "public safety scenarios".

3. Background

The performance evaluation of communication technologies can be done through a variety of methods, including analytical models, simulation models, emulation, or testing. The quality and usefulness (e.g. generalization) of the results are highly dependent on the assumptions made. In particular, for public safety communication, the behaviors and needs of the first responders are very different than those of commercial users. For example, while analyses of commercial networks typically consider uniformly distributed traffic and heavier traffic in the downlink, first responders are concentrated in an incident area, possibly generating a high volume of uplink traffic from video cameras. Reliability and coverage requirements are also much higher than commercial networks since losing connection, even for a few seconds, can be critical. For example, a firefighter may miss an evacuation order while moving inside a building that is on fire, or a police officer may not hear information about an armed suspect moving in his or her direction. Public safety communication scenarios found in the literature [1] [2] [3] [4] [5] [6] have mainly focused on network capacity needs, spectrum allocation, and network planning. These scenarios lack many details such as personnel locations and first responder traffic throughout the duration of the incident, making it difficult to reuse them for other research topics. Other public safety scenarios, such as those in [7], are very detailed regarding the first responders' activities but do not adequately capture the communication aspect of the incident. While different scenarios can be developed, each serving different objectives, it is important to create a set of scenarios that cover the different aspects of public safety operations. For example, the study of Quality of Service (QoS), priority, and preemption (QPP) will use incidents that generate a lot of data and may cause congestion, while the study of network resiliency may focus on scenarios that are coverage limited, such as wildfires. The catalog of incidents provided in [8] is a good starting point in identifying the various types of incidents to consider.

4. Public Safety Scenario Building Blocks

The development of public safety scenarios is shown in the building blocks in Figure 1. A scenario is defined as the combination of a detailed description of an incident and the networking capabilities provided during the incident. A documented implementation of a scenario will allow for reproducible results. To successfully provide valid information, each part will require inputs from different stakeholders.

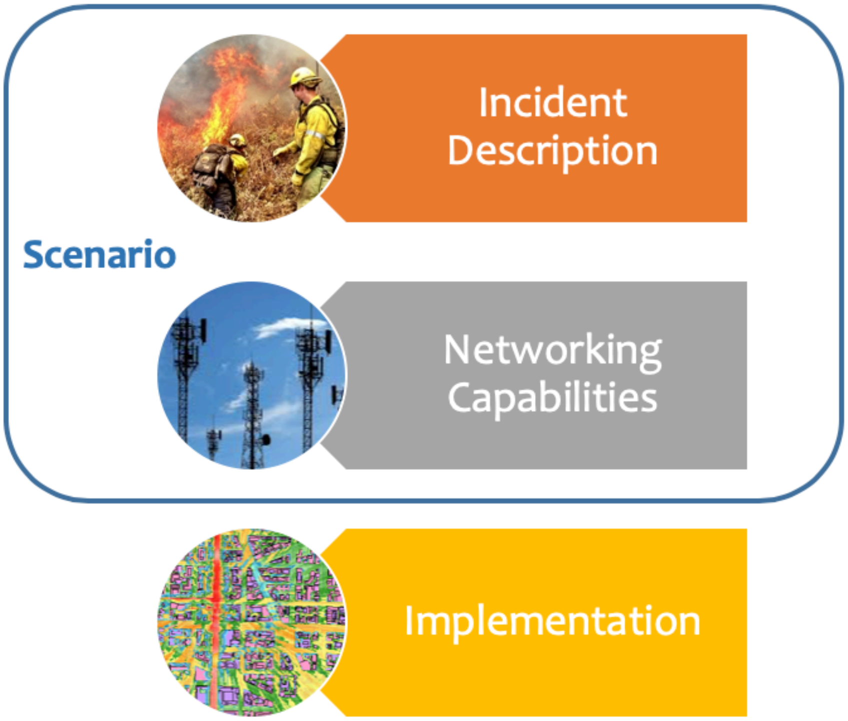

Figure 1: Public safety scenario building blocks

Incident description: Description of first responder activities, timing of events, and communication needs. The description of the incident should be technology independent in order to provide flexibility in the ways communication is provided. This effort requires input and validation from first responders to ensure that the details provide a realistic representation of the incidents considered.

Networking capabilities: Description of what is available with regards to communication technologies. This includes the network deployment, the types of devices used, and available services. While some input may come from first responders and operators when considering current capabilities, we expect that researchers will propose different solutions based on their research interests.

Implementation: Description of how the incident and communication capabilities are implemented. This includes assumptions and configuration parameters used in a particular implementation that are likely dependent on the tools employed.

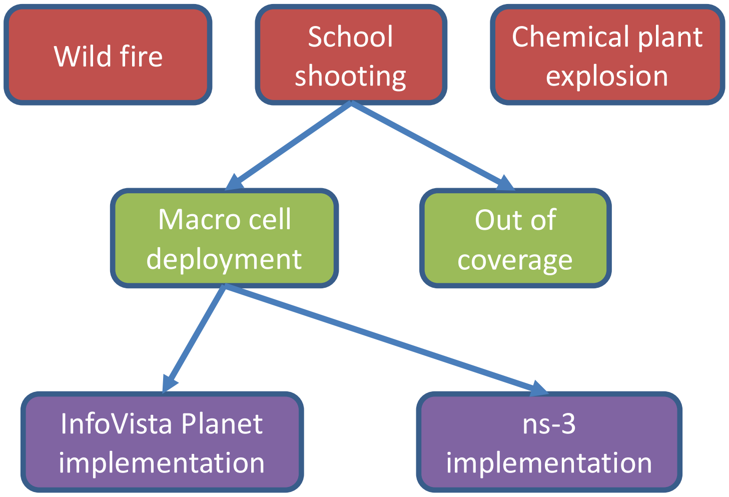

Figure 2: Examples of incidents and relationships with networking capabilities and implementations

Figure 2 shows examples of incidents that could be included in a scenario set. For each incident, multiple networking capabilities can be evaluated. For example, it is possible to study a school shooting scenario when the cellular network deployment is available, or in the case of an outage, where first responders may have to rely on deployables, direct mode communication, or both. Finally, each scenario can be evaluated on different simulation platforms, such as Planet [9] (a radio frequency planning tool), or ns-3 [10] (a discrete event simulator).

Using the proposed building blocks allows great flexibility in the development of a scenario. It is possible to focus on documenting a list of incidents without worrying about the networking capabilities and implementation. However, if a specific incident is of interest, a single incident scenario can be developed by all three building blocks. The structure of the building blocks also does not preclude the combination of multiple incidents into one scenario to create more complex scenarios.

5. Scenario Generation

As mentioned in Section 4, each scenario consists of two parts: incident(s) and networking capabilities. This section details data to be included in each part.

5.1. Incident Description

The information contained in the incident description must be detailed enough to understand the evolution of the incident(s) over time and the specific communication needs of each first responder. However, the description should not include technology specific information in order to be flexible. We identified the following key elements to be included in an incident description.

5.1.1. High level description

Brief description of the public safety incident under consideration, such as a ‘dirty bomb’ in New York City [6]. This information is intended to identify the type of incident (e.g., wildfire, shooting), environment (e.g., rural, urban, mountain), and the scale of the incident in terms of area, personnel, and equipment (e.g., 32-hectare fire with 50 responders).

5.1.2. Context

The context surrounding an incident is any information that helps researchers better understand the environment in which first responders operate and how it may affect the communication needs. This can help in establishing potential constraints to consider for the research.

Some elements to specify in the context include:

- Weather: indicates special weather-related conditions, such as tornadoes, dry wind, high temperature, icy conditions.
- Population: information about general public, such as number of occupants in a building, people attending a special event like a concert or sports event.

For example, if the incident occurs during high winds, the use of Unmanned Area Vehicles (UAVs) will be challenging. A storm with heavy rains may also cause a lot of background noise that impair the ability to communicate clearly.

5.1.3. Incident area

The incident area describes the layout of the incident and its immediate surrounding. This includes not only the size of the incident, but any additional information that may impact communication channels (especially wireless communications). As such the incident area description must include the following:

- Dimension: the size of the incident. It is important because public safety incidents vary greatly in size. For example, Hurricane Ike in Texas on Sept 13, 2008 [2] was almost 1500 km wide when it rolled across the Gulf of Mexico and eventually passed 160 km to the east of Dallas, Texas. However, a residential fire incident [11], which could occur in one apartment complex may be limited to few hundred feet.
- Terrain: a general description of the terrain (e.g., mountains, plains), or a specific location where terrain information can be retrieved (e.g., using Geographical Information System (GIS) data).
- Clutter type: a description of what is above ground, such as forest, residential, commercial. This is usually provided in the form of GIS data.
- Buildings: the location and shape of the buildings. This could also be provided by GIS data.

The detail of the information is likely to vary between incidents. In the case of a shooting in a school, the location of the buildings, as well as their sizes (and possible materials, layout, etc.) are important, but it would be almost impossible to describe all the building configurations in a natural disaster scenario.

5.1.4. Personnel

Just as the size of the incident varies, public safety incidents vary in terms of the number of first responders involved. One example of a large number of first responders is Hurricane Ike mentioned above [2], where more than ten thousand first responders were involved. The residential fire incident [11] is an example of an incident that involves a small number of first responders, with fewer than 20 first responders. Note that incidents within a small geographic area could involve a large number of first responders, and vice versa. For example, the toxic gas incident described in [1] could encompass only one square mile while its response could involve more than 300 responders.

The following information needs to be provided regarding each incumbent:

- Type (e.g., law enforcement, emergency medical services (EMS) units, firefighters).
- Role (e.g., special weapons and tactics (SWAT) member, patrol, incident commander).
- Status (e.g., on/off duty).
- Jurisdiction or groups.

When applicable, grouping of personnel information can be done based on the type, role, or both.

Since incident responses follow standard operating procedures (SOPs) and pre-defined organizational structures, it could be useful to indicate the Incident Command System (ICS) [12] used for the incident.

5.1.5. Equipment

Equipment information refers to non-personnel assets that are involved in the incident. Those assets may be associated with certain communication needs (e.g., video feed from a dash camera) and can also be used to provide certain networking capabilities.

The following information is needed for each piece of equipment:

- Type: the asset type (e.g., car, truck, helicopter).
- Mobility: describes if the equipment could be moved during an incident.

Note: this list does not limit the equipment used to support the networking capabilities. For example, given an incident, it should be possible to study the impact of Cell on Wheels (COWs) or drones, which may not be listed in this section.

5.1.6. Communication Needs

Based on the proposed building blocks, the description must contain details about information exchanges that occur throughout the incident without specifying any particular technology, to the extent possible.

For example, a description can include:

- Upon entering the building, each SWAT team lead starts reporting location information to the incident commander periodically, at least every 2 min, or
- Incident commander must monitor locations of SWAT teams as they enter the building and at least every 2 min.

This would allow the same incident to be tested on a variety of communication capabilities such as:

- SWAT team leads only have access to voice and manually report every 1 min to 2 min or,
- SWAT team leads are equipped with global positioning system (GPS)/indoor location devices that send information onto the incident command screen every 10 s.

Specifically, each communication path must include:

- Source: the initiator of the communication, which can be a personnel or device.

- Destination: the target of the communication. The destination can be a single entity or a group (in which case group affiliation must be specified).
- Purpose: indicates what this communication is used for. Examples include location reporting, indoor building monitoring, and access to building maps.
- Constraints: list of requirements associated with the communication. This can be how frequently it must be done (e.g., location must be reported at least every 2 min), how quickly some information is needed (e.g., maps must be available within 10 min).
- Importance: a characterization of how important the communication is in this incident. This information can be used to associate priorities to devices, users, applications, or any combination, and to evaluate the impact of that this communication will have on the incident response.

5.1.7. Timeline of events

The timeline documents events that occur during the incident and provides critical information to determine where the responders are located, what they are doing, for what purpose, or in response to what.

A time needs to be associated with each event. This time can be a fixed value (at t=30 min, an explosion in building A occurs) or a range of time (SWAT team arrives at the scene between 10 min and 20 min). Note that in this example t=0 min refers to the beginning of the incident.

The event list should include:

- Unit deployments: initial position of the responders when they arrive at the scene.
- User mobility: personnel trajectories including pattern, destination, and speed (contextual information can be added to make a scenario descriptive (e.g., EMT carrying injured woman to the ambulance)).
- Communication events: list specifying the start and stop times of each of the communication needs (e.g., at time 27 min, SWAT team leader A starts communicating with Incident Command until he leaves the building at time 50 min).
- Context events: those events are not related to first responders but may trigger a response, thus providing useful information (e.g., explosion, fire expanding, shots being fired).

5.2. Networking capabilities

For a given incident, there are an undefined number of technological solutions that can be studied. This part of the work is where public safety practitioners and operators can document existing deployments and where researchers can envision new technologies to better serve the needs of first responders.

The communication capabilities have been separated into two elements: network infrastructure (i.e., core, access network, and devices), and services and applications as described below.

5.2.1. Network Infrastructure

Information regarding network infrastructure aims at covering the core networks, the radio access networks (RANs) inter-connected to the core, and the subscribers that connect to the RAN.

When generating scenarios by combining the incident(s) and the network, it is important to note that the location of the incident(s) relative to the network plays a significant role in the resulting user experience. One example is that, for an incident with small geographic size, the amount of traffic the network can serve differs significantly when the incident is at the center of the cell or at the cell edge, and when the incident is served by one sector or multiple sectors. It is expected that the same incident will be tested at different locations relative to the same network unless specified otherwise.

5.2.1.1. Core network

The description of the core (e.g., backbone) network includes the architecture, layout, and configuration parameters used to connect the RANs to the servers hosting services and applications available to the first responders. Therefore, the description includes the backhaul used to connect the RANs to the core network, as well as the core network itself.
Parameters for intermediate nodes include:

- Type: type of the intermediate node in the network (e.g., router, switch).
- Protocols: list of protocols and supported versions (e.g., Internet Protocol (IP) version 4, IP version 6, tunneling).
- Processing delay: time needed to route a packet from an incoming interface to an outgoing interface (e.g., in the form of statistical distribution).
- Interfaces: description of each interfaces available on the node.

Parameters for each interface include:

- Technology: the type of link (e.g., Institute of Electrical and Electronic Engineers (IEEE) 802.3, IEEE 802.11, 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE)).
- Queue: the size of the queue (in bytes or packets) and dropping policies (e.g., drop tail, random early detection (RED)).

Parameters for the links include:

- Technology: the type of link (e.g., coaxial, fiber, microwave).
- Capacity: the maximum bandwidth or data rate of the link.
- Delay: the link latency.

The information provided will determine the capacity of the core network, as well as the delay and loss associated with packets going through the core network.

5.2.1.2. Radio access network

The RAN defines a list of access points that enable user devices to connect to the network. For each point of access, the following list contains parameters that should be specified to accurately represent its configuration:

- Technology: the radio access technology used (e.g., LTE, IEEE 802.11).
- Carrier frequencies: the operating frequencies, specified in frequency (e.g., 700 MHz) or band (e.g., Band 14). In case of frequency division duplexing (FDD), an uplink and downlink value are needed.
- Bandwidth: The frequency bandwidth used (e.g., 10 MHz downlink and 10 MHz uplink)

- Location: The location of the point of access (e.g. cell tower). The location can be derived from an existing network deployment (e.g., using GPS coordinates) or from generic layouts (e.g., using a hexagon layout with fixed inter-site distance (ISD)).
- Antenna configuration: the antenna parameters that determine the wireless signal transmitted such as transmit power, antenna height, and radiation pattern.
- Technology specific parameters: each technology has specific parameters that will affect its performance. Any parameter that can significantly affect coverage or capacity should be specified.

5.2.1.3. Subscriber devices

In our context, a subscriber device is any equipment that can exchange information with another subscriber or server by connecting to the RAN, or over the air in case the devices communicate directly with each other. This includes not only handheld devices such as cell phones or tablets, but also connected vehicles, drones capable of transmitting data, sensors, and camera devices. For each device used in the incident response, information that is relevant to the device's communication capability must be included.

While an exhaustive list is impossible to compile due to the variety of devices, technologies, and aspects that may or may not be relevant to a particular study, the following parameters are deemed important:

- Technology: what technology is used to communicate (e.g., LTE, IEEE 802.11, IEEE 802.15.4).
- Transmit power: maximum transmit power of the device
- Noise floor: degradation of the signal-to-noise ratio (SNR), caused by components in a radio-frequency (RF) signal chain.
- Modulation and coding schemes (MCS): types of modulations supported by the device. Advanced devices typically support higher MCS allowing for higher throughput.
- Antenna configuration: number of antennas, the gain and pattern associated. The supported modes can also be specified (e.g., Multiple Input / Multiple Output (MIMO), transmit diversity, beamforming).
- Battery life: a duration that the device can operate, or a power consumption associated with a battery size.

5.2.2. Services and Applications

For each communication need listed in the incident (See Section 5.1.6), there can be an associated service or application that is available to the first responders.

The following information must be provided:

- Communication need: a reference to the communication need specified in the incident(s) that this service will satisfy (e.g., location tracking for SWAT team).
- Type: the application type (e.g., Voice over LTE (VoLTE), streaming video).
- Application behavior: while the incident(s) will indicate when an application should start and stop, the application used will determine the on/off pattern (e.g., if voice is used to report location, it may happen less frequently than an automated GPS tracking application). Similarly, the packet transmission pattern or packet process is needed.

This could be codec information (e.g., adaptive multi-rate wideband (AMR-WB) 12 kb/s, H.264 1080p), or transmission parameters (e.g., packet size distribution, packet interval distribution). Since a particular data rate can be achieved in many ways (e.g., constant traffic or burst traffic), it is important to provide information that reflects the actual application behavior.

- Application specific properties: when applicable, this is any information relevant to the application behavior. For example, a File Transfer Protocol (FTP) download can be characterized by the file size.
- QoS requirements: typical public safety incidents use a variety of applications with different guaranteed QoS requirements [1] [5] [13], which means that some applications only operate within a certain level of network performance. For example, if the packet loss or packet delay is too high, there is a back-off mechanism or the application shuts down. This information, when provided, will guide resource allocation schemes and help determine if the network performance is meeting the application requirements.
- The application server: any information that will affect the service performance. For example, the location of the server hosting the application will affect the communication latency.

6. Implementation

Testing or modeling a particular scenario can be done using a variety of tools. Each tool typically provides different levels of details and abstraction based on its purpose, and capabilities often change over time. Important implementation elements are discussed in the following text.

6.1. Implementation details

6.1.1. Propagation/Channel models

Propagation models are used to calculate the signal degradation between a transmitter and a receiver. There are many models defined in standard documents such as International Telecommunication Union (ITU) or 3GPP, as well as in the literature. Each model characterizes a particular environment (e.g., urban, rural, indoor) and its complexity can vary. Some are stochastic models which only consider the distance between the transmitter and receiver while more complex models take into account various obstacles (e.g., terrain, buildings), and how they affect the signal (e.g., diffraction and reflection).

6.1.2. Application models

The traffic generated by an application is affected by its model. Some tools do not consider time, and applications can be characterized by a data rate and a utility factor (e.g., a voice application generated 12 kb/s of traffic in each direction and is used 20 % of the time). Tools that consider time need more information including distribution of packet size, packet interval, and when applications are turned on and off. The models may also reflect the dynamic behavior of applications depending on the network condition (e.g. an application may shutdown or adjust its transmission rate during congestion).

6.1.3. Protocol implementation

For cases where multiple implementations of a protocol are available, it is necessary to specify which version is being used. One example is TCP where many variants have been developed (e.g., Tahoe, Reno, NewReno, SACK, Vegas, BIC, CUBIC) to handle network congestion differently. For scenarios that are capacity limited, this becomes an important parameter.

6.1.4. Mobility

The incident description may include mobility patterns that are not supported by the tool or are ignored to make an implementation simpler. In this case, user locations may be fixed throughout the incident, though their location may be randomized.

6.2. Code availability

Detailed documentation of the implementation is necessary to allow other researchers to reproduce the same results. However, to reduce the risk of missing important information, efforts should be made to provide source code or project files that allow other researchers and practitioners to replicate the obtained results.

References

[1] NPSTC Technology and Broadband Committee, "Priority and Quality of Service in the Nationwide Public Safety Broadband Network," Rev. 1.4. August 2015.

[2] "Emergency Communications during Hurricane Ike Harris County Regional Radio System: A Technical Case Study by the Federal Communications Commission’s Public Safety and Homeland Security Bureau’s Communications Systems Analysis Division," December 01, 2009.

[3] "Emergency Communications During the Minneapolis Bridge Disaster: A Technical Case Study by the Federal Communications Commission's Public Safety and Homeland Security Bureau's Communications System Analysis Division," November 13, 2008.

[4] C. Smith, "Future First Responders and FirstNet: Response to a multiple-vehicle accident (MVA) scenario," http://urgentcomm.com/public-safety-broadbandfirstnet/future-first-responders-and-firstnet-response-multiple-vehicle-accid, 2014.

[5] M. Navolio, "Minnesota Department of Public Safety, Public Safety Wireless Data Network Requirements Project Needs Assessment Report," May 27, 2011.

[6] "Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan—NBP Public Notice #8, COMMENTS OF THE CITY OF NEW YORK," November 2009.

[7] The National Institute for Occupational Safety and Health (NIOSH), "Fire Fighter Fatality Investigation and Prevention," [Online]. Available: https://www.cdc.gov/niosh/fire/investigations/investigations.html. [Accessed 29 Mars 2019].

[8] Y.-Y. Choong, S. T. Dawkins, K. Greene and M. F. Theofanos, "Incident Scenarios Collection for Public Safety Communications Research: Framing the Context of Use," NIST, 2017.

[9] InfoVista, [Online]. Available: https://www.infovista.com/products/Mentum-Planet-Live -RF-planning-and-optimization. [Accessed 28 March 2018].

[10] NS-3 Consortium, "ns-3 Network Simulator," [Online]. Available: https://www.nsnam.org/. [Accessed 29 March 2019].

[11] C. Kiefer, A. Gibson, C. Seymour and A. Handa, "Firefighter-Residential Fire Scenario Bandwidth Simulation Final Report," https://twiki.wnd.nist.gov/twiki/pub/ProjectPublicSafety/TrafficModeling/Residential_Fire_Scenario_Report_Final_June_27_2008.doc. 2008.

[12] Federal Emergency Management Agency, "National Incident Management System (Third edition)," 2017.

[13] FirstNet CTO Whitepaper, "Nationwide Public Safety Broadband Network (NPSBN) QoS Priority and Preemption (QPP) Framework," Version 0.9 draft. November 18, 2015.