International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/jb1exe12

Article – e005

Review of Security Vulnerabilities and Authentication Mechanisms in Cellular Public Warning Systems: Spoofing, Alert Suppression, and Verification Approaches

Nomsa Nkosi[1]✉

[1] *University of Cape Town, South Africa*

Received: 02/09/2026 **Revision Received:** 01/10/2026 **Accepted:** 06/10/2026

ABSTRACT

Cellular public warning systems provide a mechanism for disseminating urgent alerts to mobile devices within geographically defined areas. Their effectiveness depends not only on timely message delivery but also on the authenticity, availability, and interpretability of warnings received by the public. Security research has demonstrated that cellular warning mechanisms can be exposed to message spoofing, unauthorized alert injection, and alert suppression, creating risks of false public instructions and missed legitimate warnings. This critical narrative review examines the security properties of cellular public warning systems, with particular attention to LTE and 5G environments, the relationship between broadcast signaling and warning authentication, and the feasibility of proposed verification mechanisms. We draw on experimental security research, cellular standards, and studies of public warning communication. We distinguish authentication of warning content from authentication of the cellular signaling environment and examine the limits of approaches that require network changes, device modifications, or observations from several cells. A seven-dimensional threat-to-control framework is proposed covering adversarial capability, entry point, attack mechanism, affected security property, verification mechanism, deployment dependency, and residual risk. The review finds that neither authenticated network signaling nor improved warning-message design independently resolves the full range of spoofing and suppression threats. Effective protection requires attention to message provenance, network trust boundaries, warning availability, operational deployment constraints, and the ability of recipients to interpret alerts correctly. Further research is needed to evaluate defenses under realistic deployment conditions, particularly where legitimate warning delivery must remain reliable during emergencies.

KEYWORDS: Cellular public warning systems; wireless emergency alerts; LTE; 5G; cell broadcast; alert spoofing; alert suppression; authentication; emergency communications; mobile network security

1 Introduction

Public warning systems are essential components of emergency communication infrastructure. They enable authorized organizations to disseminate information about natural disasters, severe weather, public safety threats, and other situations requiring immediate public attention. Cellular networks provide a widely deployed channel for delivering such warnings to mobile devices. Depending on the national implementation, warning services may use cell broadcast mechanisms to distribute geographically targeted messages without requiring individual recipient subscriptions or conventional point-to-point messaging. The effectiveness of these systems depends on several properties. Warnings must reach the intended population within an appropriate period. Their content must accurately represent instructions issued by an authorized source. Recipients must also be able to distinguish legitimate warnings from misleading or malicious communications.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Security weaknesses can undermine these requirements. A false warning may cause unnecessary public concern, disrupt transportation, or encourage people to take inappropriate actions. Conversely, suppression of a legitimate warning may prevent recipients from receiving information needed to respond to an emergency. The risk is serious because recipients often treat public warnings as authoritative. Research has demonstrated practical attacks against cellular warning mechanisms. Lee et al. [1] investigated the spoofing of emergency alerts in 4G LTE networks, illustrating how weaknesses in the warning-delivery environment can permit unauthorized warning presentation. Bitsikas and Pöpper [2] subsequently examined attacks against warning and emergency mechanisms in 5G, demonstrating that the evolution of cellular networks does not automatically eliminate all relevant threats.

Both studies show that warning security depends on the signaling and trust mechanisms used to deliver an alert. Yet warning security is not exclusively a cryptographic problem. Public warning messages must remain deliverable under emergency conditions, including periods of network congestion or infrastructure degradation. Security controls that introduce excessive dependencies or failure conditions may adversely affect the availability of legitimate warnings. Also, even an authentic warning may be ineffective if its content is unclear or recipients misunderstand the required action. Research on wireless emergency alert communication therefore provides an important complementary perspective [3–7]. We examine the security vulnerabilities and authentication mechanisms associated with cellular public warning systems. Our objectives are to:

1. Identify the principal spoofing and suppression threats affecting cellular warning delivery.
2. Examine the security assumptions and limitations of existing warning mechanisms.
3. Distinguish authentication of warning content from authentication of cellular system information.
4. Critically evaluate cryptographic, infrastructure-based, and cross-cell verification approaches.
5. Assess the relationship between technical authenticity and effective public warning communication.
6. Propose a structured framework for comparing threats and corresponding controls.

We focus mainly on cellular public warning mechanisms associated with LTE and 5G networks. We do not attempt to cover every emergency communication channel.

2 Review Approach and Scope

2.1 Review design

We use a critical narrative review approach. The analysis draws on peer-reviewed cellular security research, relevant technical standards, publicly available research preprints, and studies of wireless emergency alert communication. The aim is to compare security threats and proposed defenses while identifying differences in technical assumptions, experimental evidence, and deployment feasibility. The review is not a systematic review or meta-analysis. The available studies investigate different cellular generations, attack models, warning implementations, and defense mechanisms. Their results therefore do not support a meaningful pooled estimate of attack success or defense effectiveness.

2.2 Scope of the review

We focus on cellular warning delivery and its associated security properties. Relevant topics include unauthorized warning generation, radio-level spoofing, alert suppression, signaling authentication, warning provenance, and verification using observations from multiple cells. The analysis also considers the role of warning-message design and public interpretation where these affect the practical consequences of technical compromise. We do not treat ordinary SMS messaging, internet-based notifications, and cellular broadcast warnings as technically interchangeable.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

2.3 Evidence classification

We distinguish three forms of evidence. Experimental security research provides evidence of vulnerabilities or defenses under specified technical conditions. Standards documents describe requirements, message structures, and supported procedures. Communication studies examine how warning messages are interpreted and acted upon by recipients. Each source type answers a different question. A standard describing a supported warning mechanism does not demonstrate that every deployed implementation is secure. Likewise, a laboratory attack demonstration does not establish the frequency with which the attack occurs in operational networks.

2.4 Limitations of the approach

We do not claim exhaustive coverage of all cellular warning implementations. National deployments, device behavior, network configurations, and regulatory requirements may differ. Some proposed defenses remain at the research or prototype stage and have not been evaluated through large-scale operational deployment. We take these limits into account when judging how widely the findings apply.

3 Cellular Public Warning System Architecture

3.1 Purpose and operational requirements

Cellular public warning systems are designed to distribute urgent information to devices located within a defined geographic area. Unlike conventional one-to-one messaging, cell broadcast can distribute information to many compatible devices through the cellular network. Cell broadcast is useful when a large population must be warned quickly. The 3GPP Public Warning System requirements specification [8] describes requirements for warning services supported by cellular networks. The 3GPP Cell Broadcast Service specification [9] provides relevant technical procedures and message structures. Together, the specifications provide the standard basis for cellular warning delivery. Still, the presence of standardized functionality does not by itself guarantee resistance to adversarial radio signaling.

3.2 Warning originators and delivery infrastructure

A typical public warning process involves an authorized warning originator, an alert distribution system, mobile network infrastructure, and recipient devices. The precise implementation varies between jurisdictions and network operators. Warning information may pass through several organizational and technical components before reaching a mobile device. Each component introduces assumptions concerning authorization, integrity, availability, and correct message handling. The end-to-end security of a warning therefore depends on more than the final radio transmission.

3.3 Cell broadcast and geographic targeting

Cell broadcast is designed to deliver messages through selected cellular coverage areas. Operators can target a geographic area without identifying each recipient. At the same time, the radio environment creates a potential attack surface. Mobile devices must interpret network signaling to determine the information transmitted by nearby cells. If an adversary can cause a device to accept unauthorized signaling or warning content, the device may display information that did not originate from a legitimate warning authority.

3.4 Standards and national implementations

ETSI TS 102 900 [10] specifies requirements associated with the European public warning approach commonly referred to as EU-ALERT. The Common Alerting Protocol, CAP 1.2 [11], provides a structured format for representing warning information across alerting systems. CAP and the cellular standards serve different parts of the warning chain. CAP addresses the representation and exchange of alert information. Cellular warning standards address requirements and procedures associated with

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

distribution through mobile networks. As a result, the use of a standardized alert format should not be confused with end-to-end cryptographic verification by the receiving device.

3.5 Security boundaries

The warning architecture includes several distinct security boundaries. The first concerns whether a warning was authorized by the legitimate issuing organization. The second concerns whether the warning content remained intact during processing and distribution. The third concerns whether the receiving device is interpreting signaling from a legitimate network source. The fourth concerns whether the warning reaches the intended recipient. Each boundary needs separate analysis because an attack or defense may affect only one security property.

4 Security Properties of Cellular Warning Systems

4.1 Authenticity

Authenticity concerns whether a warning originates from an authorized source. A warning may appear legitimate because it uses a familiar alert interface or message category. Yet presentation within an official-looking device interface does not establish cryptographic provenance.

4.2 Integrity

Integrity concerns whether warning content has been modified without authorization. A message may originate from an authorized source but become altered through compromise or unauthorized processing. Integrity protection therefore addresses a different question from whether the message was issued by the correct authority.

4.3 Availability

Availability concerns whether legitimate warnings reach intended recipients. Suppression attacks target this property. A system may successfully reject forged messages while remaining vulnerable to attacks that prevent authentic warnings from being received.

4.4 Timeliness

Emergency warnings may lose practical value if they arrive too late. Authentication and verification mechanisms must be evaluated for their effect on warning delivery latency. A defense that significantly delays message presentation may create an operational trade-off.

4.5 Geographic correctness

Warning systems are intended to reach populations within relevant geographic areas. Unauthorized or inaccurate targeting may result in warnings being displayed outside the intended area or not reaching people who need them. Geographic correctness is therefore an important operational security property.

4.6 Interpretability

Recipients must understand the warning and the recommended protective action. Research on wireless emergency alert communication demonstrates that message content and presentation influence public interpretation [3–7]. Interpretability is not equivalent to cryptographic security, but it affects whether the warning system achieves its public safety objective.

5 Threat Models and Adversarial Capabilities

5.1 Remote infrastructure compromise

An adversary may attempt to compromise systems involved in warning origination, processing, or distribution. Such attacks differ from radio-level spoofing because they target the infrastructure or organizational processes responsible for producing legitimate messages. The available research does

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

not establish that all such compromises are equally feasible. Their likelihood and consequences depend on the architecture and security controls of the relevant deployment.

5.2 Radio-level adversaries

A radio-level adversary may attempt to transmit signals that nearby devices interpret as legitimate cellular signaling. The model covers false base stations and manipulated signaling. The adversary's capabilities may depend on radio equipment, proximity, signal conditions, cellular generation, and device behavior. Experimental feasibility under one configuration should not be generalized to every operational network.

5.3 Device-level compromise

A compromised mobile device may display misleading information independently of the cellular warning infrastructure. Device compromise crosses a different trust boundary from unauthorized network signaling. The distinction matters because network-level authentication cannot necessarily protect a device whose operating system or warning presentation software has been compromised.

5.4 Suppression adversaries

An adversary may seek to prevent legitimate warning delivery rather than generate a false warning. Suppression may involve interference with warning reception, manipulation of relevant signaling, or exploitation of device and network behavior. Alert suppression must also be separated from an ordinary network outage.

5.5 Scope of attacker assumptions

Security studies should explicitly identify the attacker capabilities required for a demonstrated exploit. Relevant assumptions include radio proximity, control of transmitting equipment, ability to influence cell selection, knowledge of network parameters, and access to compromised infrastructure. Without these details, comparisons between attacks may be misleading.

6 Spoofing Attacks in LTE Public Warning Systems

6.1 Nature of warning spoofing

Warning spoofing occurs when an unauthorized party causes a recipient to receive or display a warning that appears to originate from an authorized public warning mechanism. The central security problem is the acceptance of false warning information. Spoofing may undermine public trust even if the message does not cause immediate physical harm.

6.2 Experimental evidence

Lee et al. [1] investigated the spoofing of alerts in 4G LTE networks. Their research demonstrated practical weaknesses associated with the cellular warning-delivery environment. The significance of this work is that it moves beyond theoretical concerns and examines how unauthorized warning presentation can occur under experimental conditions. Still, the study's findings must be interpreted in relation to the tested devices, network conditions, and attack configuration. It does not establish that every LTE device or public warning deployment is equally vulnerable.

6.3 Trust in broadcast signaling

Cellular devices must process certain broadcast information before completing all network security procedures. An authenticated communication session does not necessarily make earlier or separately protected broadcast information trustworthy. A device's successful authentication to a cellular network does not by itself establish that every broadcast message it processes has been independently authenticated.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

6.4 Consequences of spoofing

A false emergency warning may direct recipients toward inappropriate protective actions, create confusion, or reduce confidence in future legitimate warnings. The severity of these consequences depends on message content, location, timing, and recipient behavior. The existence of a technical spoofing vulnerability does not independently establish that a particular real-world public safety consequence occurred.

6.5 Implications for defenses

Spoofing defenses must address the mechanism by which unauthorized information becomes accepted. Potential approaches include authenticated warning content, stronger signaling protection, and independent verification. Each approach has different assumptions and deployment requirements.

7 Spoofing and Suppression in 5G Warning Systems

7.1 Security evolution and residual exposure

5G introduces changes to cellular architecture and security procedures. At the same time, improvements in network security do not necessarily protect every form of broadcast signaling or emergency warning functionality. Security analysis must therefore consider the specific procedures involved in warning delivery.

7.2 Experimental research

Bitsikas and Pöpper [2] examined attacks affecting warning and emergency mechanisms in 5G. Their study presented two spoofing attacks and three suppression attacks. The distinction matters: warning security covers both false information and the loss of a genuine warning.

7.3 Spoofing versus suppression

Spoofing and suppression have different objectives. Spoofing attempts to introduce false information. Suppression attempts to prevent legitimate information from reaching the recipient. A defense that rejects forged warnings may not prevent suppression. Likewise, a mechanism that improves warning availability may not establish the authenticity of received content.

7.4 Implications for 5G security evaluation

The findings of Bitsikas and Pöpper [2] indicate that the security of public warning functions must be evaluated directly rather than inferred from the overall security improvements associated with a newer cellular generation. Even so, success in an experiment does not show that every 5G deployment is vulnerable in the same way. Relevant conditions include device implementations, network configurations, and attacker capabilities.

7.5 Availability as a first-class security requirement

Warning availability is especially important during emergencies. A system that prevents unauthorized alerts but fails to deliver legitimate warnings may still be unsuitable for its intended public safety purpose. For this reason, evaluations of warning authentication should also consider whether the proposed mechanisms preserve timely and reliable delivery.

8 Cellular System Information and Authentication

8.1 Role of system information

Cellular networks broadcast system information used by devices to identify and interact with cells. Some of this information is processed before a device has established a fully protected communication context. Broadcast system information therefore raises different security questions from authenticated user-plane traffic.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

8.2 System-information vulnerabilities

Ross et al. [12] examined the security of cellular system information broadcasts and proposed approaches for improving their protection. Their work is relevant because attackers may exploit weaknesses in broadcast signaling to influence device behavior. Yet system-information security and public warning security are not identical problems.

8.3 Distinguishing authentication layers

Three separate questions should be considered:

- Is the cellular signaling source authentic?
- Is the warning content authentic and unchanged?
- Is the warning being delivered within the intended geographic and operational context?

A mechanism addressing one question may not fully resolve the others. For example, authenticating system information may reduce certain false-cell or signaling-manipulation risks. It does not by itself establish end-to-end authenticity of a warning issued through a separate application or organizational process.

8.4 Deployment implications

Changes to cellular signaling authentication may require support from network infrastructure, standards, and device implementations. A theoretically effective defense may therefore face substantial deployment barriers. Compatibility with existing devices is particularly important for public warning services because emergency communications must reach a broad population.

8.5 Critical interpretation

The relevance of system-information authentication lies in its potential to strengthen a trust boundary that warning delivery may depend upon. It should not be presented as a complete solution to all warning spoofing and suppression attacks.

9 Cryptographic Authentication of Warning Messages

9.1 Purpose of message authentication

Cryptographic authentication can provide evidence that warning content originated from an authorized source and has not been modified. Potential mechanisms include digital signatures and related verification procedures. The suitability of a particular mechanism depends on how keys are managed, how authorized issuers are identified, and how recipient devices perform verification.

9.2 End-to-end authenticity

End-to-end warning authentication seeks to preserve verifiable provenance from an authorized warning originator to the receiving device. End-to-end authentication does not rely only on the trustworthiness of intermediate network infrastructure. Still, achieving end-to-end authentication requires a trust framework connecting authorized issuers and recipient devices.

9.3 Key management

A cryptographic mechanism is only as reliable as its key management and trust establishment. Relevant challenges include issuer authorization, key distribution, key renewal, revocation, and the handling of compromised credentials. Key management becomes harder when several government agencies, network operators, and device manufacturers share responsibility.

9.4 Compatibility and deployment

Introducing cryptographic verification may require changes to warning formats, infrastructure, or mobile device software. Existing deployments may not support the same verification capabilities. A

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

proposed defense must be evaluated against compatibility requirements and the need to reach older devices.

9.5 Failure handling

A critical design question concerns what a device should do when verification cannot be completed. Rejecting an unverifiable warning may reduce exposure to spoofing but could also prevent delivery of a legitimate warning during infrastructure failure. Displaying every unverifiable warning may preserve availability but weaken protection against false alerts. Designers must weigh this trade-off against both security and public safety needs.

9.6 Limitations

Cryptographic authentication does not inherently prevent radio interference, denial of service, or every form of alert suppression. It also does not guarantee that an authentic warning contains accurate or understandable instructions. As a result, cryptography is an important component of warning security but not a complete substitute for operational resilience and communication quality.

10 Cross-Cell and Independent Verification Approaches

10.1 Rationale

Cross-cell verification seeks to evaluate warning information using observations from more than one cellular source. The underlying idea is that information received from multiple cells may provide additional evidence concerning the legitimacy of a warning. At the same time, the effectiveness of this approach depends on the independence and trustworthiness of the observations.

10.2 Research proposals

Abou Hasna et al. [13] proposed an emergency alert spoofing testbed and a cross-cell verification approach. The proposal offers a way to give receiving devices another source of evidence. As a research preprint, its findings should be distinguished from mechanisms that have undergone extensive independent evaluation or operational deployment.

10.3 Assumptions concerning independence

Cross-cell verification may be less effective if an attacker can influence multiple observed cells or manipulate the information used for comparison. A device may also be located in an area where only limited cell observations are available. For that reason, the mere presence of multiple observations does not establish independent corroboration.

10.4 Legitimate warning differences

Warnings may legitimately differ between geographic areas. Adjacent cells may serve different warning regions or receive updates at different times. A verification mechanism must therefore distinguish suspicious inconsistency from legitimate differences in warning distribution.

10.5 Availability and latency

Verification using multiple cells may introduce additional processing or waiting requirements. Any added delay must be weighed against the urgency of the warning. A mechanism that improves confidence in warning authenticity but significantly delays legitimate warnings may create an undesirable operational consequence.

10.6 Evaluation requirements

Future studies should examine cross-cell verification under varying coverage conditions, attacker capabilities, mobility patterns, and device implementations. Its effectiveness should be assessed against both spoofing and suppression threats rather than only a single attack scenario.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

11 Cellular Authentication and Privacy-Preserving Security Research

Ferrag et al. [14] reviewed authentication and privacy-preserving mechanisms for 4G and 5G cellular networks. Their survey provides broader context for understanding cellular security architectures and authentication challenges. Yet general cellular authentication mechanisms cannot be assumed to authenticate public warning content automatically. Cellular authentication often concerns the establishment of trust between network entities and subscribers. Public warning delivery has different requirements because messages must reach large populations, potentially without individualized interaction. That difference is a basic design constraint. A mechanism appropriate for authenticating a subscriber session may not be directly suitable for broadcast emergency warnings. In the same way, privacy-preserving authentication research addresses important cellular security concerns but does not fully resolve warning spoofing or suppression.

The contribution of broader cellular authentication research is therefore conceptual and architectural. It helps identify trust assumptions and potential cryptographic approaches, but the applicability of those approaches to public warning systems must be demonstrated separately.

12 Standards and Their Security Implications

12.1 3GPP Public Warning System requirements

3GPP TS 22.268 [8] establishes requirements associated with cellular public warning services. The requirements describe how standardized warning systems are intended to behave. Still, functional requirements do not necessarily constitute a complete security evaluation.

12.2 Cell Broadcast Service

3GPP TS 23.041 [9] describes relevant cell broadcast procedures. The specification is important for understanding the technical mechanisms through which warning information is distributed. Security research must examine how these procedures interact with device behavior and network trust boundaries.

12.3 EU-ALERT

ETSI TS 102 900 [10] provides requirements associated with the European public warning system. It illustrates how cellular warning services are standardized for particular regional and regulatory contexts. At the same time, implementation and deployment practices may differ across countries and operators.

12.4 Common Alerting Protocol

CAP 1.2 [11] provides a standardized structure for representing alert information. Its use can support interoperability between warning originators and distribution systems. Yet the use of CAP does not, by itself, prove that the final warning received by a mobile device has been authenticated end to end.

12.5 Standards compliance versus demonstrated security

A deployment may conform to relevant functional specifications while retaining vulnerabilities associated with particular implementation choices or unprotected signaling. Security assessments should therefore distinguish standards compliance, implementation correctness, and resistance to demonstrated attack techniques. Compliance, correct implementation, and resistance to attack are related but separate properties.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

13 Public Trust, Warning Interpretation, and Message Design

13.1 Technical authenticity and public interpretation

An authentic warning must still be understood by its recipients. Conversely, a spoofed warning may be persuasive if it appears in a familiar emergency alert interface. Technical security and public communication therefore cannot be assessed in isolation.

13.2 Research on mobile warning messages

Bean et al. [3] reviewed research concerning mobile public warning messages and identified important issues for further investigation. Their work provides a foundation for understanding warning effectiveness beyond the technical delivery mechanism.

13.3 Trust in wireless emergency alerts

Bean and Grevstad [4] examined public understanding, trust, and preferences following a nationwide wireless emergency alert test in the United States. Such research is relevant because public response depends partly on how recipients interpret the authority and purpose of alerts. Still, survey findings about trust do not independently establish the technical security of the underlying warning mechanism. Morrow, Stoddard, and Elm [15] used Bayesian belief-network simulations to examine factors affecting public and alert-originator trust in Wireless Emergency Alerts. Their model treats security and system reliability as contributors to trust, but the simulated relationships do not measure attack resistance in deployed cellular networks.

13.4 Message completeness

Olson et al. [5] examined wireless emergency alert message content and completeness over time. Their findings contribute to understanding whether warning messages contain the information recipients need to interpret a threat and determine an appropriate response. Message completeness and technical authenticity are distinct requirements. An authentic but incomplete warning may fail to support effective action.

13.5 Message length and communication effectiveness

Carlson et al. [6] investigated the effectiveness of different wireless emergency alert message lengths. The study links warning design to recipient understanding. At the same time, increasing message length does not automatically improve security against unauthorized transmission.

13.6 Warning interpretation under unfamiliar hazards

Bean et al. [7] examined how audiences interpret mobile alerts concerning unfamiliar hazards. People may need to act quickly even when the hazard is unfamiliar. Clear instructions and credible presentation can influence warning effectiveness.

13.7 Implications for spoofing

The consequences of spoofing may depend on the credibility of the message and the recipient's interpretation. Yet communication studies should not be used to infer technical attack success rates. They provide evidence about the human dimensions of warning systems rather than direct measurements of cellular security vulnerabilities.

14 A Seven-Dimensional Threat-to-Control Framework

14.1 Framework rationale

The literature describes several attack surfaces and several kinds of defense. A single classification based on whether an attack involves spoofing or suppression is insufficient to capture the differences between threats. The proposed framework therefore identifies seven dimensions.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

14.2 Dimension 1: Adversarial capability

Adversarial capability records what the attacker can control. Examples include local radio transmission, compromised infrastructure, or device-level software. Explicitly identifying adversarial capability helps distinguish experimentally demonstrated threats from hypothetical scenarios.

14.3 Dimension 2: Entry point

Entry point identifies the component or interface through which the attack begins. Relevant entry points may include warning origination systems, cellular signaling, network infrastructure, or recipient devices.

14.4 Dimension 3: Attack mechanism

Attack mechanism describes how the attack works. Examples include unauthorized warning injection, signaling manipulation, false-cell behavior, and suppression of legitimate warning reception. The mechanism should be described at a level supported by the underlying research.

14.5 Dimension 4: Affected security property

Affected security property records whether the attack harms authenticity, integrity, availability, timeliness, or geographic correctness. A single attack may affect more than one property. Still, the consequences should be established rather than assumed.

14.6 Dimension 5: Verification mechanism

Verification mechanism identifies the proposed or deployed defense. Examples include cryptographic warning authentication, stronger signaling protection, and independent verification using multiple observations. The assessment should identify precisely what the mechanism verifies.

14.7 Dimension 6: Deployment dependency

Deployment dependency lists the infrastructure, software, standards, and organizational changes needed for the defense. A defense requiring widespread device updates has different deployment implications from a measure implemented entirely within existing warning infrastructure.

14.8 Dimension 7: Residual risk

Residual risk records the threats that remain after the defense is applied. For example, warning-content authentication may reduce unauthorized message acceptance without preventing radio-level suppression. Residual risk is essential for avoiding claims that a defense provides comprehensive protection when it addresses only a particular attack mechanism.

14.9 Framework summary

Dimension	Assessment question	Illustrative considerations
Adversarial capability	What can the attacker control?	Radio equipment, infrastructure, device software
Entry point	Where is the attack introduced?	Broadcast signaling, alert distribution, recipient device
Attack mechanism	How does the attack operate?	Spoofing, suppression, signaling manipulation
Affected security property	What is compromised?	Authenticity, integrity, availability, timeliness
Verification mechanism	What does the defense verify?	Message provenance, signaling authenticity, cross-cell consistency
Deployment dependency	What changes are required?	Device updates, network changes, key infrastructure

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Dimension	Assessment question	Illustrative considerations
Residual risk	What threats remain?	Denial of service, compromised issuers, verification failure

14.10 Interpretation

The framework is intended for structured comparison rather than numerical ranking. The literature does not provide validated weights for combining these dimensions into a single security score. Its principal purpose is to make the assumptions, coverage, and limitations of proposed controls explicit.

15 Illustrative Application of the Framework

15.1 Scenario

Consider a hypothetical attacker attempting to cause mobile devices in a limited area to display an unauthorized emergency warning. The attacker is assumed to possess local radio transmission capabilities but not control over the legitimate warning authority. The scenario is illustrative; it is not a new experiment.

15.2 Adversarial capability and entry point

The relevant adversarial capability is local radio transmission. The entry point is the cellular signaling environment interpreted by recipient devices.

15.3 Attack mechanism

The attack attempts to induce acceptance of unauthorized warning information. Its feasibility depends on the signaling procedures, device behavior, and environmental conditions involved.

15.4 Affected security property

The principal affected property is authenticity. Depending on the implementation, the attack may also affect geographic correctness or public trust.

15.5 Candidate controls

Potential defenses include warning-content authentication, protection of relevant cellular signaling, and cross-cell verification. Each defense addresses a different part of the trust problem.

15.6 Deployment dependencies

Warning-content authentication may require trusted issuer keys and compatible recipient software. Signaling authentication may require changes to network and device implementations. Cross-cell verification may depend on the availability of sufficiently independent observations.

15.7 Residual risks

Even if unauthorized warning acceptance is prevented, an adversary may attempt to disrupt legitimate warning reception. A comprehensive assessment must therefore consider availability as well as authenticity.

15.8 Framework contribution

The scenario demonstrates how the proposed framework can distinguish the assumptions and coverage of different defenses. It also illustrates why a defense against one attack mechanism is not a universal solution.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

16 Comparative Assessment of Proposed Defenses

16.1 Cryptographic warning authentication

Cryptographic warning authentication can strengthen confidence in message provenance and integrity. Its limitations include key management, compatibility, verification failure handling, and the inability to prevent all forms of suppression.

16.2 Signaling authentication

Stronger authentication of relevant cellular signaling may reduce opportunities for certain false-cell and signaling-manipulation attacks. At the same time, its applicability depends on the specific signaling procedures protected. It does not establish the authorization of the warning originator.

16.3 Cross-cell verification

Cross-cell verification may provide additional information for detecting suspicious warning delivery. Its limitations include coverage conditions, correlated observations, legitimate geographic differences, and possible verification delays.

16.4 Operational monitoring

Network and warning-system monitoring may help detect abnormal behavior. Yet monitoring is not equivalent to preventing a device from accepting an unauthorized warning. Its effectiveness depends on visibility, detection logic, and response capability.

16.5 Communication improvements

Clearer warning messages can improve interpretation and protective action. Still, message design does not prevent radio-level spoofing or suppression. Communication quality should therefore complement technical security rather than replace it.

16.6 Comparative summary

Defense approach	Principal security contribution	Main dependency	Important residual risk
Warning-content authentication	Message provenance and integrity	Trusted keys and compatible verification	Suppression and denial of service
Cellular signaling authentication	Stronger trust in relevant broadcast signaling	Network and device support	Compromised warning originator
Cross-cell verification	Additional consistency evidence	Multiple sufficiently independent observations	Coordinated manipulation and limited coverage
Operational monitoring	Detection of suspicious behavior	Network visibility and response processes	Undetected or rapidly executed attacks
Improved warning design	Better public comprehension	Message policy and presentation	Technical spoofing and suppression

The comparison illustrates why a layered approach may be appropriate. At the same time, layering defenses does not guarantee comprehensive protection unless their combined behavior has been evaluated under realistic conditions.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

17 Implications for Public Warning Security

17.1 Separating authenticity from availability

Public warning security programs should assess authenticity and availability separately. Preventing false warnings does not establish that legitimate warnings will be delivered. Likewise, maintaining delivery capacity does not establish that received warnings are authentic.

17.2 Evaluating end-to-end trust

Security assessments should examine the complete path from warning authorization to device presentation. The path includes warning origination, distribution infrastructure, cellular signaling, and recipient behavior. The assessment should identify where trust is established and where it is assumed.

17.3 Testing under realistic conditions

Research prototypes should be evaluated under conditions reflecting actual deployment constraints. Relevant factors include device diversity, mobility, limited radio coverage, network congestion, and emergency operating conditions.

17.4 Compatibility requirements

Public warning systems must reach a broad population. Security enhancements should therefore consider the consequences for devices that cannot support newly introduced verification mechanisms. Compatibility is a public safety consideration, not merely an engineering convenience.

17.5 Coordinating technical and communication controls

Technical authentication can help establish whether a warning is legitimate. Communication design helps recipients understand what action is required. Both functions are necessary for effective warning delivery, but they address different problems.

17.6 Incident response and public confidence

Operators and warning authorities should prepare procedures for responding to suspected false warnings or warning-delivery failures. Such procedures may include verification of warning issuance, coordination with network operators, and appropriate public clarification. Yet the effectiveness of these procedures should be tested rather than assumed.

18 Research Gaps and Future Directions

18.1 Independent replication of attacks

Further research should replicate demonstrated spoofing and suppression attacks across different devices, software versions, and deployment conditions. Replication would show where the reported vulnerabilities do and do not apply.

18.2 Authentication deployment studies

Research should evaluate the practical feasibility of cryptographic warning authentication, including key distribution, revocation, compatibility, and verification failure handling.

18.3 Cross-cell verification evaluation

Cross-cell verification requires further examination under realistic mobility and coverage conditions. Studies should also investigate how legitimate differences between warning regions affect verification outcomes.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

18.4 Availability-preserving security

Future work should evaluate how authentication mechanisms behave when networks are congested, partially unavailable, or subject to interference. A security mechanism should not be assessed solely by its ability to reject false warnings.

18.5 Human response to spoofed warnings

Further interdisciplinary research could examine how recipients interpret technically convincing false alerts and how clarification messages affect public trust. Such studies should distinguish experimental communication outcomes from real-world attack incidence.

18.6 Comparative security frameworks

The proposed seven-dimensional framework requires validation through application to a wider range of attack and defense studies. Future research should examine whether it improves the consistency and transparency of security comparisons.

19 Discussion

Cellular public warning systems occupy a distinctive position within telecommunications security. They must deliver urgent information to large populations, often without individualized interaction between the warning originator and each recipient. Broadcasting to a large population creates problems that differ from those of conventional authenticated communication. The research reviewed in this article demonstrates that cellular warning mechanisms can be exposed to spoofing and suppression threats. Lee et al. [1] provide experimental evidence concerning unauthorized warning presentation in LTE. Bitsikas and Pöpper [2] demonstrate that warning-related vulnerabilities remain relevant in 5G environments and that both spoofing and suppression require attention. The findings show that stronger cellular security does not automatically secure every warning procedure.

Research on cellular system-information authentication [12] contributes to understanding the trust boundaries associated with broadcast signaling. Still, authentication of system information and authentication of warning content address different security questions. Likewise, cross-cell verification [13] offers a potential additional means of evaluating warning legitimacy, but its effectiveness depends on assumptions concerning observation independence, coverage, and attacker capabilities. The broader cellular authentication literature [14] provides useful architectural context without establishing a complete solution to public warning security. A central conclusion of this review is that authentication mechanisms must be evaluated according to the specific security property they protect. A mechanism may improve authenticity while leaving availability vulnerable.

Another may strengthen signaling trust without proving that the warning was issued by an authorized public authority. The operational consequences of these distinctions are significant. A false warning can undermine public confidence and prompt inappropriate action. A suppressed warning can prevent recipients from receiving necessary instructions. Both threats affect the public safety objective of the warning system, but they require different defensive considerations. The communication literature adds a further dimension. Studies of public warning messages [3–7] demonstrate the importance of message content, trust, and interpretation. Message content and public trust do not fix technical flaws, but they shape how people respond.

The proposed seven-dimensional framework integrates these considerations by requiring explicit identification of adversarial capability, entry point, attack mechanism, affected security property, verification mechanism, deployment dependency, and residual risk. Its contribution is to support more precise comparisons between security threats and proposed defenses. The framework also discourages overly broad claims about the effectiveness of individual controls. Still, the framework remains conceptual. Its usefulness must be evaluated through application to additional research and operational scenarios.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

20 Limitations

Several limitations should be noted. First, it adopts a critical narrative approach rather than a systematic review methodology. Second, experimental security studies may involve specific devices, network configurations, and attacker capabilities that limit generalizability. Third, cellular public warning implementations differ between jurisdictions and network operators. Fourth, some proposed defenses remain at the research or prototype stage. Fifth, the review includes a research preprint that is not equivalent to independently validated, peer-reviewed evidence. Sixth, standards documents establish requirements and procedures but do not independently demonstrate the security of every implementation. Seventh, studies of public warning communication address recipient understanding and trust rather than directly measuring technical attack resistance.

Finally, the proposed framework has not been empirically validated as a standardized assessment instrument.

21 Conclusion

Cellular public warning systems are essential to emergency communication, but their security cannot be evaluated solely through the presence of standardized warning-delivery mechanisms or general cellular authentication procedures. Experimental research has demonstrated that warning spoofing and suppression are relevant threats in LTE and 5G environments. Spoofing and suppression affect different security properties and need different defenses. Cryptographic warning authentication, stronger protection of cellular signaling, and cross-cell verification offer potentially complementary approaches. At the same time, each mechanism has limitations concerning deployment, compatibility, trust assumptions, or residual risk. The review proposes a seven-dimensional threat-to-control framework to support structured comparison of attacks and defenses.

The framework emphasizes adversarial capability, entry point, attack mechanism, affected security property, verification mechanism, deployment dependency, and residual risk. Future research should prioritize independent replication, realistic deployment evaluation, availability-preserving authentication, and the integration of technical security with effective public warning communication. The security of cellular public warning systems ultimately depends on ensuring that legitimate warnings are authentic, timely, available, and understandable to the people who need them.

REFERENCES

[1] Lee, G., Lee, J. H., Lee, J., Im, Y., Hollingsworth, M., Wustrow, E., Grunwald, D., & Ha, S. (2019). This is your president speaking: Spoofing alerts in 4G LTE networks. Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2019), 404–416. https://doi.org/10.1145/3307334.3326082

[2] Bitsikas, E., & Pöpper, C. (2022). You have been warned: Abusing 5G's warning and emergency systems. Proceedings of the Annual Computer Security Applications Conference (ACSAC 2022), 561–575. https://doi.org/10.1145/3564625.3568000

[3] Bean, H., Sutton, J., Liu, B. F., Madden, S., Wood, M. M., & Mileti, D. S. (2015). The study of mobile public warning messages: A research review and agenda. Review of Communication, 15(1), 60–80. https://doi.org/10.1080/15358593.2015.1014402

[4] Bean, H., & Grevstad, N. (2023). Wireless emergency alerts: Public understanding, trust, and preferences following the 2021 US nationwide test. Journal of Contingencies and Crisis Management, 31(2), 273–288. https://doi.org/10.1111/1468-5973.12438

[5] Olson, M. K., Sutton, J., Cain, L. B., & Waugh, N. (2024). A decade of wireless emergency alerts: A longitudinal assessment of message content and completeness. Journal of Contingencies and Crisis Management, 32(1), e12518. https://doi.org/10.1111/1468-5973.12518

[6] Carlson, E. J., Bean, H., Ratcliff, C., Pokharel, M., & Barbour, J. (2024). Do 360-character Wireless Emergency Alert messages work better than 90-character messages? Testing the risk communication consensus. Journal of Contingencies and Crisis Management, 32(2), e12587. https://doi.org/10.1111/1468-5973.12587

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

[7] Bean, H., Liu, B. F., Madden, S., Sutton, J., Wood, M. M., & Mileti, D. S. (2016). Disaster warnings in your pocket: How audiences interpret mobile alerts for an unfamiliar hazard. Journal of Contingencies and Crisis Management, 24(3), 136–147. https://doi.org/10.1111/1468-5973.12108

[8] 3rd Generation Partnership Project. (n.d.). Public Warning System (PWS) requirements (3GPP TS 22.268). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=639

[9] 3rd Generation Partnership Project. (n.d.). Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=748

[10] European Telecommunications Standards Institute. (2019). Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service (ETSI TS 102 900 V1.3.1). https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf

[11] OASIS. (2010). Common Alerting Protocol Version 1.2. OASIS Standard. https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf

[12] Ross, A. J., Reaves, B., Nasser, Y., Cukierman, G., & Piqueras Jover, R. (2024). Fixing insecure cellular system information broadcasts for good. Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024), 693–708. https://doi.org/10.1145/3678890.3678924

[13] Abou Hasna, A., Chendeb, N., & El Falou, A. (2026). From spoofing to trust: Emergency alerts spoofing testbed and cross-cell verification. arXiv preprint, arXiv:2604.24404. https://doi.org/10.48550/arXiv.2604.24404

[14] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101, 55–82. https://doi.org/10.1016/j.jnca.2017.10.017

[15] Morrow, T., Stoddard, R. W., & Elm, J. P. (2014). Wireless Emergency Alerts: Trust Model Simulations. Carnegie Mellon University Software Engineering Institute, CMU/SEI-2013-SR-026. https://insights.sei.cmu.edu/library/wireless-emergency-alerts-trust-model-simulations/

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)