DEA: A Trusted Decentralized Emergency Alert Protocol

Brian O'Neill
broneill@pdx.edu
Portland State University
Portland, Oregon, USA

Nirupama Bulusu
nbulusu@pdx.edu
Portland State University
Portland, Oregon, USA

ABSTRACT

Wildfires and other emergencies disrupt critical communication infrastructure when needed most. In this paper, we propose a decentralized alternative to the current Wireless Emergency Alerts protocol, that allows for alert notifications to be broadcast even when traditional infrastructure is disrupted, enabling greater reach.

CCS CONCEPTS

• **Networks** → **Network protocol design**.

KEYWORDS

Ad Hoc Networks, Emergency Notifications

ACM Reference Format:
Brian O'Neill and Nirupama Bulusu. 2021. DEA: A Trusted Decentralized Emergency Alert Protocol. In *Students in MobiSys (SMS '21), June 24, 2021, Virtual, WI, USA*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3469262.3472388

1 INTRODUCTION

In September of 2020, the Beachie Creek Fire [7] in Oregon met high temperatures, low humidity and 50-75 mile per hour winds, which caused the fire to grow from an estimated 500 acres to over 130,000 acres in one night. By the time that the evacuation notice was issued to several towns in the area, the fire had already caused power and wireless network outages. This resulted in many residents never receiving the potentially lifesaving notification [8]. To address this issue, we are designing a decentralized emergency alert system that can allow for emergency evacuation orders and other lifesaving information to be disseminated when traditional network infrastructure is not available. We plan to examine the efficacy of augmenting the current Wireless Emergency Alert (WEA) program for use in wildfire disasters. Our augmented WEA is called Decentralized Emergency Alerts (DEA).

1.1 Current State of Wireless Emergency Alerts

Current WEAs are issued over LTE networks to commercial off the shelf smartphones. A strength of this system is that it is an opt-out system with wide adoption. But, it has the following limitations.

Active LTE connection. WEA messages are sent over carrier LTE network connections [3]. Emergency situations (e.g. wildfires) typically include disruptions in the electrical infrastructure that can disrupt these connections.

Spoofing vulnerability. With no current process for verifying message authenticity, WEA alerts could be subject to spoofing attacks that allow an adversary to impersonate a carrier LTE tower and transmit potentially malicious emergency alerts to victims [3].

No confirmation of message receipt. WEA messages are broadcast notifications that do not collect any indication of whether it was received. This is sub optimal because during an evacuation first responders need to prioritize helping those who did not get the message or have not already evacuated [8].

Limited information. Interviews with alert originators highlighted areas for improvement, one important suggestion was that WEA messages should provide more information than just an alarm. They suggested it should provide additional information such as maps and links to improve the preparedness of the recipients [2].

1.2 Design Goals

To address the above limitations, an ideal emergency alert system must satisfy the following design goals, ordered by priority.

1. Offline Capable. The primary goal for an ideal emergency notification system is to provide offline notifications, given disrupted electrical and network infrastructure during disasters.

2. Trusted. The solution must provide a method to ensure the authenticity of received notifications. This would provide protection against malicious messages sent over the adhoc networks.

3. Energy Efficient. Since the solution is being designed to run in environments where electrical infrastructure may be disrupted, it must attempt to limit the amount of energy being consumed, to minimize the impact on subscriber devices.

4. Quantifiable Reach. The solution must provide a way to receive acknowledgements that messages were received no matter how they were received (e.g. ad hoc networks). The purpose of this is to provide insight for emergency response teams.

2 RELATED WORK

There are several proposed solutions for sending alerts in disaster scenarios where internet connectivity is limited such as Help Me [5], which uses a mechanism for sending and receiving messages over a multi-hop ad-hoc network. Therefore they require a network of nearby devices to route messages. This type of network may not be available in a wildfire scenario where people are actively evacuating the area. One method to address the lack of available nodes on a network is a Disruption Tolerant Network [6] which relies on a store-and-forward mechanism to route messages as network nodes become available. However, such a network does not meet many of

SMS '21, June 24, 2021, Virtual, WI, USA

ACM ISBN 978-1-4503-8602-9/21/06…$15.00
https://doi.org/10.1145/3469262.3472388

the requirements of emergency notification systems. Our proposed work bridges this gap.

3 DEA DESIGN AND EVALUATION

3.1 Design Choices

With the stated design goals in mind, we designed a decentralized emergency alert system (DEA), with many of the following trade offs inherent in design choices we made to meet these goals.

Offline Capable vs. Trusted. To prove that the messages can be trusted, we rely on public key infrastructure with digital signatures embedded in the alerts. This limits the offline capabilities by requiring an online subscription process to allow for a key exchange to take place. This also means that an online connection is required to replace public keys over time. We believe this trade off is appropriate because key exchange can be established a priori.

Offline Capable vs. Energy Efficient. To provide energy efficiency with offline capabilities, we want to reduce the amount and size of broadcast messages. We plan to rely on a trickle-based [4] algorithm to limit broadcasts when there are nearby nodes and only broadcast the whole message when it is needed. The trickle-based algorithm is described in more detail in Section 3.2.

Quantifiable Reach vs. Energy Efficient. We rely on a store and forward approach to handle acknowledgements indicating an alert was received. To prioritize energy efficiency, messages are only forwarded when a connection to a trusted rebroadcaster exists.

3.2 DEA Protocol

Entities. DEA has several entities to represent different types of users of DEA, depicted in Figure 1.

(1) Notifier: A server operated by the message originator, operated by the local office of emergency management.
(2) Subscriber: A smart phone device operated by a community member in the area affected by the emergency event which triggered the notification. Subscribers also act as nodes to pass notifications to other subscribers within range.
(3) Re-Broadcaster: A trusted device (e.g. sheriff's department, local hospital) that can broadcast additional messages during an emergency notification event.

DEA comprises the following steps, interacting in the sequence demonstrated in Figure 2.

1. Initialization. Subscriber devices are initialized with an ad hoc wireless network and an active internet network connection. This step is the equivalent of a subscriber downloading a required app on their smartphone for the first time.

2. Subscription. This is an opt-in step that is completed by a subscriber device while the device has an active internet connection. During this step the device registers with the notifier to receive notifications and downloads a public key to verify messages originating from notifier. At this time the notifier will also create a unique identifier for identifying the subscriber and provide the identifier to the subscriber.

3. Network disruption. During the following steps, some network disruption has occurred resulting in a subset of subscriber devices being disconnected from the internet connection but without the subscriber's ad hoc wireless capabilities being impacted.

4. Emergency Notification. An emergency notification is broadcast from the notifier to registered subscribers. Subscribers who receive this notification will also act as nodes in the ad hoc wireless network to pass the notification to nearby devices on the ad hoc network. These notifications are broadcast using a trickle based algorithm to notify nearby subscribers that an alert is available and will only broadcast the alert when requested. Trickle [4] is an algorithm applied in sensor networks to minimize the communication required to update sensors in the network. In DEA, this methodology is applied by broadcasting the most current message id. When an older message id or 0 is broadcast, that indicates that the latest message should be broadcast.

5. Re-Broadcast. During this step trusted Re-Broadcasters in the emergency area can forward the notifier notification as well as new notifications, enabling the notification to reach more subscribers as well as update information provided to already notified subscribers.

6. Acknowledgement. After receiving the emergency notification, subscribers return an acknowledgement, which includes their unique subscriber identification as well as location information, so that the receipt of the notification can be tracked and updated information about the subscriber can be provided to the notifier. When the acknowledgment is passed over the ad-hoc network, it is stored until it can be sent to a trusted re-broadcaster.

7. End of Event. The initial emergency notification will have an associated end date/time associated. Once that date has passed DEA ignores all messages related to that notification regardless of the source and subscribers no longer act as nodes in the ad hoc network.

3.3 Simulation

What makes this research unique is that it must simultaneously address multiple conflicting goals of being offline capable, trusted and energy efficient while also attempting to quantify the reach of the alerts. Research is required to optimize DEA to meet these goals while examining the impact of their trade-offs. Additionally, novel solutions are required to bring trusted communication over untrusted intermediary nodes. To analyze these trade-offs and the efficacy of DEA, as a first step, we plan to implement DEA in a ns-3 simulation [1]. Assuming that all devices in the simulation are opted-in to DEA, we can examine how adjustments to DEA, such as different interval lengths affect the following outcomes:

(1) percentage of devices that receive the notification over time
(2) percentage of devices that lose power during the emergency event over time
(3) number of devices that have reported back to an official source indicating that the message was received over time

Subscribers are randomly distributed over a geographical area when initialized in the simulation. The periodicity of ad hoc device broadcasts will be a parameter, with the optimum value determined heuristically during different simulation trials. Upon receiving the notification, subscribers will begin to move to a designated evacuation area in the simulation to simulate subscribers evacuating from a wildfire emergency. We will also compare these results in simulation against the alternative solutions of WEA, a multi-hop ad hoc network-based protocol and a store-and-forward-based protocol.

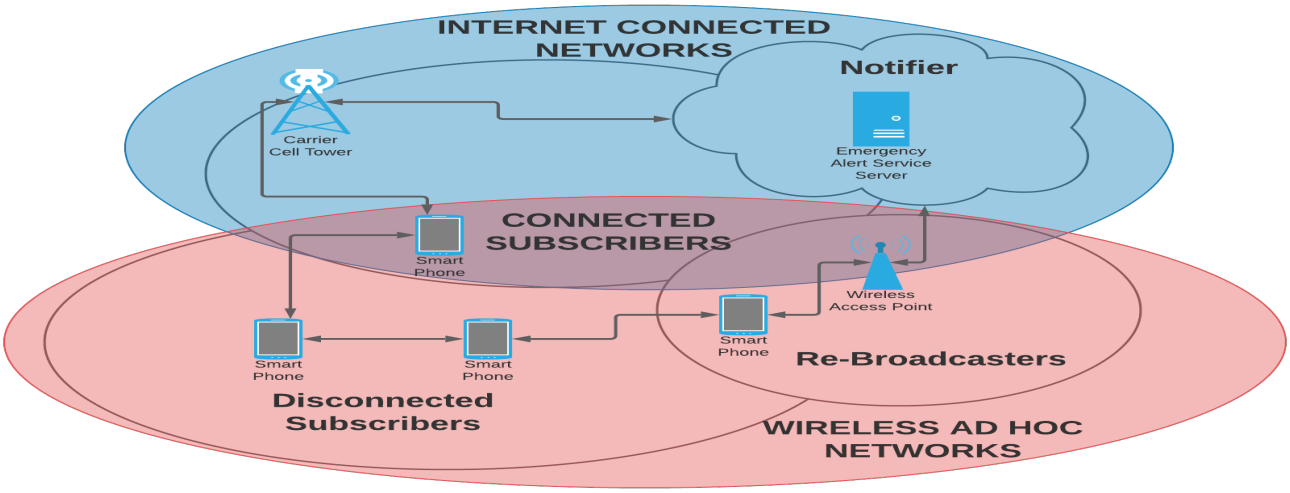

Figure 1: Overview of protocol entities

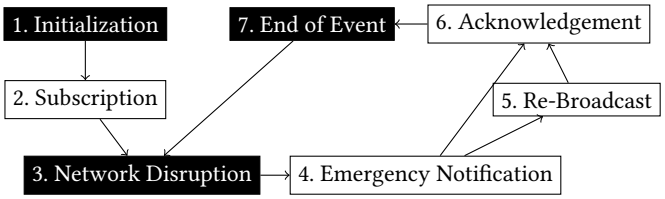

Figure 2: Overview of protocol steps. A black background indicates steps external to the protocol.

4 DISCUSSION

Besides benefits over WEA, DEA also introduces new challenges.

4.1 Security Threats

Relying on mobile ad hoc networks introduces additional security threats not prevalent with WEA. This includes being subject to replay attacks as communication travels through potentially malicious nodes in the network. In a replay attack, a legitimate message from a previous event can be broadcasted after that event has ended. By including an end date in the message, DEA ensures that the message cannot be replayed after the event has ended. This date will be encoded in the signature, meaning that malicious actors would invalidate the signature if this date was adjusted.

4.2 User Adoption

An opt-in step is required, which may mean that subscribers need to download an application or complete some other step to utilize DEA. This may result in fewer subscribers than there would be following the current opt-out model. Some incentives would be needed to encourage adoption of this updated system.

4.3 Rural Communities

Rural communities are some of the hardest hit in wildfires and the distance between neighbors is so great that they cannot be reached using mobile device based ad hoc wireless networks. This could be addressed using the DEA protocol with a drone.

5 CONCLUSION

Our conjecture is that DEA can potentially outperform WEA over LTE carrier networks, WEA over a multi-hop ad hoc wireless network and WEA over a disruption tolerant network. We intend to report on results from ns-3 comparative evaluation, and study our protocol on wireless testbeds, in future work.

REFERENCES

[1] Thomas R Henderson, Mathieu Lacage, George F Riley, Craig Dowell, and Joseph Kopena. 2008. Network simulations with the ns-3 simulator. *SIGCOMM demonstration* 14, 14 (2008), 527.

[2] Sumeet Kumar, Hakan Erdogmus, Bob Iannucci, Martin Griss, and João Diogo Falcão. 2018. Rethinking the Future of Wireless Emergency Alerts: A Comprehensive Study of Technical and Conceptual Improvements. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 71 (July 2018), 33 pages. https://doi.org/10.1145/3214274

[3] Gyuhong Lee, Jihoon Lee, Jinsung Lee, Youngbin Im, Max Hollingsworth, Eric Wustrow, Dirk Grunwald, and Sangtae Ha. 2019. This is Your President Speaking.. In *Proceedings of the 17th Annual International Conference on Mobile Systems*, Vol. Applications, and Services,. ACM, 404–416.

[4] Philip Levis, Neil Patel, David Culler, and Scott Shenker. 2004. Trickle: A Self-Regulating Algorithm for Code Propagation and Maintenance in Wireless Sensor Networks. In *First Symposium on Networked Systems Design and Implementation (NSDI 04)*. USENIX Association, San Francisco, CA. https://www.usenix.org/conference/nsdi-04/trickle-self-regulating-algorithm-code-propagation-and-maintenance-wireless

[5] Osnat Mokryn, Dror Karmi, Akiva Elkayam, and Tomer Teller. 2012. Help Me: Opportunistic smart rescue application and system. In *2012 The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*. 98–105. https://doi.org/10.1109/MedHocNet.2012.6257129

[6] Christian Raffelsberger and Hermann Hellwagner. 2013. A hybrid MANET-DTN routing scheme for emergency response scenarios. In *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. 505–510. https://doi.org/10.1109/PerComW.2013.6529549

[7] U.S. Forest Service. 2020. Beachie Creek Fire. On the WWW. URL https://inciweb.nwcg.gov/incident/7001/.

[8] Whiteney Woodworth. 2020. 'Completely botched': Failed emergency alerts raise questions for future disasters. *Salem Statesman Journal* (28 September 2020).