A Peer-to-Peer Communication Method for Distributed Earthquake Early Warning Networks: Preliminary Findings

Benjamin Hong
Victoria University of Wellington
b.hong@massey.ac.nz

Chanthujan Chandrakumar
Massey University
c.chandrakumar2@massey.ac.nz

Danuka Ravishan
Synopsys, Sri Lanka
danukaravishan1@gmail.com

Raj Prasanna
Massey University
r.prasanna@massey.ac.nz

ABSTRACT

This work-in-progress paper presents preliminary findings of ongoing research into alternative peer-to-peer (P2P) communication methods for earthquake early warning (EEW) systems. It expands upon previous work (Prasanna et al., 2022) that explores a network architecture for a decentralised EEW system. This paper explores using Quick UDP Internet Connections (QUIC) over a hole-punched UDP tunnel as a potential alternative to a Software-Defined Wide Area Network (SD-WAN) for peer-to-peer networking in an experimental EEW network architecture. The performance of QUIC is tested and compared to TCP over ZeroTier, an SD-WAN chosen as a P2P communication method in the previous work, over a realistic network topology. The results show that QUIC can outperform TCP over ZeroTier. Future work is needed to produce a method suitable for actual use in an EEW system. This paper contributes to the EEW literature by introducing a new method of communication tailored for EEW.

Keywords

Earthquake Early Warning, QUIC, Peer-to-peer, Decentralised

BACKGROUND

Earthquake early warning (EEW) systems are designed to rapidly disseminate warnings of impending earthquakes to allow people and infrastructure to take protective measures (Strauss & Allen, 2016). Traditional centralised EEW systems typically consist of a network of sensors that detect the first signs of an earthquake, called the primary wave, and a series of computer algorithms that use the sensor data to estimate the location, magnitude, and arrival time of the main shock wave (Yih-Min, Kanamori, Allen, & Hauksson, 2007). The warnings are then disseminated to the public through various channels, such as sirens, smartphones, and radio broadcasts.

The effectiveness of EEW systems depends on the timely delivery of warnings to the people and infrastructure that are at risk (Grasso, Beck, & Manfredi, 2007). EEW systems must have a robust and reliable communication network to achieve this. The traditional communication paradigm for EEW systems is a client-server architecture, in which sensors send data to a central server, and the server then disseminates warnings to the public (Böse et al., 2014; Brooks et al., 2021). However, this paradigm can create significant bottlenecks and limitations (Prasanna et al., 2022).

This paper presents preliminary findings of research into an alternative peer-to-peer (P2P) communication method for earthquake early warning (EEW) systems. P2P communication has several advantages over traditional

communication paradigms, such as being more resilient to infrastructure damage because there is no single point of failure and better performance because the connection is more direct without a server in the middle (Fleming et al., 2009). However, P2P communication also has challenges, such as the need for a reliable discovery mechanism and some networks preventing connections from being established (Ford, Srisuresh, & Kegel, 2005). This paper expands upon previous work exploring an experimental Earthquake Early Warning network architecture (Prasanna et al., 2022) that uses a distributed peer-to-peer sensor network for EEW.

In the previous work (Prasanna et al., 2022), a decentralised EEW network architecture consisting of Internet of Things (IoT) seismometers hosted by the public was proposed as an alternative to the traditional centralised EEW networks. It is designed to be resilient during disasters due to its decentralised nature and be highly scalable while maintaining high-performance capabilities. In this architecture, an extensive network of sensors communicates using a Software Defined Wide Area Network (SD-WAN), ZeroTier. It uses a two-station trigger concept to decrease false positives and increase accuracy. Each sensor connects to others within a 30km radius. When a sensor detects sufficient ground motion, it will notify the connected sensors, and if the other sensor also detects sufficient ground motion, an alert will be issued.

Using the ZeroTier P2P-VPN raised some concerns. ZeroTier is a commercial solution, and, as such, it has associated fees. It also, by default, allows network members unfiltered communication with each other, which can lead to security concerns, although this can be mitigated using flow rules (ZeroTier). Because individual members of the general public host sensors, it is not impossible for someone to attempt to gain control of individual sensors and launch attacks across the network. Further, complications could arise during deployment when organisations are hesitant to allow another VPN into their internal networks. Therefore, as one of the ongoing research activities on a community-engaged low-cost EEW network, this work-in-progress paper investigates an open-access and free-to-use method for peer-to-peer communications as a potential alternative to a Software Defined Wide Area Network (SD-WAN).

METHOD

Peer-to-peer communication without needing to pass through a centralised server is ideal for the resiliency and performance advantages mentioned in the background. Hole punching is an established simple and effective method for establishing peer-to-peer communication between computers on the internet. Peers connect to a public server, exchange their public IP addresses and ports, and connect peer-to-peer with this information. Previous research found that 82% of networks support UDP hole punching, while 64% support TCP (Ford et al., 2005). In order to maximise direct peer-to-peer communication, the explored method uses UDP hole punching. There is, however, a risk of losing packets that come with UDP and a lack of encryption and security.

Missed alerts due to lost packets mean the EEW will not protect some people, so retransmission of lost packets is essential. Sending out false alarms can impact the credibility of the issuing organisation and reduce the effectiveness of future alarms, so it is essential to lower the risk of false alarms (Grasso et al., 2007; Simmons & Sutter, 2009). Therefore, the possibility of malicious actors impersonating sensors and sending out false notifications of ground motion should be minimised by authenticating them. In this particular scenario, only the sensor sending the notification needs to be authenticated, so security can be improved by using existing client-server technologies such as HTTP, where the server authenticates using Public Key Infrastructure (PKI).

Looking into HTTP leads us to Quick UDP Internet Connections (QUIC), a new transport protocol designed by Google, which is the base for HTTP/3. QUIC uses UDP as its underlying transport layer and provides many benefits over TCP, such as reduced latency, improved security, and better congestion control (Roskind, 2012). Features of interest for this scenario are the use of UDP, the ability to reliably transmit data in order, and the built-in Public Key Infrastructure (PKI) based encryption, providing authentication. Combining UDP hole punching with QUIC achieves a free, encrypted, low latency, and reliable peer-to-peer connection.

IMPLEMENTATION

Performance/latency is a significant consideration when comparing the different networking solutions, as it directly affects the detection time and human safety (Prasanna et al., 2022). In order to compare the latency of this solution to the chosen solution in the previous work (Prasanna et al., 2022), we recreate a test used in the previous work. This test involves using a small group of Raspberry Shake ground motion sensors connected to the internet and running the solutions to be compared in parallel and measuring the latency. For this test, a proof-of-concept implementation of the explored solution was put together in Node.js using the WebTransport library and compared with TCP over ZeroTier. Over 6 hours, pings were sent out every 10 seconds, and the round-trip time was recorded. The sensors used in the original test could not be accessed, so to maintain consistency and have a fair comparison, a new group of sensors was selected in positions as close as possible to those used in the Wellington

region in the previous test. A total of 5 sensors were part of the test and are shown in Figure 1.

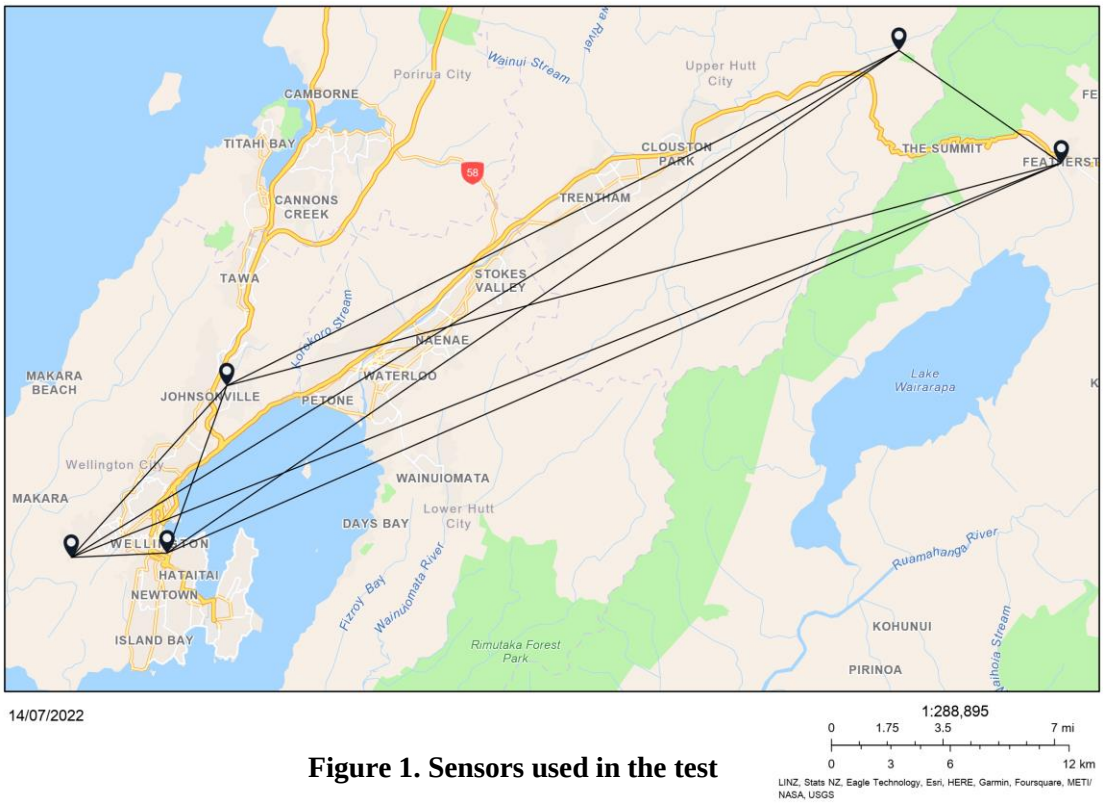

Figure 1. Sensors used in the test

Because only latency is being tested, the test can be simplified. Instead of testing with simulated ground motion data like in the previous work, it is sufficient to simply run a ping server. This simplification significantly reduced the complexity of the codebase and simplified the testing procedures.

Implementation findings

For future proofing and ease of use, the implementation is split into two modular components: the router and the application. The router is responsible for the peer-to-peer communication and forwards packets to the application. The application handles encryption, authentication and business logic and can be implemented similarly to a regular QUIC application using any QUIC library. This means that programs such as the EEW software can implement the application using its native languages' existing APIs and libraries, significantly decreasing the work needed to integrate this method into existing projects.

The Router

To initiate peer-to-peer communication, a practice known as signalling is used to allow peers to find each other. This involves a server with a public IP address and two peers. This process includes NAT traversal, so peers behind a NAT will be able to communicate.

First, both peers send a UDP packet to a public server, and then the server replies with the address of the other peer. Once each peer has the address of the other, they each send a packet to the other. When both peers receive replies from the other peer, the connection is considered successful, and the application can start sending data. The public server is similar to a Session Traversal Utilities for NAT (STUN) server (Rosenberg, Mahy, Matthews, & Wing, 2008).

For each incoming address, a new local UDP client with a unique address is created and used to forward only packets from the incoming address, so each peer still appears to have a unique address, and the application can

treat it as a regular client. Because the router emulates a regular UDP client, the router should be compatible with most UDP-based protocols.

The Application

The application interfaces with the router and performs business logic such as authentication and earthquake alerts. For this proof of concept, it is a simple echo server for testing performance.

This application uses Public Key Infrastructure (PKI) to authenticate sensors. A Certificate Authority is set up to issue certificates to each sensor and is installed on every sensor so they can verify other sensors' certificates. Sensors use these certificates to authenticate with a TLS handshake when a QUIC connection is initiated. In an EEW system, the sensor which is the source of alerts is the server and presents the certificate. This way, each alert can be verified to be from the claimed sensor. Mutual TLS (mTLS) can also be enabled, but it was deemed unnecessary because of the public nature of earthquake alerts and how it does not have any runtime performance impact, so test results without mTLS are still applicable to it.

On an incoming connection, the application initiates a bidirectional stream and immediately returns received data. The application creates connections to other sensors, sends the message "ping" every 10 seconds, and times how long it takes for the reply to arrive back.

When the application wants to create a tunnel, it sends a message to the router containing the peer ID, and the router will communicate with the public server to find the peer, hole punch to get a peer-to-peer communication, and then open a local port that the application can communicate with as though it were the peer application.

RESULTS

Raw ping times were collected from the sensors in the test and loaded into Microsoft Excel. For each connection between two sensors and for each connection type, the median and 90th percentile round trip time was calculated. The median time shows average performance, but the 90th percentile is also important because even a few slower messages can slow down detection time. The difference between the median and 90th percentile is shown to help in comparison.

Each connection yielded ~2,000 ping measurements over six hours. For all ten connection pairs possible in a group of five sensors, this results in ~20,000 pings for each connection type and ~40,000 pings in total. The results are shown in Table 1.

Table 1. Comparison of Round Trip Time (milliseconds)

Peers	ZeroTier Median	ZeroTier 90th Percentile	QUIC Median	QUIC 90th Percentile	Median Delta	90th Percentile Delta
1 - 2	52	113	48	59	-4	-54
1 - 3	26	79	30	32	4	-47
1 - 4	22	85	25	28	3	-57
1 - 5	10	66	13	17	3	-49
2 - 3	69	130	63	76	-6	-54
2 - 4	68	150	59	74	-9	-76
2 - 5	51	118	54	64	3	-54
3 - 4	26	79	29	32	3	-47
3 - 5	27	80	31	34	4	-46
4 - 5	17	74	20	26	3	-48
Average	**36.8**	**97.4**	**37.2**	**44.2**	**0.4**	**-53.2**

The results show that the median time across all sensors is similar; the average median time for QUIC is 0.4 milliseconds higher than ZeroTier. However, the average 90th percentile time is significantly lower for QUIC compared to ZeroTier: 44.2 and 97.4, respectively. QUIC has almost half the 90th percentile latency, indicating that QUIC latency is more consistently lower. Therefore, it can be said that QUIC outperforms TCP over ZeroTier.

LIMITATIONS AND FUTURE WORK

The findings found that using QUIC over hole-punched UDP appears to be a viable method for peer-to-peer communication in an EEW context. More work still needs to be done to get an implementation capable of actual

use in an EEW. A significant limitation in the explored method is that there are no fallback mechanisms if a sensor cannot establish connectivity in environments that do not allow UDP Hole Punching, like a symmetric NAT. Future work aims to resolve this by implementing a relay running on a publicly exposed server, similar to a TURN server (Rosenberg et al., 2008), which sensors that cannot communicate peer to peer may use as a proxy.

A limitation in the test conducted is that the throughput of QUIC over hole-punched UDP is not tested. This was done because, in the architecture proposed in (Prasanna et al., 2022), communication between peers consists solely of single packet notifications of ground motion, so very little bandwidth is required. If bandwidth were to be tested, the results should be consistent with other comparisons between QUIC and TCP and show that QUIC supports a higher throughput (Soni & Rajput, 2021).

Additional improvements can also be made. In the explored method, clients still rely on a centralised server for initiating connections, which could be a problem as this is a single point of failure. A possible solution is using Universal Plug and Play Internet Gateway Device (UPnP IGD) to allow sensors already part of the peer-to-peer network to act as the public servers, as described in the implementation section. This is possible because it allows the sensor to request a public port to be forwarded to it by the router, essentially removing the complications in P2P communication introduced by a NAT (Boucadair, Penno, & Wing, 2013). This decentralises the connection initiation process and makes the system much more resilient in disasters, as sensors attempting to reconnect after a telecommunications fault only need to reach one other sensor to join the network. This also solves the issue of maintaining low latency when UDP Hole Punching is impossible, as the relay server can be one of these sensors acting as a public server, which would be much closer than a cloud server. Future works also include adding compatibility with LoRa, a radio communication technique to allow running the network independent from the internet.

CONCLUSION

This paper introduced a new method of peer-to-peer communication designed with a decentralised EEW system in mind: QUIC over Hole Punched UDP. The latency of a proof-of-concept implementation of this is compared with a peer-to-peer method chosen in previous work (Prasanna et al., 2022), TCP over ZeroTier, and the results show that QUIC over Hole Punched UDP outperforms TCP over ZeroTier.

Both approaches are similar, using UDP hole-punching as the underlying technology, but QUIC over Hole Punched UDP has several advantages, mainly that it is free and open access and has lower latency than ZeroTier. Though more work is still needed until it is suitable for actual use, QUIC over Hole Punched UDP has the potential to be a better method for peer-to-peer communication in an EEW system than TCP over ZeroTier.

ACKNOWLEDGEMENTS

In addition to the low-cost EEW community of practice, which includes domestic and international researchers, practitioners, sensor manufacturers, aligned research programmes, and local and national government agencies, the authors would like to thank the members of the larger research group conducting numerous aligned research activities beyond the work presented in this paper for their invaluable support and contributions.

This research was funded by the Earthquake Commission, New Zealand: EQC Project No 20794, Massey University: SIF Funding 2020, MURF Funding 2020–2021, and QuakeCoRE, a New Zealand Tertiary Education Commission-funded Centre. This is QuakeCoRE publication number 0788.

REFERENCES

Böse, M., Allen, R., Brown, H., Gua, G., Fischer, M., Hauksson, E., . . . Jordan, T. (2014). CISN ShakeAlert: An Earthquake Early Warning Demonstration System for California. In F. Wenzel & J. Zschau (Eds.), *Early Warning for Geological Disasters: Scientific Methods and Current Practice* (pp. 49-69). Berlin, Heidelberg: Springer Berlin Heidelberg.

Brooks, B. A., Protti, M., Ericksen, T., Bunn, J., Vega, F., Cochran, E. S., . . . Glennie, C. L. (2021). Robust Earthquake Early Warning at a Fraction of the Cost: ASTUTI Costa Rica. *AGU Advances, 2*(3), e2021AV000407. doi:https://doi.org/10.1029/2021AV000407

Fleming, K., Picozzi, M., Milkereit, C., Kuhnlenz, F., Lichtblau, B., Fischer, J., . . . Ozel, O. (2009). The Self-organizing Seismic Early Warning Information Network (SOSEWIN). *Seismological Research Letters - SEISMOL RES LETT, 80*, 755-771. doi:10.1785/gssrl.80.5.755

Ford, B., Srisuresh, P., & Kegel, D. (2005). *Peer-to-Peer Communication Across Network Address Translators.* Paper presented at the USENIX Annual Technical Conference, General Track.

Grasso, V. F., Beck, J. L., & Manfredi, G. (2007). Seismic Early Warning Systems: Procedure for Automated

Decision Making. In (pp. 179-209): Springer Berlin Heidelberg.

Prasanna, R., Chandrakumar, C., Nandana, R., Holden, C., Punchihewa, A., Becker, J. S., . . . Tan, M. L. (2022). "Saving Precious Seconds" - A Novel Approach to Implementing a Low-Cost Earthquake Early Warning System with Node-Level Detection and Alert Generation. *Informatics, 9*(1), 25.

Rosenberg, J., Mahy, R., Matthews, P., & Wing, D. (2008). *Session traversal utilities for NAT (STUN)* (2070-1721). Retrieved from

Roskind, J. (2012). QUIC: Design Document and Specification Rationale. Retrieved from https://docs.google.com/document/d/1RNHkx_VvKWyWg6Lr8SZ-saqsQx7rFV-ev2jRFUoVD34/edit

Simmons, K. M., & Sutter, D. (2009). False Alarms, Tornado Warnings, and Tornado Casualties. *Weather, Climate, and Society, 1*(1), 38-53. doi:10.1175/2009wcas1005.1

Soni, M., & Rajput, B. S. (2021). Security and Performance Evaluations of QUIC Protocol. In (pp. 457-462): Springer Singapore.

Strauss, J. A., & Allen, R. M. (2016). Benefits and Costs of Earthquake Early Warning. *Seismological Research Letters, 87*(3), 765-772. doi:10.1785/0220150149

Yih-Min, W., Kanamori, H., Allen, R. M., & Hauksson, E. (2007). Determination of earthquake early warning parameters, τc and Pd, for southern California. *Geophysical Journal International, 170*(2), 711-717. doi:10.1111/j.1365-246X.2007.03430.x