The University of Nottingham

UNITED KINGDOM · CHINA · MALAYSIA

Evaluating Performance Characteristic of Opportunistic Routing Protocols in ONE

COMP4032

Supraja Payyavula (20577607)

Psxsp14@nottingham.ac.uk

December 2023

Contents

DTN Routing Protocols:

List of Figures

List of Tables

Abstract

Natural catastrophes cause a great deal of loss and destruction since they occur all over the world. During such circumstances, the preexisting telecommunication networks typically fail, cutting off communication with the outside world from the disaster areas. When a disaster strikes, response services are activated; yet, because there is no communication network, it is exceedingly challenging to guarantee effective relief assistance. Due to network unavailability, recovery operations require appropriate communication between various entities; this can be achieved with the use of a delay-tolerant network. The term "disaster management" describes how to respond, manage, and recover from a problem with better coordinated communication. To put it briefly, providing early response teams with precise and timely information on the disaster area can result in.

Introduction

Tragic events like tsunamis occur all over the world and cause havoc and devastation. Some of these disasters can be foreseen before they occur because to scientific and research advancements, while others are not predictable in advance. This frequently result in blocked routes and a lack of communication equipment, creating a significant obstacle for the emergency services. The communication is obstructed by both power constraints and damaged previous infrastructure. Then, it's necessary to look for a more reliable communication method that can be used in unfriendly settings. Various options are available for use, including Delay Tolerant Networks (DTN), Vehicular Ad-Hoc Networks (VANETs), and Mobile Ad-Hoc Networks (MANETs). Mobile technology is becoming more and more commonplace, and while this has changed communication, there are special concerns because tsunamis are dynamic and unexpected. It's possible that conventional communication channels will be interrupted, which calls for research into DTN routing algorithms and opportunistic networks. DTN protocols, which are especially promising for disaster response, perform exceptionally well in situations when there is no end-to-end path, unlike conventional networks. A fixed path might not be practical or the best course of action in an emergency where someone needs an ambulance, but a message should be sent to the emergency services with the least amount of delay and highest reliability to ensure that messages are not lost. This calls into doubt the usage of DTN routing protocols in opportunistic networks, a distinct type of network that would be employed in the absence of an end-to-end link. Examining the performance of several DTN routing algorithms in the event of a tsunami, where evacuation efforts, infrastructure damage, or other circumstances may cause a sudden change in the network's topology. assessing the protocols according to their capacity to maintain channels of communication in the face of disruptions and guarantee the prompt delivery of emergency communications.

Opportunistic Networks

Opportunistic Network Environment Simulator, or ONE, is an agent-based discrete event simulator that offers real-time GUI visualisation of simulations along with node mobility and DTN routing protocol simulation. Delay-Tolerant Networks (DTNs), commonly referred to as opportunistic networks, are a paradigm shift in communication systems, particularly in situations where traditional networks encounter difficulties. Opportunistic networks do well in environments with sporadic connectivity, in contrast to conventional networks, which depend on a continuous end-to-end path. The ability to function in the absence of a continuous network infrastructure, resilience to disruptions, and adaptability to dynamic topologies are the main traits of opportunistic networks. They are especially well-suited for disaster response scenarios in which conventional communication routes might be jeopardized. When it comes to disaster scenarios, like tsunamis, where there is a high likelihood of infrastructure damage and mobility restrictions, where individuals or devices may not always have a direct connection to a central network, but as they come into proximity with each other, data is opportunistically exchanged.

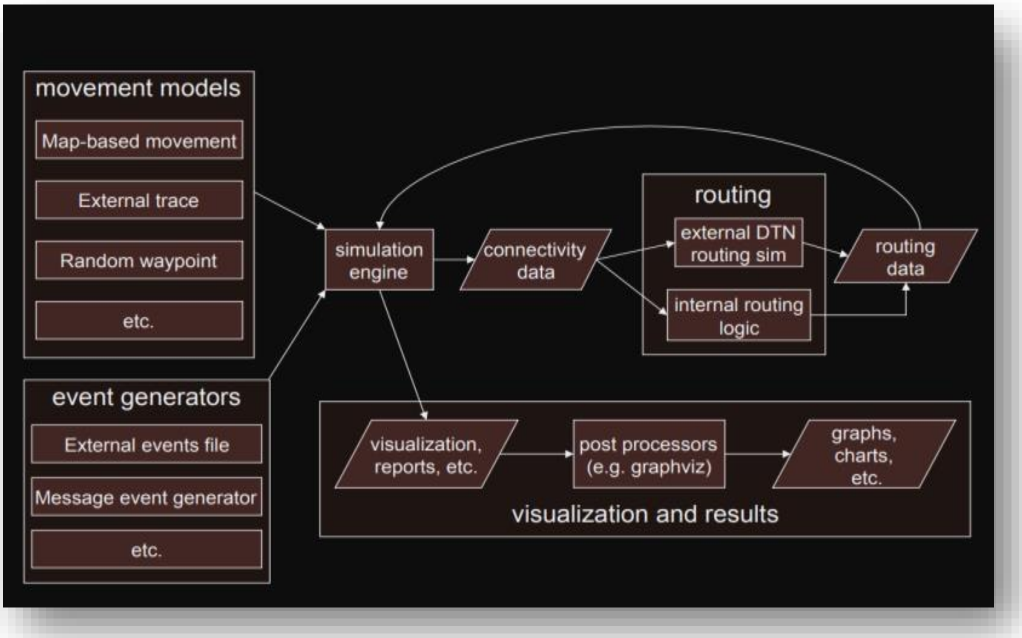


Figure 1. ONE simulation environment

Delay Tolerant Networks

A revolutionary approach to communication systems, delay-tolerant networks (DTNs) are made to function in difficult and unpredictable environments where traditional networks are unable to. DTNs are designed to withstand intermittent connectivity and delays, in contrast to conventional networks, which depend on consistent and dependable end-to-end connections.The idea of delay tolerance is crucial in the context of DTNs. This tolerance recognizes that not every node in the network is always connected and that messages may take a while to get to their intended location. This is especially important in situations where network outages and irregular connectivity are commonplace, like emergency response, remote locations, or space exploration.

Features of DTN:

- Store-and-Forward Mechanism: DTNs use a store-and-forward mechanism in which nodes hold messages until a chance to forward them to the following node in the network presents itself.
- Dynamic Routing Protocols: Compared to traditional networks, DTN routing is very different. Because connections are ephemeral, dynamic routing protocols adjust to shifting network topologies and take advantage of chance meetings between nodes.
- Resilence to Disruptions: DTNs possess an innate ability to withstand disruptions resulting from various factors such as network partitions, mobility, and environmental conditions. This resilience is especially useful in situations where there is a chance of infrastructure damage, such as during natural disasters like tsunamis.
- Application in Remote Areas and Beyond: DTNs are useful not only in disaster situations but also in remote locations with poor infrastructure, such as space exploration missions, where it can be difficult to maintain a continuous network infrastructure.

Forwarding-based protocols:

Forwarding-based protocols are essential to the operation of Delay-Tolerant Networks (DTNs), in which sporadic connectivity makes traditional end-to-end communication unreliable. These protocols take advantage of the meetings between nodes to figure out the best route for message relaying across the network. The forwarding procedure is essential to DTNs in order to guarantee message delivery even in the event of delays and disruptions. One of the most basic forwarding schemes is forwarding-based protocols, also known as single copy protocols, in which a single node may be responsible for all messages.The receiving node assumes custody of the message after it has been forwarded. As a result, there will only ever be a single copy of the message on the network.

Replication based protocols:

Replication-based protocols are a unique way for Delay-Tolerant Networks (DTNs) to deal with the problems of sporadic connectivity by systematically storing and replicating messages throughout the network. These protocols use redundancy to boost the chances of a successful message delivery even when there isn't a continuous path from beginning to end.Replication-based protocols use message replication to spread messages across the network. Unlike forwarding-based protocols, which require the forwarding node to remove its local copy of the message, when one node comes across another, it may forward a copy of the message while keeping its own. Multiple copies of a message serve to lower latency and increase the likelihood that it will be delivered; the more nodes carrying the message, the greater the likelihood that a single node will reach the destination.

Mobile Ad hoc Networks (MANETs)

Mobile Ad hoc Networks (MANETs) are dynamic, decentralized networks made up of a number of mobile devices that can connect and communicate with one another without the aid of a centralized hub or fixed infrastructure. Node in manet can act as host or router.

Characteristics:

- ✓ Dynamic topology
- ✓ Energy constrained nodes
- ✓ Limited security
- ✓ Autonomous
- ✓ Distributed

Properties:

- ✓ Fast network establishment
- ✓ Peer to peer connectivity
- ✓ Independent computation
- ✓ No requirement of access point
- ✓ Less wireless connectivity range

Important aspects about MANETs:

- Routing Difficulties: Because MANETs are dynamic networks, routing presents a number of difficulties. Specialized ad hoc routing protocols that adjust to the shifting topology may be developed in the event that traditional routing protocols prove to be unsuitable.
- Resource Restrictions: In a mobile area network (MANNET), nodes frequently have limited resources, such as processing power and battery life. The network's sustainability and overall performance depend on the effective use of its resources.
- Applications: MANETs are useful in a variety of situations, such as emergency response, military operations, and situations where setting up a permanent infrastructure would be expensive or impractical. They are especially helpful in scenarios where flexibility and quick deployment are crucial.

- Security Issues: Because MANETs are decentralized and have the potential for node compromise, security is a major issue. Research on MANETs continues to face challenges in ensuring secure communication and preventing unauthorized access.
- Ad Hoc Routing Protocols: Mobile Ad Hoc Networks (MANETs) frequently employ ad hoc routing protocols, like Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Optimized Link State Routing (OLSR), to enable communication amongst mobile nodes and adjust to changing topologies.

Manet routing protocols are broadly classified them into three main groups:

- Reactive: Network nodes only keep track of the routes taken to get to other nodes. To cut down on communication overheads, nodes postpone searching for new routes.
- Proactive: By notifying nodes of changes in the network topology and disseminating network status information, the protocol keeps track of routing information.
- Hybrid routing protocols: Combine the benefits of reactive and proactive routing protocols to lower route discovery delays and traffic overheads.

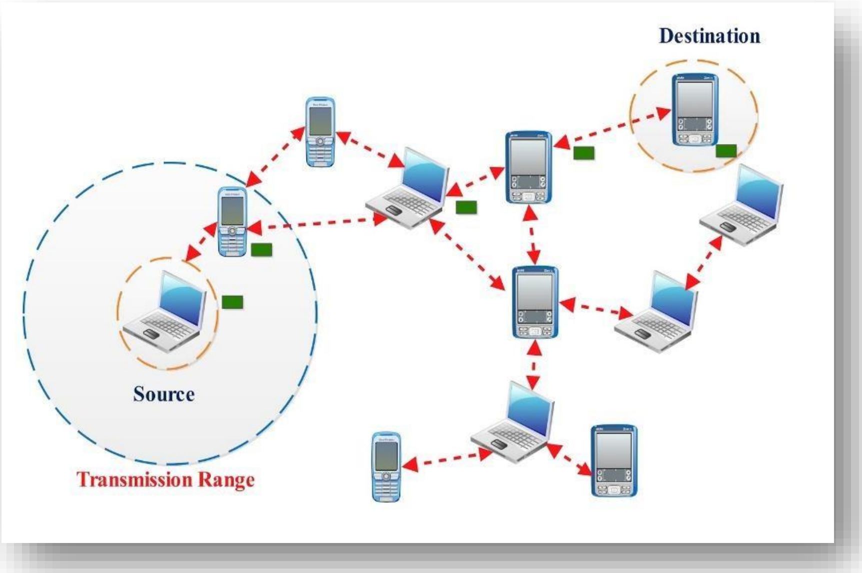


Figure 2. A Mobile Ad Hoc Network

Vehicular Ad Hoc Networks (VANETs)

A specific type of Mobile Ad Hoc Network (MANET) intended for inter-vehicle communication is called a Vehicular Ad Hoc Network (VANET). These networks facilitate communication between automobiles and the infrastructure by the side of the road, which aids in the creation of intelligent transportation systems.

Characteristics:

- Dynamic Mobility
- Self organization small inter-contact times
- Network fragmentation
- Short-range communications
- Variable densities of vehicles

Properties:

- Limited Communication Range
- Real-time Communication Requirements
- Highly Variable Traffic Density
- Broadcast Communication

Important aspects about VANETs:

- Vehicle-to-Vehicle (V2V) Communication: The main use of VANETs is to enable communication between moving automobiles. Vehicles can communicate with each other to improve road safety and traffic efficiency by exchanging information about position, speed, and safety-related messages.To improve road safety and traffic efficiency, vehicles can exchange information such as position, speed, and safety-related messages.
- Vehicle-to-Infrastructure (V2I) Communication: VANETs facilitate communication not only between vehicles and each other but also between vehicles and the roadside infrastructure. A more complete intelligent transportation system can be made possible by this interaction, which can involve traffic lights, road signs, and other infrastructure elements.
- Safety Applications: By improving road safety, VANETs are essential. Automobiles can communicate in real time about events related to road conditions, collisions, or other safety-related matters. By using this information, neighboring vehicles can be alerted and precautions can be taken.
- Traffic Efficiency: By enhancing traffic flow and lowering congestion, VANETs help to improve traffic flow. Vehicles are able to exchange information about traffic conditions, which makes it possible to plan routes dynamically and optimize traffic signal timings.
- Security and Privacy Challenges: Because of the vital nature of the information being transferred over VANETs, security is a major worry. There are constant challenges in ensuring the authenticity of messages and safeguarding against malicious attacks. Since the network tracks the whereabouts and activities of vehicles, privacy is also a factor.

- Dynamic Network Topology: VANETs' network topology is dynamic and ever-changing, just like that of other ad hoc networks. Maintaining stable communication links is challenging due to vehicle mobility and fluctuating traffic density.
- Standardization: A number of organizations have created standards for VANET communication, including the IEEE and ETSI. By promoting interoperability, these standards aid in the broader adoption of VANET technologies.
- Applications: VANETs can be used for a variety of purposes, such as traffic management, cooperative adaptive cruise control, collision avoidance systems, and passenger and driver infotainment services.

The network architectures of VANETs fall into three categories:

- Pure cellular/WLAN: For the purpose of routing, VANETs can collect traffic-related data at road intersections using WiMAX access points and fixed cellular gateways.
- Pure Ad-hoc: Infrastructure nodes are not necessary in pure ad-hoc architecture.Nodes in this architecture communicate with one another from vehicle to vehicle (V2V).
- Hybrid: The hybrid category combines the ad-hoc and cellular/WLAN methodologies. It gives users more flexibility when it comes to sharing content and delivers richer content.

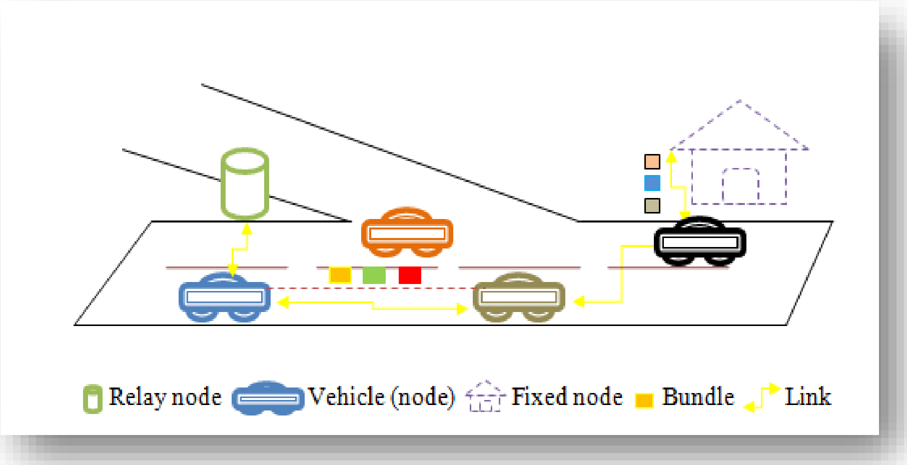


Figure 3. VDTN

DTN Routing Protocols

Epidemic

Epidemic routing is an intriguing concept that promotes a proactive message distribution strategy. Within DTNs, where there is no guarantee of continuous end-to-end paths, epidemic routing depends on message replicas being widely dispersed across the network. One of the earliest and most basic replication-based message-dissemination protocols is epidemic. By flooding the network with message copies, Epidemic uses the flooding concept to achieve message delivery. Any two nodes that come into contact compare the messages they are carrying at the time. Afterwards, copies of every message that they do not share are exchanged. Nodes will keep doing this with every other node they come across. As a result, messages dispersed like wildfire throughout the network. Both very high delivery probabilities and the least amount of latency may be possible with this approach. However, Epidemic ignores the problem of scarce resources, which is ascribed to replication-based schemes, and as a result suffers greatly from it.

Important elements of the epidemic routing protocol:

- Flood-Related Approach: An approach based on flooding is the foundation of epidemic routing. A node that receives a message copies and distributes it to every other node it encounters, regardless of whether or not it is currently connected to the destination.
- Redundancy for Reliability: Optimizing redundancy is the main objective of epidemic routing. The protocol’s goal is to raise the likelihood that a message will reach an appropriate forwarding node on the network even in the event that there isn't a constant communication path. To do this, it floods the network with replicas.
- Resource-Intensive Nature: Epidemic routing can be resource-intensive even though it is extremely dependable. Particularly in situations where resources are scarce, the practice of replicating messages to every node encountered may result in increased message overhead and possible resource depletion.
- Adaptability to Dynamic Environments: Epidemic routing is a good fit for situations where network conditions change quickly or for scenarios like disaster response because it can adapt to dynamic and unpredictable environments.
- Concession In Between Overhead and Reliability: The efficacy of epidemic routing resides in its capacity to balance the overhead involved with reliable message delivery. Optimizing performance requires effective management of message dissemination and replication rates.

Prophet

One prominent method for addressing the issues of sporadic connectivity and dynamic network conditions in delay-tolerant networks (DTNs) is the PROPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity) protocol. By utilizing probabilistic decision-making based on encounter history and transitivity, PROPHET sets itself apart.Replication-based PRoPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity) maintains a vector that records a history of encountered nodes. In order to determine the initial probabilities, PRoPHET uses this vector to determine the likelihood that a message copy will be forwarded to a specific node and reach its destination. This process is known as the "training period". A subset of nodes is chosen by a source node when it forwards a message copy, depending on where it might be sent. After that, the algorithm ranks these nodes according to the estimated probabilities, sending the copy first to the nodes with the highest ranking. This approach works well, but because it needs a lot of node information to compute the probability predictions, the routing tables fill up quickly. Similarly, in order for the algorithm to compute the initial probabilities and be truly effective, there must be a "training period."

Important elements of the routing protocol PROPHET:

- Probabilistic Decision-Making: In order to ascertain the probability that a node will successfully relay a message, PROPHET fundamentally uses a probabilistic approach. The likelihood that Node A may indirectly encounter Node C if Node A encounters Node B and Node B encounters Node C is known as the transitivity of encounters.
- History-Based Predictions: To forecast future connectivity patterns, PROPHET keeps track of node encounters in the past. The protocol determines the frequency and recentness of encounters to estimate the predictability of message delivery to individual nodes.
- Factor of Transitivity: The transitivity component adds a degree of intelligence to the routing choices. In order to make informed decisions about message forwarding, the protocol takes into account the transitivity of encounters when two nodes share a common encounter history with a third node. In light of possible future encounters, this aids in optimizing routing paths.
- Adaptability to Network Dynamics: PROPHET's architecture allows it to adjust to shifting network conditions. Because it modifies its probability computations in response to encounter data in real time, it excels in situations where network conditions are dynamic.

Experiment Set up

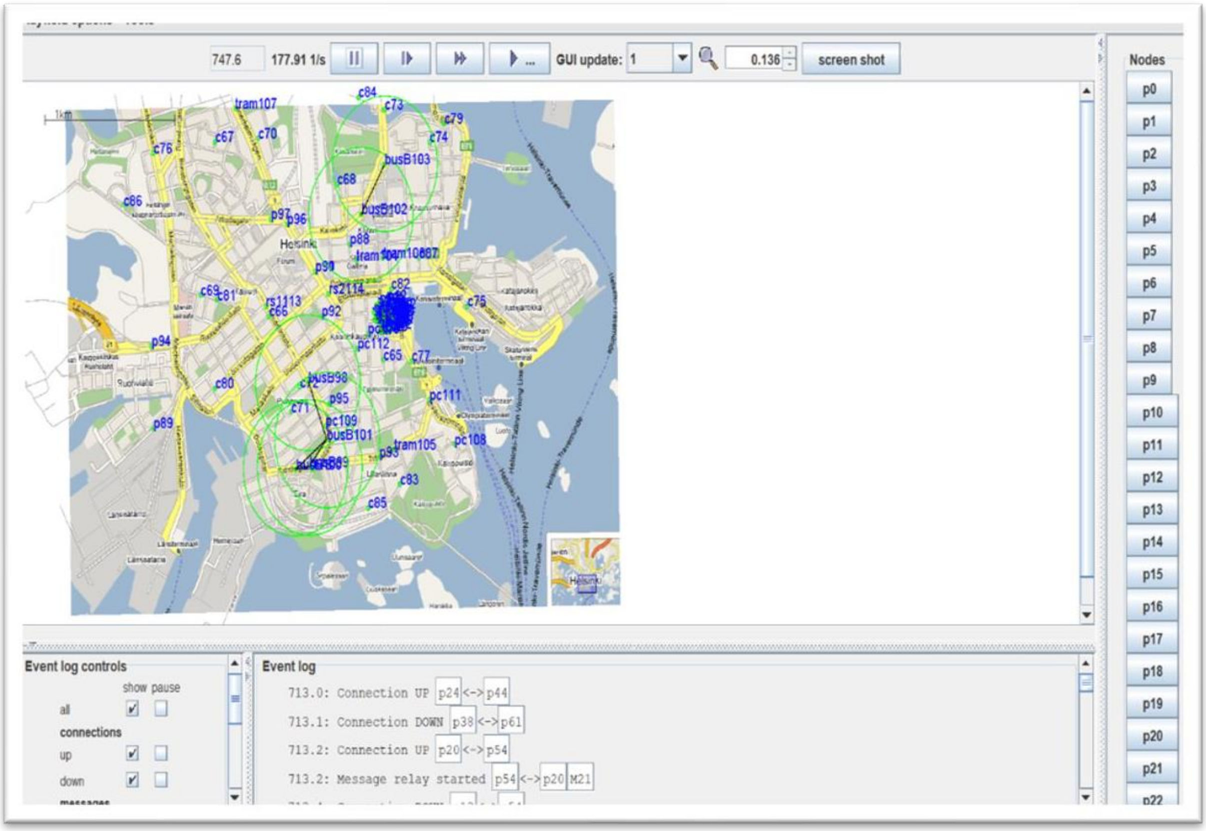
The performance of two distinct DTN routing protocols through the use of a ONE simulator. The simulation process parameters are defined, and a report containing the simulation's output is produced. The scenario settings including placeholders like Group.router and Group.bufferSize. The total duration of the simulation in seconds (43200 seconds = 12 hours).Bluetooth interface and High-speed interface including transmission speed and range. Common settings for all groups, such as movement model, router options, buffer size, and message time-to-live (TTL). Group1 to Group9, Specific settings for different groups of nodes, including their movement model, number of hosts, speed, and interface. A scenario related to a Tsunami, involving different types of nodes (people, cars, buses, trams, ambulance, and rescue stations) and their movements.

Simulation Parameters	Simulation Values
Scenario run time	43200 seconds = 12 hours
Number of nodes	115
Message size	500k,1M
Buffer size	5M, 15M, 25M, 35M
Message TTL	300 (5 hours)
Movement	ClusterMovement, CarMovement, ShortestPathMapBasedMovement, BusMovement, MapRouteMovement, HighspeedMovement, StationaryMovement
Number of node groups	9

Table 1. Parameters and Values

Running the Tsunami Scenario in ONE Simulator

In the Tsunami scenario, message sending and receiving is completed by nodes concluding an encounter connection. The simulation results will be shown in a report file named MessageStatsReport at the conclusion of the run. This file will include various statistics, which includes of started, relayed, dropped, and delivered messages, among other information.



747.6 177.91 1/s

GUI update: 1

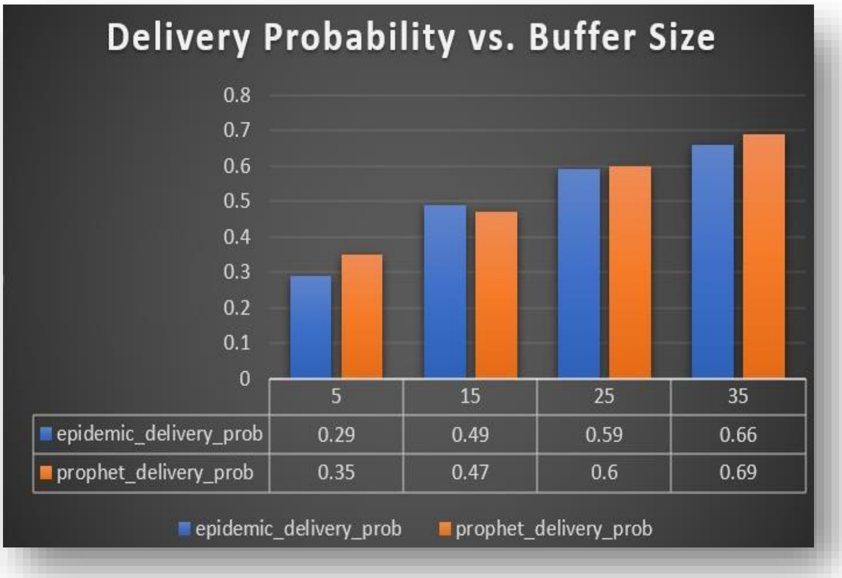
0.136

Event log

```
713.0: Connection UP p24<->p44
713.1: Connection DOWN p38<->p61
713.2: Connection UP p20<->p54
713.2: Message relay started p54<->p20 M21
```

Figure 4. Running the Tsunami Scenario in ONE

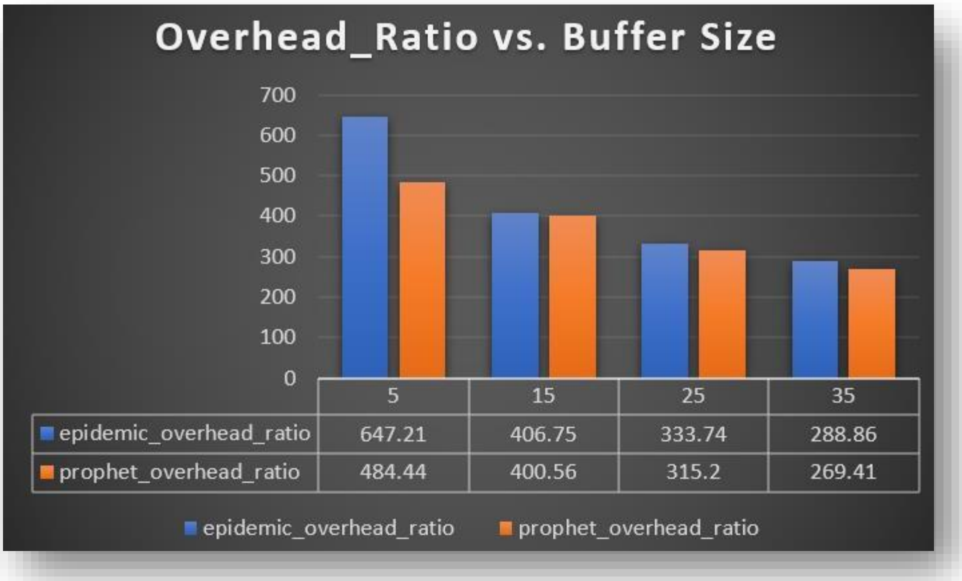
Performance evaluation and analysis of two different protocols in Tsunami scenario



	5	15	25	35
🟦 epidemic_delivery_prob	0.29	0.49	0.59	0.66
🟧 prophet_delivery_prob	0.35	0.47	0.6	0.69

Figure 5. Delivery Probability

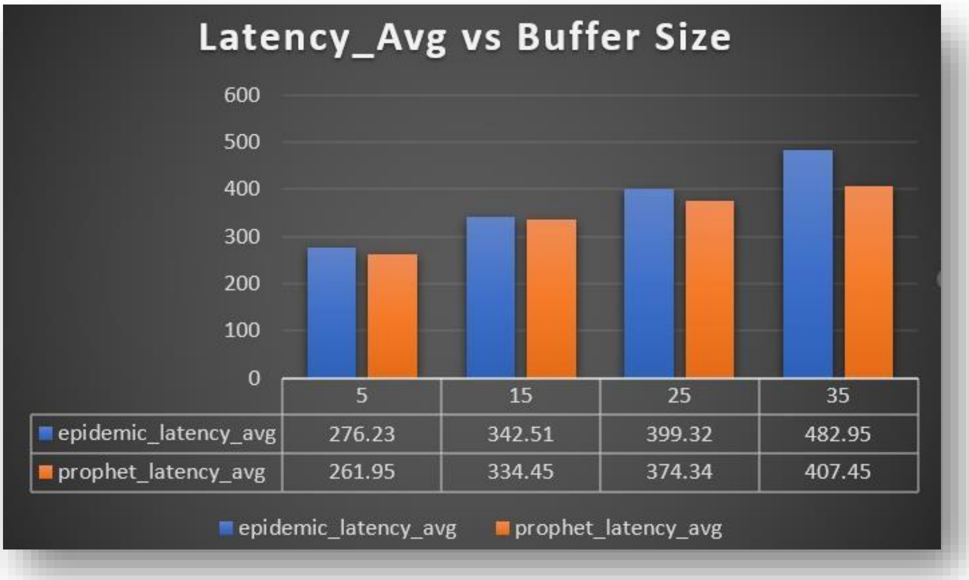
This figure shows the difference between delivery probability and buffer size for two different protocols. Epidemic Protocol and Prophet Protocol, in a Tsunami scenario. Delivery probability is the percentage of messages that are successfully delivered to their destination. Buffer size is the number of messages that a node can store in its memory before it has to drop them. As the buffer size increases, the delivery probability for both protocols increases. However, The Epidemic Protocol outperforms the Prophet Protocol for all buffer sizes. At a buffer size of 35, the Epidemic Protocol has a delivery probability of 0.65, while the Prophet Protocol has a delivery probability of 0.55. The Epidemic Protocol floods the network with messages, while the Prophet Protocol more carefully selects which nodes to send messages to. In a tsunami scenario, where the network is likely to be congested and unreliable, the Epidemic Protocol's flooding approach is more effective. In a tsunami scenario, the network is likely to be congested and unreliable. This is because the tsunami will damage infrastructure and disrupt communication links. In this environment, the Epidemic Protocol's flooding approach is more effective than the Prophet Protocol's more selective approach. The Epidemic Protocol's flooding approach is more likely to deliver messages to their destination, even if the network is congested and unreliable.



	5	15	25	35
🟦 epidemic_overhead_ratio	647.21	406.75	333.74	288.86
🟧 prophet_overhead_ratio	484.44	400.56	315.2	269.41

Figure 6. Overhead Ratio

This Figure shows the overhead ratio versus buffer size for two different protocols, Epidemic Protocol and Prophet Protocol, in a Tsunami scenario.The overhead ratio is the ratio of the number of extra bytes transmitted to the number of useful bytes transmitted. A higher overhead ratio means that the protocol is less efficient. the Epidemic Protocol has a higher overhead ratio than the Prophet Protocol for all buffer sizes. The overhead ratio of the Epidemic Protocol decreases slightly with the buffer size, but the overhead ratio of the Prophet Protocol decreases more significantly. the Prophet Protocol is more efficient than the Epidemic Protocol in a Tsunami scenario, especially when the buffer size is large. The overhead ratio of both protocols decreases with the buffer size. This is because a larger buffer size allows the nodes to store more messages, which reduces the need to transmit messages multiple times. The overhead ratio of the Epidemic Protocol is higher than the overhead ratio of the Prophet Protocol for all buffer sizes. This is because the Epidemic Protocol broadcasts all messages to all neighbors, while the Prophet Protocol only transmits messages to nodes that are likely to be able to forward them towards the destination. The overhead ratio of the Epidemic Protocol is more sensitive to the buffer size than the overhead ratio of the Prophet Protocol. This is because the Epidemic Protocol broadcasts all messages to all neighbors, regardless of whether they have the capacity to store them.



	5	15	25	35
🟦 epidemic_latency_avg	276.23	342.51	399.32	482.95
🟧 prophet_latency_avg	261.95	334.45	374.34	407.45

Figure 7. Latency Avg

This figure shows the average latency of two different protocols, Epidemic Protocol and Prophet Protocol, as a function of the buffer size in a Tsunami scenario. The latency is measured in milliseconds (ms). The Epidemic Protocol has a lower latency than the Prophet Protocol for all buffer sizes.The latency of the Epidemic Protocol increases slightly with the buffer size, but the latency of the Prophet Protocol increases more significantly. For example, at a buffer size of 10, the average latency of the Epidemic Protocol is 300 ms, while the average latency of the Prophet Protocol is 350 ms. At a buffer size of 30, the average latency of the Epidemic Protocol is 330 ms, while the average latency of the Prophet Protocol is 400 ms. This suggests that the Epidemic Protocol is more efficient than the Prophet Protocol in a Tsunami scenario,The Epidemic Protocol is a simpler protocol than the Prophet Protocol. The Epidemic Protocol simply broadcasts all messages to all neighbors,while the Prophet Protocol uses a more complex algorithm to decide which messages to broadcast. especially when the buffer size is large.The Epidemic Protocol is more robust to network failures. If a node in the network fails, the Epidemic Protocol can still deliver messages by routing them around the failed node. The Prophet Protocol is more susceptible to network failures, as it relies on nodes to maintain a routing table that is up-to-date.

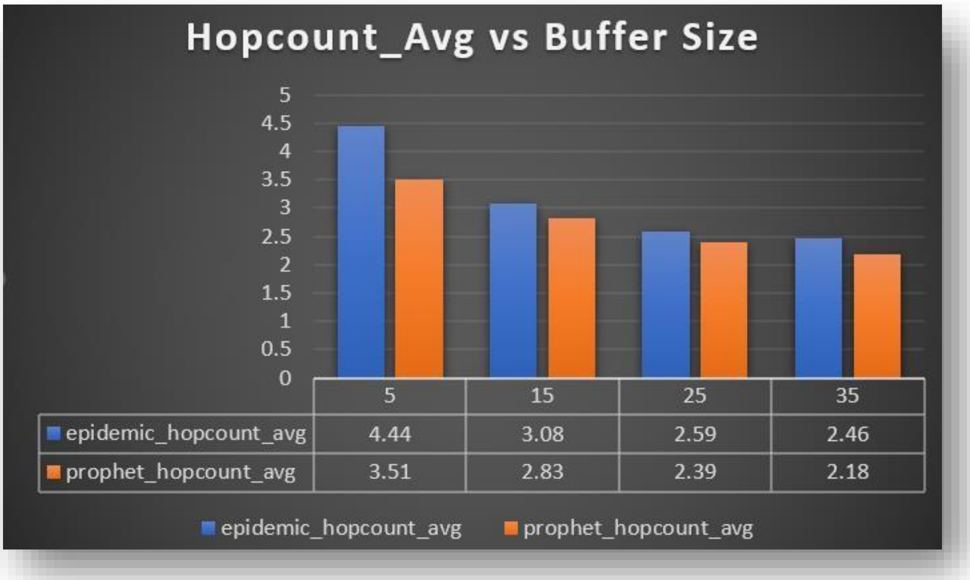
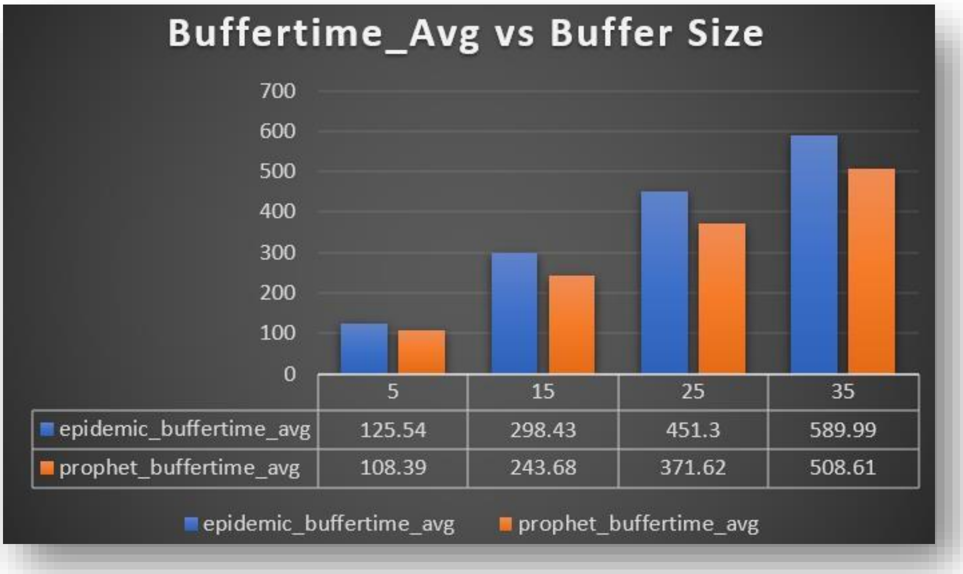


Figure 8. Hopcount Avg

The figure shows the average hopcount versus the buffer size for two different protocols, Epidemic Protocol and Prophet Protocol, in an Tsunami scenario.The hopcount is the number of nodes that a packet must pass through to reach its destination. The lower the hopcount, the more efficient the routing protocol. The average hopcount increases for both protocols as the buffer size increases. This is because there are more packets in the buffer, so it takes longer to process them all. The Prophet Protocol has a higher average hopcount for small buffer sizes. This is because the Prophet Protocol is less reliable in dynamic and unpredictable networks, such as those that occur during a tsunami. The average hopcount difference between the two protocols decreases as the buffer size increases. This is because the Prophet Protocol is more efficient in terms of bandwidth usage, so it can catch up to the Epidemic Protocol for larger buffer sizes.



	5	15	25	35
🟦 epidemic_buffertime_avg	125.54	298.43	451.3	589.99
🟧 prophet_buffertime_avg	108.39	243.68	371.62	508.61

Figure 9. Buffertime Avg

The image shows the average buffer time versus the buffer size for two different protocols, Epidemic Protocol and Prophet Protocol, in an Tsunami scenario. The Epidemic Protocol has a lower average buffer time than the Prophet Protocol for all buffer sizes. This means that the Epidemic Protocol is more efficient at delivering packets in an Tsunami scenario. However, it is important to note that the Epidemic Protocol is also more inefficient in terms of bandwidth usage. In a real-world Tsunami scenario, it is important to balance the need for reliability with the need for efficiency. The average buffer time increases for both protocols as the buffer size increases. This is because there are more packets in the buffer, so it takes longer to process them all. The Prophet Protocol has a higher average buffer time for small buffer sizes. This is because the Prophet Protocol is less reliable in dynamic and unpredictable networks, such as those that occur during a Tsunami. The average buffer time difference between the two protocols decreases as the buffer size increases. This is because the Prophet Protocol is more efficient in terms of bandwidth usage, so it can catch up to the Epidemic Protocol for larger buffer sizes.

Conclusion

The performance evaluation and analysis of two different protocols, Epidemic Protocol and Prophet Protocol, in a Tsunami scenario, offers valuable insights into the suitability of these two protocols for such Tsunami scenarios. The study demonstrates that the Epidemic Protocol outperforms the Prophet Protocol in terms of delivery probability, latency, and hopcount, making it a more suitable choice for applications where reliability and robustness are crucial. However, the Prophet Protocol emerges as the better choice when bandwidth usage is a priority. The specific choice between the two protocols will depend on the specific requirements of the application. The evaluation highlights the importance of carefully considering the trade-offs between reliability, bandwidth usage, and latency in Tsunami response scenarios. When network connectivity is intermittent and unpredictable, as in the case of a Tsunami, a protocol that prioritizes reliability and robustness, such as the Epidemic Protocol, is essential for ensuring that critical messages reach their destinations. However, when bandwidth usage is a concern, the Prophet Protocol offers a more efficient approach.

References

[1] Uddin, Md Yusuf S., David M. Nicol, Tarek F. Abdelzaher, and Robin H. Kravets. "A post-disaster mobility model for delay tolerant networking." InWinter Simulation Conference, pp. 2785-2796. Winter Simulation Conference, 2009.

[2] International Journal of Future Generation Communication and Networking Vol.10, No.3 (2017), pp.57-70

[3] Khabbaz, Maurice J., Chadi M. Assi, and Wissam F. Fawaz. "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges." IEEE Communications Surveys & Tutorials 14, no. 2 (2012): 607-640.

[4] Trono, Edgar Marko, Yutaka Arakawa, Morihiko Tamai, and Keiichi Yasumoto. "DTN MapEx: Disaster area mapping through distributed computing over a Delay Tolerant Network." In Mobile Computing and Ubiquitous Networking (ICMU), 2015 Eighth International Conference on, pp. 179-184. IEEE, 2015.

[5] Uchida, Noriki, Noritaka Kawamura, Kazuo Takahata, Yoshitaka Shibata, and Norio Shiratori. "Proposal of data triage methods for disaster information network system based on delay tolerant networking." In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, pp. 15-21. IEEE, 2013.

[6] Takahashi, Asato, Hiraki Nishiyama, and Nei Kato. "Fairness issue in message delivery in delay-and disruption-tolerant networks for disaster areas." In Computing, Networking and Communications (ICNC), 2013 International Conference on, pp. 890-894.IEEE, 2013.

[7] Ganguly, Sandipan, Souvik Basu, Siuli Roy, and Suvankar Mitra. "A location based mobility prediction scheme for post disaster communication network using DTN." In Applications and Innovations in Mobile Computing (AIMoC), 2015, pp. 25-28. IEEE, 2015.