ACN_Report

by Tejas Muniswamy

Submission date: 28-Nov-2023 11:56PM (UTC+0000)

Submission ID: 217191175

File name: 349992_Tejas_Muniswamy_ACN_Report_7172548_513487848.docx (856.07K)

Word count: 4087

Character count: 23929

Introduction

In the rapidly evolving world of wireless communications, delay tolerant networks also known as opportunistic networks have emerged as life changing technology that can reshape the way we connect and share information. Unlike the traditional network protocol known as TCP/IP which operates on a principle of end-to-end connectivity between source and the destination. The Opportunistic network protocol (OppNets) is implemented for the networks that may lack continuous end-to-end connections, which is why OppNets is most valuable protocol in environments where the infrastructure is limited or non-existence.

OppNets operates on the principle of 'store-carry-forward' approach in which the devices hold the data as a temporary message relay until they encounter another device that can carry forward the message to its destination or closer to its destination. This decentralized approach enables communications in difficult environments such as disaster zones, remote regions, interplanetary and underwater.

This unique characteristics of the OppNets offers a plethora of chances for innovation and advancement. Additionally, they are appropriate for important applications that require unwavering reliability because to their resilience to interruptions and adaption to dynamic topologies. OppNets have enormous potential to transform communications across a wide range of areas, despite the inherent difficulties presented by sporadic connectivity and data storage limitations.

As research and development in OppNets continue to thrive, we can expect more evolution in data delivery protocols, application adaption and connectivity management. This growth opens door to many sectors that can use OppNets for number of use cases and revolutionising communication theory which leads to globally interconnected society.

This effort contributes to the study of performance analysis of Epidemic and Prophet routing protocols which are under the OppNets protocols under a catastrophic environment, like a terrorist attack.

Opportunistic Networks

Opportunistic networks are the unique class of wireless communication systems designed to operate in environments with intermittent connectivity and long or variable delay. In situations where regular wireless infrastructure is either unavailable or unfeasible, these networks are especially well suited. The OppNets architecture is type of decentralized and self-organizing which helps to handle network connection disruptions. The OppNets functions without preset routes or centralized management. OppNets device interact with one another opportunistically, making transient connections as they pass by one another's communication range.

The key components of OppNets architecture:

- Nodes: Individual devices that serve as communications nodes, such as computers, smartphones, or sensors, are the basic building pieces of OppNets. To link and communicate with other nodes, these nodes are outfitted with wireless communication interfaces like Bluetooth, high speed interfaces or Wi-Fi.
- Messages: The exchange of messages which are data packets between OppNets devices contains information to be transmitted. Bundles are used to encapsulate these messages and offer further information for handling and routing.
- Routing Protocols: The route that messages take across the network is decided by routing protocols. They use a variety of algorithms to determine which nodes are best for forwarding the messages so that it can be delivered to the destination. The protocol considers factors like message delivery probability, network conditions and node capabilities which helps to decide if the message should be forwarded to the node.
- Store-and-Forward: OppNets have sporadic connectivity, thus nodes use a store-and-forward technique. Upon receiving a message, a node store it in its memory until it comes across another node that has a greater likelihood of reaching the intended destinations.

Effective communications require addressing numerous issues introduced by the intrinsic properties of OppNets. The challenges faced by the opportunistic networking as follows:

- Message delivery: One major problem is making sure communications reach their intended recipients even in the face of erratic network conditions and connectivity. If direct connections are not available, routing systems need to be able to locate alternate channels and manage message delays.
- Resource optimization: Routing protocols should reduce resource consumption to increase the lifetime of devices and networks. This entails cutting down on pointless communications, adjusting to the capabilities and energy conservation of the devices.
- Adaptability: To ensure dependable communication, routing protocols should adjust to the shifting network circumstances and device availability. It could be necessary to make dynamic changes to message handling and forwarding strategies as a result.

Classification of OppNets protocols

Numerous routing protocols each with unique advantages and disadvantages, have been devised to handle the OppNets difficulties. Routing protocols have many different properties, but one of the most effective ways to categorise them is by determining whether a protocol creates message replication. Forwarding based routing refers to routing protocol that never replicates a message and have single custodian of that message, while replication-based routing refers to routing protocol that replicate messages and many devices have local copies of the messages.

Forwarding-based routing is a class of routing protocol often known as single copy protocol, in which a single node may be responsible for all messages. As a result, there will only ever be a single copy of the message on the network. Example of forwarding based protocols are Direct Transmission and first contact. Direct Transmission is routing protocol which uses minimal resources where a node broadcasts the message to every other node in its range. The message is delivered directly if the destination node is one of the receivers. First contact is a routing protocol that selects a node at a random from all potential connections and then sends as many messages as it can to that node. The transfer will be completed with the first person to be contacted if there are no connections available. This protocol suffers from dead end routing where it roams between number of nodes without making any positive progress towards the destination.

Replication-based routing techniques distribute several copies of messages around the network to compensate for forwarding-based protocol's inefficiency with resources. This rises the likelihood that at least one copy of the message will reach its intended destination. Unlike forwarding-based protocol where every message has single custodian and removes local copy after transferred to another node, replication-based protocol retains the local copy of the message and forwards a copy of the message. This multiple copy of the message improves the chances of message to being delivered while decreasing the latency. The disadvantage of this protocol is that with increase in message copies increases the resource consumed. The fact that numerous reductant copies of messages may persist within the network even after one has been successfully delivered to the intended recipient.

The replication-based protocols can be further divided into following:

- Unlimited Replication: This category of routing techniques permits all network nodes to duplicate messages and transmit them throughout the network to their intended recipient. If n is the number of network nodes, then a message may, in the worst scenario, be replicated n-1 times before it reaches its destination. Some examples of this routing are Epidemic, Prophet, Rapid and MaxProp.
- Quota-based Replication: This series of routing protocols sets a quota to restrict the amount of message copies that can be produced. Quota is usually a protocol parameter that has been predefined. Example of this type is Spray and wait.
-

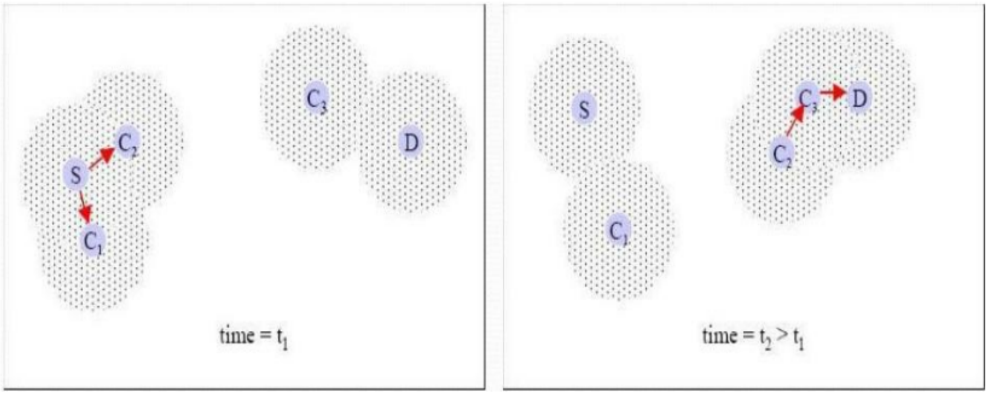
In this project the Epidemic and Prophet routing protocols will be used to study the performance analysis during the scenario Terrorist Attack.

EPIDEMIC

One of the earliest and most basic replication-based for disseminating messages. By flooding the network with copies, epidemic uses the flooding idea 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, communication dispersed like wildfire throughout the network. The key characteristics of epidemic routing protocol are:

- Simplicity: It is well suited for devices with limited resources because it is straightforward conceptually and simple to execute.
- Adaptability: It adapts effectively to fluctuating network conditions where the messages are routed opportunistically whenever contact chances exists.
- Reliable Delivery: It promises message delivery even in largely disconnected networks.

The epidemic routing strategy is easy to use. However, because there are so many message copies added to the network, it uses an enormous number of resources. Large quantities of power and bandwidth are needed because of using a lot of buffer space. The fact that epidemic spreads message copies around the network even after the recipient has received them is another problem. The idea of death certificates has been put forth to lessen this issue. The purpose of a death certificate is to spread a notification telling the network nodes to remove the sent message. In general, less resources are used because the notification size is lower than the original message. The below image illustrates the working of epidemic protocol where the node S exchanges it message with C1 and C2 node which are in communication range. Then the node C2 travels and comes inside the communication range of nodes C3 and D where the message exchange takes place like this all the nodes get the message flooded in the network.



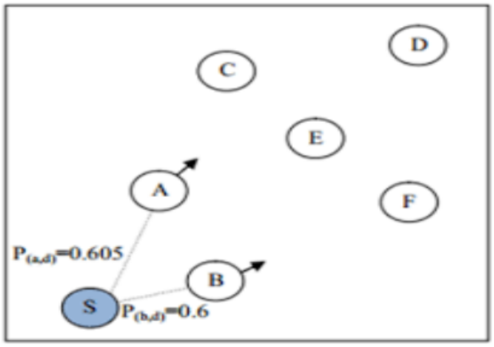
Epidemic Routing Protocol is specifically well-suited for applications that place a premium on message delivery over resource efficiency. Here are several examples:

- Epidemic router can help with communication in disaster zones where infrastructure is damaged for connectivity is limited.
- In sensor networks with intermittent connectivity, it can enable data gathering and distribution.
- Epidemic router can aid in the exchange of messages between vehicles in VANETs, particularly in urban areas.

PRoPHET

PRoPHET also known as Probabilistic routing protocol using History of encounters and transitivity is a replication-based protocol that uses a vector to track a history of encountered nodes. Using these vectors, it attempts to capitalise on the non-randomness of real-world encounters by keeping a set of probabilities for successful delivery to known destinations in the network and replicating messages during opportunistic encounters only if the nodes that does not have the message appears to have a better chance of delivering it.

Each node's delivery predictability is determined using an adaptive algorithm. For each known destination D, the node N holds the delivery predictabilities P (N, D). P (N, D) is presumed to be zero if the mule has not stored a predictability value for a destination. The delivery predictabilities employed by each node are adjusted according to three rules at each opportunistic encounter. The Prophet routing system is especially well-suited for applications that demand consistent message delivery in opportunistic networks, such as Disaster relief communications, sensory data collection, traffic management in VANETs, etc. The below image illustrates the working of prophet where it determines the delivery probabilities of Node A and B.



The benefits of Prophet Routing are:

- Prophet's predictive routing method eliminates unwanted transmissions and network congestion.
- It conserves resources by forwarding communications only when there is a good possibility of delivery.
- It reacts to changing network conditions by updating delivery prediction based on recent encounters.

The Drawbacks of Prophet Routing are:

- Storage Requirements: Prophet requires nodes to save meeting history data, which increases storage requirements.
- Prophet's predicting routing algorithm is more complicated than simpler protocols such as flooding.
- Sensitivity to encounter patterns: The performance is dependent on the regularity of node encounters.

VANETs

A Vehicular Ad Hoc Network (VANET) is a type of disruption Tolerant Network (DTN) distinguished by its intermittent connectivity and high node velocity. Aside from road safety applications designed to prevent casualties, comfort and inventive applications that utilises the power of vehicular networks are becoming increasingly popular. The VANETs are a paradigm shift in the field of intelligent transportation systems. These dynamic networks use wireless communication technology to transform automobiles into networked nodes, providing a mobile infrastructure that allows for real-time information exchange and improves road safety, traffic efficiency, and overall transportation management.

Some of the key characteristics of VANETs are:

- Variable Network Topology: The vehicles are in constant movement because of which VANETs have very dynamic topology, resulting in a network that constantly builds and reforms.
- Intermittent Connectivity: The connectivity between vehicle's is irregular and might be disrupted by obstructions or environmental factors.
- Due to the usage of short-range wireless technology, the communication range of VANETs is often restricted to a few hundred metres.
- Non-infrastructure network: VANETs perform without the need for a fixed infrastructure, allowing interactions even in faraway places.

The main challenges for data dissemination in these types of protocol are:

- Routing messages among highly churned and disconnected nodes.
- Scalability to deal with varying traffic densities.
- High velocity of vehicles.
- Being adaptable to environmental factors like accident, detours, etc.

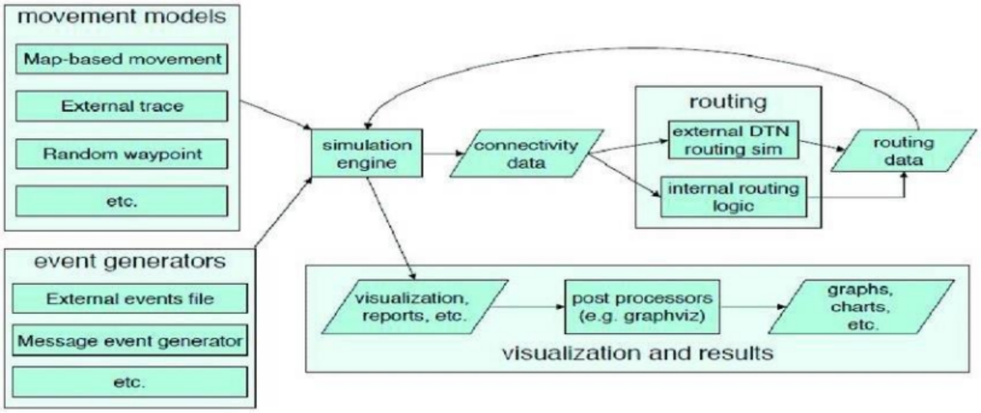
The areas where the VANETs are being deployed as follows:

- Cooperative Collision Avoidance
- Traffic Management and Optimization
- Emergency Notification and Management
- Cooperative Driving and Automated Driving
- Infotainment and Personalization Services
- Virtual Marketplace

VANETs hold tremendous potential to transform the transport location by improving road safety, boosting congestion efficiency, and promoting the development of intelligent transport systems. VANETs are poised to become a vital component of future mobility as research and development advances, influencing the way we travel and interact with transportation infrastructure.

THE ONE SIMULATOR

The Opportunistic Network Environment is a java-based simulator for study in Delay Tolerant Networks and their variants. Aside from allowing users to quickly and easily simulate numerous scenarios, the ONE also gives an easy way to generate statistics from the simulations completed. The ONE simulator can be run on Linux, Windows, or any other Java-enabled platform. The official webpage contains information about the ONE, including how to download and operate it. The ONE simulator's primary features are to represent node movement, inter-node connections, routing, and message handling. Visualisation, reporting, and post-processing are used to collect and analyse results. The results of simulations are typically collected via reports generated by report modules during the simulation execution. Report modules accept events from the simulation engine and provide results based on them (for example, message or distance events). The output may be event logs that are then analysed by external post-processing tools, or it may be aggregate data computed in the simulator. Second, the graphical user interface (GUI) gives a visualisation of the simulation state, including node locations, active contacts, and messages.



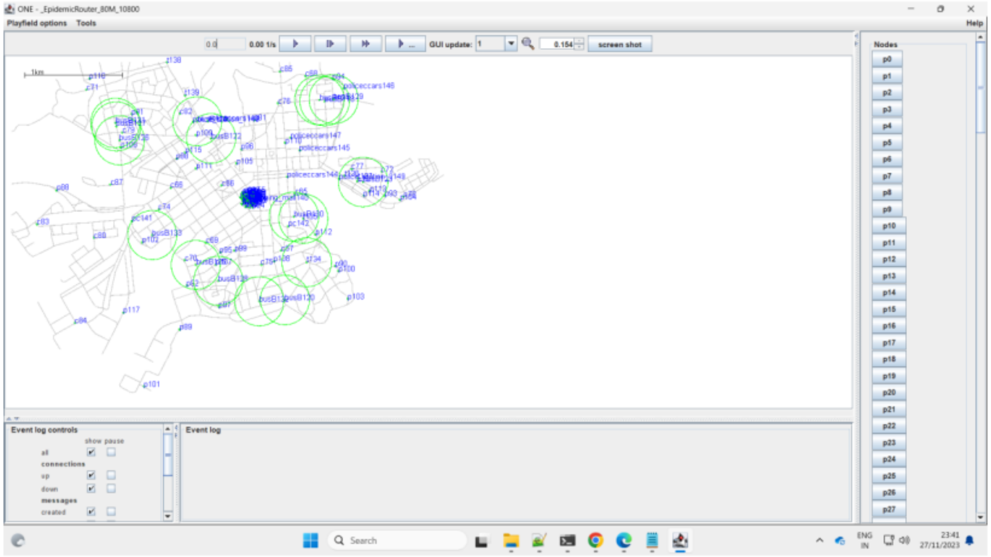
ONE Simulator's Key Features are:

- Mobility Models: ONE includes several mobility models for simulating diverse node movement patterns in OppNets, including Random Waypoint Model, Random Walk Model, Random Direction Model, etc.
- Communication Models: ONE supports a broad spectrum of communication models, including radio propagation, interference, and packet transmission.
- Routing Protocols: For OppNets, ONE can recreate a wide range of routing protocols, including forwarding-based, replication-based, and hybrid protocols.
- Performance Metrics: ONE provides comprehensive measurements for assessing routing methods, such as message delivery rate, end-to-end delay, and network overhead, and latency.
- Visualisation: ONE offers tools for visualising network topology, node movement, and the delivery of messages.

Node Movement capabilities are implemented using Mobility Models. The methods and rules that generate node movement pathways are defined by mobility models. To simulate real-world mobility, Map-based and Working day movement model are implemented. Map-based movement models restrict node movement to path defined in map data. Three map-based models are included in the ONE simulator which are Random map-based movement (MBM), shortest path map-based movement (SPMBM) and Routined map-based movement (RMBM). These movement models are simulated in map data of the Helsinki downtown area. While high level models including RMBM, MBM and SPMBM are easy to comprehend and apply in simulation, they do not produce inter-contact time and contact time distributions that matches real-world traces, especially when the number of nodes in the simulation are minimal. To tackle this Working Day movement model is created to augment the actuality of human node mobility.

The message routing is implemented comparable to movement: the simulator contains a framework for developing routing algorithms and rules, as well as ready implementation of well-know DTN routing protocols included: Direct Delivery (DD), First contact, Spray-and-wait, PRoPHET, MaxProp, and Epidemic.

The ONE can simulation can be visualised via an interactive Graphical user interface where the node's location, network topology, node movement, message transmission, connection links, etc in map. This data can help to research about the OppNets and see them in action through simulation. The map paths are shown which can be zoomed and interactive adjusting of the simulation speed. The GUI of the simulation in real time is as below:



The simulation run time speed can be changed. After completion of simulation, it generates a filtered events of contact and message log. There ONE can produce several event reports like created message, delivered message, adjacency Graphiz, message Graphiz, distance relay, message stat. The Graphiz report can be used to visualize and graph the node connection and node travelled path in network. The message stat report gathers all the statistical report of overall performance like number of messages created, delivery probability, number of messages dropped, etc.

Experimental Scenario and Setup

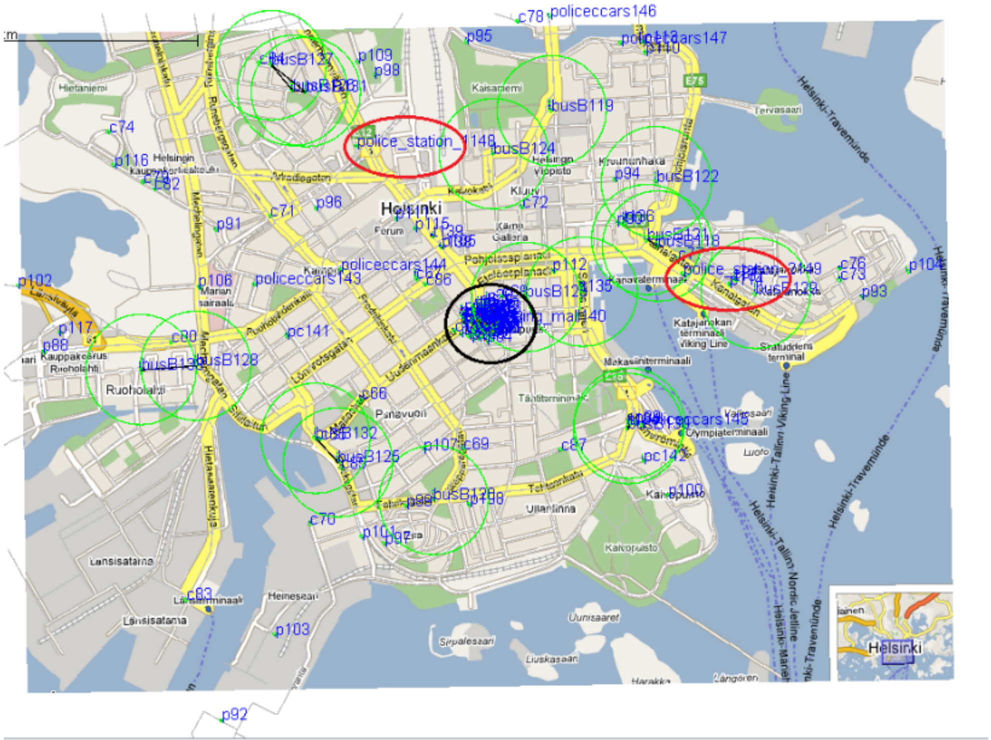
Terrorist attacks pose a major risk to public safety and security. The frequency and severity of these attacks have increased in recent years, making it critical to establish efficient communication tactics for emergency response scenarios. Two interesting ways for message propagation in dynamic and unpredictable networks are the Epidemic and Prophet routing protocols. This report describes an experimental method for evaluating the performance of the Epidemic and Prophet routing protocols in the context of a simulated terrorist attack. The impact of simulation time on protocol performance is examined. Terrorist attacks are complex and take time to develop, and the authorities' response to a terrorist strike is equally essential.

The parameter settings for the scenario as below:

Parameters	Settings
Simulation Time	3 - 12 Hours
Mobility Model	MapBasedMovement ClusterMovement MapRouteMovement StationaryMovement
Number of nodes	150
Node Groups	Peoples inside shopping mall Pedestrians Cars Buses Trams Police Cars Police Stations
Interfaces	Bluetooth and High-Speed interfaces
Number of Source nodes	8
Number of Destination nodes	4
Message size	500kB – 2MB

The above table are the settings use to configure the Epidemic and Prophet router for the scenario. The routers are using Map Based movement model for the mobility. The cluster Movement is used for the people inside the shopping during the attack. There are a total of 150 nodes which are People inside shopping mall, pedestrians, cars, buses, trams, police cars and police stations. All the nodes are using Bluetooth and high-speed interfaces respectively. The destination nodes are police cars and police station. The simulation is runed for a batch of 4 for each router respectively. Each run is for varied simulation time for epidemic and Prophet router.

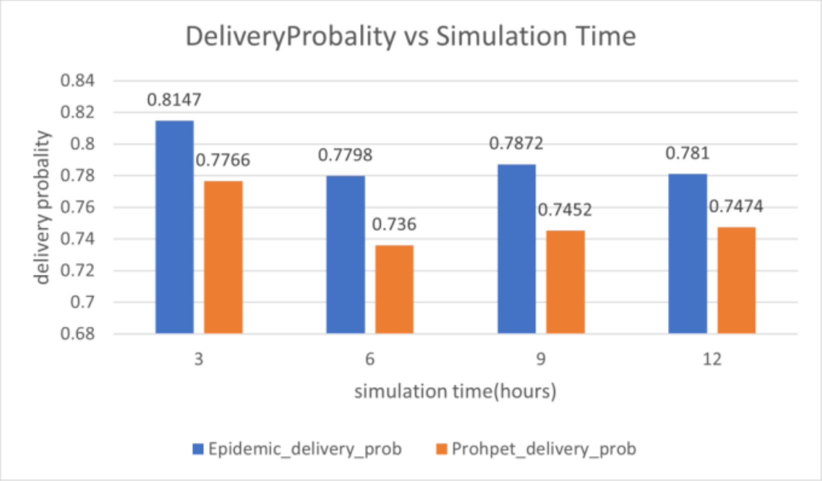
The below overlay map shows the Graphical user interface of the experimental simulation. The clustered nodes on the middle of the map marked in ‘Black circle’ is the area where the shopping mall is and where the terrorist attack is being happened. The ‘Red circle’ marked are the police station where the message is being transmitted. In between the police station and shopping mall the police cars are seen patrolling the area which is also a destination node.



Result and Performance Analysis

The Results generated after the simulation runtime are analysis for the delivery probability, overhead ratio, latency and hop count as below:

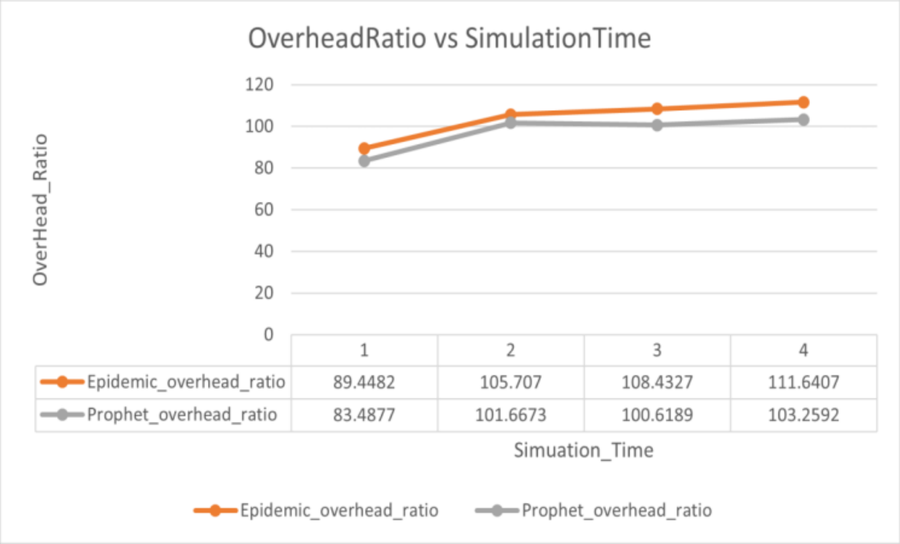
1. Delivery Probability:



Both epidemic and Prophet routing demonstrates promising performance in the simulated terrorist attack. The chart shows that both the router achieves high delivery probability at simulation time of 3 hours, and then experience a temporary drop in delivery probability before increasing again at simulation time 9 and 12 hours. There can be few possible explanations for this behaviour.

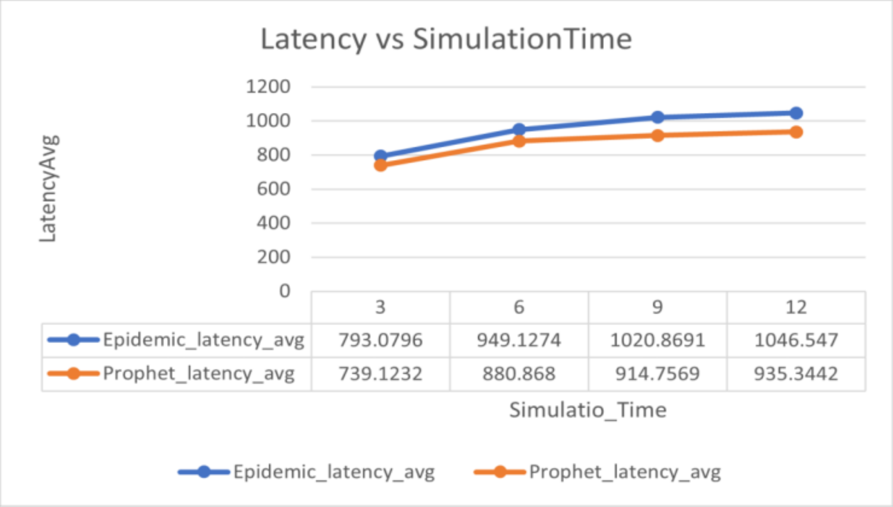
- At initial stage of simulation time 3, the messages are being transmitted through the network for the first time. This leads to high delivery probability, as messages are more likely to reach their destinations when there are fewer messages in the network.
- As the simulation progresses the network becomes congested because of the increasing messages. This leads to slight decrease in delivery probability as the message are dropped due to congestion.

2. Overhead ratio:



The Epidemic and Prophet performs well in the scenario with overhead ratio ranging from 89.4482 to 111.6407 and 83.4877 to 103.2592 respectively. However, it is important to note that the overhead ratio for both protocols increase with increasing simulation time. This is because both the protocols need to forward more messages with increasing simulation time. Epidemic routing exhibits a higher overhead ratio than prophet for all the simulations time because epidemic routing floods all newly received messages to neighbouring nodes. This mechanism of flooding cause significant amount of additional traffic and high message traffic volume. Prophet achieves a lower overhead ratio than epidemic routing is by selective forwarding messages based on estimated delivery likelihood. This helps to reduce amount of additional traffic generated by protocol. However, the overhead ratio may vary depending on the network topologies for both routing protocols.

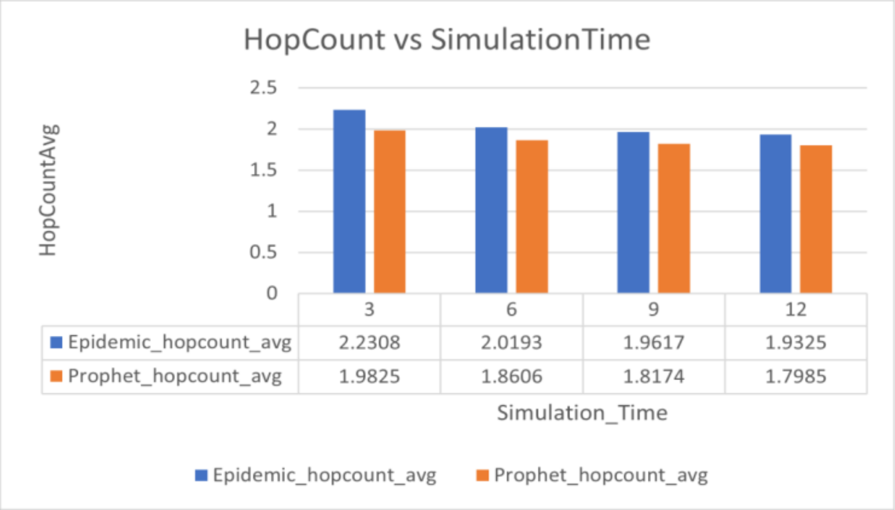
3. Latency:



	3	6	9	12
Epidemic_latency_avg	793.0796	949.1274	1020.8691	1046.547
Prophet_latency_avg	739.1232	880.868	914.7569	935.3442

The average latency of epidemic and prophet can be seen values ranging from 793.0796 to 1046.547 and 739.1232 to 935.3442 respectively. There is increase in average latency with increase in simulation time. Epidemic routing exhibits higher average latency than prophet routing for all simulation because epidemic routing floods the messages through longer paths to reach their destination and generates significant amount of traffic whereas prophet uses probabilistic approach to message forwarding. This approach allows prophet routing to select shorter paths to forward messages and it generates less additional traffic than epidemic routing, which also helps to reduce latency.

4. Hop Count:



	3	6	9	12
Epidemic_hopcount_avg	2.2308	2.0193	1.9617	1.9325
Prophet_hopcount_avg	1.9825	1.8606	1.8174	1.7985

The effect of simulation time on hop count average varies between protocols. The average hop count increases linearly with simulation time in Epidemic Routing. This is since Epidemic Routing may send messages over longer paths to their destinations, and the average path length may increase with simulation duration. The average hop count for Prophet Routing falls logarithmically with simulation time. Because Prophet Routing employs a probabilistic approach to message forwarding, it chooses shorter paths as the network topology and message propagation patterns become more understood.

CONCLUSION

The Epidemic and Prophet routing protocol are both viable options for routing in terrorist attack scenario, with acceptable performance metrics. The high delivery probability observed at simulation time - 3 hours suggest that during the early stages of an attack epidemic routing can be useful for bombarding the messages throughout the network so that it can alert the required destinations. The best choice of protocol will depend on the specific requirements of the application, such as the desired delivery probability, latency, overhead ratio, and hop count.

- If delivery probability is the primary importance, then epidemic routing is best choice.
- If a balance between delivery probability, overhead, latency, hop count, and resilience is required, then prophet routing is a better option.
- If low overhead, latency and hop count is critical, then prophet may be better choice.

It is also important to consider the impact of network topology and message traffic pattern on protocols performance when choosing a routing protocol for the scenario. When selecting a routing protocol for a terrorist attack scenario, it is important to keep the following safety criteria in mind:

- Avoiding the utilisation of protocols that can result in a considerable increase in traffic. This can contribute to increased network congestion and latency, making important message delivery more challenging.
- Selecting the protocols that are resistant to network outages. This will aid in the delivery of communications even if the network is destroyed or corrupted.
- Considering how simulation time affects protocol performance. Protocols that scale well to big networks and huge message traffic volumes may be a preferable choice if the simulation time is long.

REFERENCES

- Delay Tolerant Networks: Protocols and Applications by Athanasios V. Vasilakos (Editor).
- Delay and Disruption Tolerant Networks: Interplanetary and Earth-Bound -- Architecture, Protocols, and Applications by Pereira da Silva Aloizio (Editor), Scott Burleigh (Editor), Katia Obraczka (Editor).
- Advanced Computer Networks Lecture learning material by Dr Milena Radenkovic.
- Opportunistic Networks: An Overview" by P. Jacquet, P. Muhlethaler, A. Gallais, and P. Wirz.
- Performance Evaluation of Routing Protocols for Opportunistic Networks" by M. Zorzi and R. Meneghello.
- A Survey on Routing Protocols for Opportunistic Networks" by J. Cao, G. Zhou, Z. Yang, and T. Li.
- Routing in Opportunistic Networks: A Survey" by I. F. Akyildiz, D. S. M. Bandyopadhyay, S. Subramanian, and Y. Sankarasubramaniam.
- Delay-Tolerant Networks (DTNs): An Overview" by K. Fall, S. Farrell, and A. S. Karn.
- Energy-Efficient Routing Protocols for Opportunistic Networks: A Survey" by X. Luo, J. Huang, and Q. Li.
- Cao, Y., Zhang, Z., & Yang, G. (2010). A survey on replication-based routing protocols for delay-tolerant networks. IEEE Communications Surveys and Tutorials.
- Zhu, Y., Li, B., & Lai, T. H. (2012). A survey of replication-based routing protocols for delay-tolerant networks. IEEE Transactions on Vehicular Technology.
- Zorzi, M., & Meneghello, R. (2011). Delay-tolerant networking: An overview. Proceedings of the IEEE.

ACN_Report

ORIGINALITY REPORT

13%	4%	12%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Keränen, Ari, Teemu Kärkkäinen, and Jörg Ott. "Simulating Mobility and DTNs with the ONE (Invited Paper)", Journal of Communications, 2010. Publication	2%
2	Submitted to National Institute of Technology, Patna Student Paper	1%
3	Spyropoulos, . "Message Dissemination in Vehicular Networks", Wireless Networks and Mobile Communications, 2011. Publication	1%
4	Submitted to Queen Mary and Westfield College Student Paper	1%
5	Computer Communications and Networks, 2016. Publication	1%
6	Submitted to Issaquah High School Student Paper	1%

7	Submitted to University of Nottingham Student Paper	1 %
8	Kevin Bylykbashi, Evjola Spaho, Leonard Barolli, Fatos Xhafa. "Impact of node density and TTL in vehicular delay tolerant networks: performance comparison of different routing protocols", International Journal of Space-Based and Situated Computing, 2017 Publication	1 %
9	www.amazon.com Internet Source	1 %
10	Ramchandra S. Mangrulkar, Mohammad Atique. "chapter 6 Direction-Aware Routing Protocol for Delay-Tolerant Network", IGI Global, 2017 Publication	<1 %
11	Submitted to London Design Engineering UTC Student Paper	<1 %
12	dokumen.pub Internet Source	<1 %
13	m.alibris.com Internet Source	<1 %
14	"Advanced Network Technologies and Intelligent Computing", Springer Science and Business Media LLC, 2023 Publication	<1 %

15	aaltodoc.aalto.fi Internet Source	<1 %
16	Evjola Spaho, Leonard Barolli, Vladi Kolici, Algenti Lala. "Performance Evaluation of Different Routing Protocols in a Vehicular Delay Tolerant Network", 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015 Publication	<1 %
17	G. Anderson, L. Urbano, G. Naik, D. Dorsey et al. "A secure wireless agent-based testbed", Second IEEE International Information Assurance Workshop, 2004. Proceedings., 2004 Publication	<1 %
18	Lecture Notes in Electrical Engineering, 2016. Publication	<1 %
19	Qaisar Ayub. "Adaptive message size routing strategy for delay tolerant network", Scientific Research and Essays, 2012 Publication	<1 %
20	www.ijrte.org Internet Source	<1 %
21	Etienne C. R. de Oliveira. "NECTAR", Proceedings of the 2009 ACM symposium on Applied Computing - SAC 09 SAC 09, 2009	<1 %

	Publication	
22	Jörg Ott. "Working day movement model", Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models - MobilityModels 08 MobilityModels 08, 2008 Publication	<1 %
23	en.wikipedia.org Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		