future internet

MDPI

Article

A Secure Opportunistic Network with Efficient Routing for Enhanced Efficiency and Sustainability

Ayman Khalil [1,*,†] and **Besma Zeddini** [2,†]

[1] School of Business, Lebanese American University, Beirut 1102 2801, Lebanon
[2] SATIE Laboratory CNRS–UMR 8029, CY Tech, CY Cergy Paris University, 95000 Cergy, France; besma.zeddini@cyu.fr
* Correspondence: ayman.khalil02@lau.edu.lb
† These authors contributed equally to this work.

Abstract: The intersection of cybersecurity and opportunistic networks has ushered in a new era of innovation in the realm of wireless communications. In an increasingly interconnected world, where seamless data exchange is pivotal for both individual users and organizations, the need for efficient, reliable, and sustainable networking solutions has never been more pressing. Opportunistic networks, characterized by intermittent connectivity and dynamic network conditions, present unique challenges that necessitate innovative approaches for optimal performance and sustainability. This paper introduces a groundbreaking paradigm that integrates the principles of cybersecurity with opportunistic networks. At its core, this study presents a novel routing protocol meticulously designed to significantly outperform existing solutions concerning key metrics such as delivery probability, overhead ratio, and communication delay. Leveraging cybersecurity's inherent strengths, our protocol not only fortifies the network's security posture but also provides a foundation for enhancing efficiency and sustainability in opportunistic networks. The overarching goal of this paper is to address the inherent limitations of conventional opportunistic network protocols. By proposing an innovative routing protocol, we aim to optimize data delivery, minimize overhead, and reduce communication latency. These objectives are crucial for ensuring seamless and timely information exchange, especially in scenarios where traditional networking infrastructures fall short. By large-scale simulations, the new model proves its effectiveness in the different scenarios, especially in terms of message delivery probability, while ensuring reasonable overhead and latency.

Keywords: cybersecurity; opportunistic networks; efficiency; sustainability; delivery probability; overhead ratio; latency; trust computation; Proof-of-Trust (PoT)

check for updates

Citation: Khalil, A.; Zeddini, B. A Secure Opportunistic Network with Efficient Routing for Enhanced Efficiency and Sustainability. *Future Internet* **2024**, *16*, 56. https://doi.org/10.3390/fi16020056

Academic Editor: Sachin Sharma

Received: 8 January 2024
Revised: 2 February 2024
Accepted: 6 February 2024
Published: 8 February 2024

1. Introduction

In the ever-evolving landscape of wireless communications, characterized by a complex interplay of technological advancements, the convergence of cybersecurity and opportunistic networks (OppNets) emerges as a catalyst for a profound paradigm shift. This convergence signifies more than a mere juxtaposition of innovative concepts; it heralds the onset of a new era marked by transformative innovation and heightened potential within the wireless communication domain. In an age where the seamless exchange of data assumes unparalleled importance for individuals and organizations alike, the imperative for networking solutions transcends mere efficiency and reliability, extending into the realms of sustainability and long-term viability.

The backdrop of opportunistic networks, defined by their intermittent connectivity and dynamic environmental conditions, presents a distinct set of challenges that necessitate solutions beyond conventional approaches. This paper serves as a vanguard, introducing a groundbreaking paradigm that intricately intertwines the fundamental principles of cybersecurity and some concepts related to blockchain technology with the complex fabric of opportunistic networks. At the core of this exploration lies the revelation of a meticulously crafted routing protocol, a novel entity designed with the explicit intention of not merely surpassing current solutions but redefining benchmarks in key performance metrics. These metrics not only encompass the traditional domains of delivery probability, overhead ratio, and communication delay but also extend into the broader landscape of holistic network efficiency and sustainability.

The added value of our proposed protocol lies in its adept use of the inherent strengths embedded within the cybersecurity protocols. Beyond the conventional fortification of the network's security posture, our protocol lays a foundation for a holistic augmentation of efficiency and sustainability within opportunistic networks. It represents not merely an incremental enhancement but a transformative leap forward, addressing the intricacies of data exchange in a dynamic and unpredictable environment. As the digital realm increasingly intertwines with our daily lives, the outcomes of this study hold the promise of redefining the standards by which wireless communication networks operate, ushering in a new era where innovation and sustainability become inseparable facets of the technological scenery.

Furthermore, to ensure a high security level in distributed networks like OppNets, this study incorporates aspects proposed in blockchain technology, namely the trust value computation, the consensus algorithm, and the block generation process to establish a preliminary connection to blockchain technology, demonstrating its relevance and significance. The adoption of these specific components aligns with the fundamental principles and functionalities inherent in blockchain systems.

This paper is organized into six main sections that lay the foundation by highlighting the convergence of cybersecurity and blockchain with opportunistic networks, underscoring the imperative for reliable and sustainable networking solutions. Sections 1–4 delve into fundamental aspects, exploring challenges in routing within opportunistic networks and examining existing protocols integrated with cybersecurity. Section 5 introduces the proposed solution, detailing a two-layered organizational structure. The first layer presents the FT-OLSR protocol based on aspects implemented in blockchain, emphasizing fuzzy logic for trust evaluation and introducing the Proof-of-Trust consensus algorithm. This section also outlines the block generation process for permanently isolating malicious nodes. The second layer focuses on the proposed routing protocol specifically designed for opportunistic networks, elucidating protocol requirements, initialization, exchange of deliverable messages, procedures for non-deliverable messages, sending of accepted messages, and the criteria for message acceptance. Finally, the performance evaluation section uses the ONE simulator to assess the proposed model's performance in various simulation scenarios, including message and user numbers, transmission speed, buffer size, and the number of copies. Results demonstrate the model's effectiveness with high delivery probability, low overhead, and reduced latency, comparing these performances against established routing algorithms. The paper concludes by summarizing key findings and discussing the implications of the proposed model for enhancing efficiency and sustainability in wireless communication systems, outlining potential avenues for future research and development.

2. Challenges in Cybersecurity-Driven Opportunistic Networks

The domain of wireless communication is undergoing a transformative evolution, and at the forefront of this technological revolution stands blockchain, a groundbreaking concept introduced by Nakamoto in 2008 [1]. Anchored by key components such as consensus algorithms and cryptographic techniques, it guarantees tamper-proof data storage and facilitates secure transactions. This section delves into the intricacies of cybersecurity and blockchain technology, unraveling its multifaceted components and shedding light on its profound implications for OppNets. Blockchain serves as the bedrock for secure and auditable data sharing within the context of OppNets [2]. Some studies have investigated the current landscape of cybersecurity training for critical infrastructure protection, focusing on aviation, energy, and nuclear sectors [3]. In the dynamic realm of OppNets, decentralized identity solutions emerge as guardians of secure and privacy-preserving identification [4]. Since OppNets, characterized by high mobility and low density, pose security challenges due to limited power and susceptibility to attacks, trust, rooted in human interaction, plays a crucial role in securing OppNets. This can explore security approaches and techniques to enhance the security levels of OppNets [5].

One study investigated several deployment types for OppNets; complex network properties (average shortest distance, degree distribution, clustering coefficients) were analyzed, and the robustness against wormhole attacks was studied. Results showed wormhole severity depends on node attributes, causing notable impacts on the average shortest distance in specific scenarios. Additionally, security in selective OppNets is observed to be comparatively better than in open OppNets [6]. Moreover, in [7], the authors emphasize the growing need for safeguarding personal devices against security and privacy attacks, with manufacturers increasingly relying on Trusted Execution Environments (TEEs), especially ARM TrustZone in smartphones. Despite TEEs' widespread use, the paper reveals its vulnerability to diverse attacks and provides a comprehensive analysis of existing weaknesses, drawing attention to design flaws. It concludes with effective countermeasures and outlines compelling challenges and open issues, aiming to raise awareness among stakeholders interested in TEE technology. The authors in [8] underscore the growing significance of security in citizens' daily lives, especially with the proliferation of IoT devices, altering the traditional single-device connection model. They highlight the increased attack vectors for potential attackers, examining the concatenation of attacks on various communication protocols (WiFi, Bluetooth LE, GPS, 433 Mhz, and NFC) in a domestic setting. The paper offers a thorough analysis, identifying weaknesses in these protocols, and provides insights into the attacking procedure, along with relevant tips and countermeasures.

However, there are still many challenges for cybersecurity and blockchain-driven OppNet systems, and the following list details some of them:

- *Scalability and Latency:* Challenges such as scalability and latency become more pronounced within the unique context of OppNets [9]. Ongoing research endeavors focus on developing lightweight consensus mechanisms and off-chain solutions, aiming to alleviate these challenges and ensure the seamless functioning of blockchain-driven OppNets [10].
- *Security and Privacy Concerns:* Blockchain, though inherently secure, demands tailored solutions to address the nuanced privacy concerns that arise in the OppNet environment [11]. Cutting-edge cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, are enlisted to fortify privacy measures and safeguard sensitive information exchanged within the network [12].
- *Energy Efficiency:* Acknowledging the resource-intensive nature of blockchain operations, the research community is actively engaged in optimizing consensus algorithms and transaction validation processes within the OppNet framework [13]. The objective is to strike a balance between the security features of blockchain and the imperative of energy efficiency, thereby ensuring sustainable network operations [14]. This dual focus seeks to harness the potential of blockchain, while mitigating its environmental impact, fostering a harmonious integration within the OppNet ecosystem.

3. Routing in Opportunistic Networks

Ad hoc networks traditionally rely on continuous end-to-end paths between nodes for reliable data communication, necessitating high node density and adherence to conventional routing protocols [15]. However, in scenarios where such paths are intermittent or non-existent, conventional ad hoc networks face operational inefficiencies. Addressing this challenge, delay-tolerant networks (DTNs) offer a viable solution for communication in unstable networks, with a specific emphasis on opportunistic networks (OppNets) [16]. An OppNet strategically leverages every potential connection opportunity, overcoming the limitations posed by incomplete paths and the constant mobility of nodes. Notably, an OppNet diverges from TCP/IP-based protocols and adopts a unique "store–carry–forward" communication topology [17]. The store–carry–forward approach operates as a "hop-by-hop" technique, involving intermediate nodes to relay messages from source to destination. Messages are temporarily stored in a node's buffer until it encounters another node [18,19]. Upon contact, the message is transferred to the intermediate node, which then carries and forwards it to other nodes within the network. This iterative process continues until the message reaches its destination. However, due to the constant relocation of devices, establishing contact may take a considerable amount of time, thereby influencing OppNet performance based on node density and mobility. While the store–carry–forward paradigm is integral, it introduces a trade-off between message delivery probability and delivery delay. Routing protocols must carefully consider the number of copies distributed in the network and the selection of nodes for replication or forwarding, necessitating intelligent decision making based solely on local information at nodes. Existing routing algorithms for opportunistic networks fall into two principal classes: oblivious algorithms and contact-history-based algorithms [20]. Oblivious algorithms encompass direct delivery and Epidemic forwarding, with direct delivery exhibiting the worst delay and delivery probability. In contrast, Epidemic forwarding results in resource wastage. Contact-history-based algorithms, including Prophet, Fresh, and Meed, use nodes' encounter history to inform forwarding decisions. This study specifically delves into a comparative analysis of Epidemic, Prophet, Fresh, and Spray and Wait routing algorithms. The primary goal is to present an in-depth examination of their respective advantages and disadvantages while aiming to propose a novel, simple, and scalable routing model [21–23]. Epidemic and Prophet algorithms entail pairwise information exchange, with Prophet additionally considering delivery predictability. Spray and Wait, a more intricate algorithm, strategically restricts the number of message copies disseminated within the network through a two-phase process: Spray, where a finite number of copies are initially forwarded, and Wait, where nodes carrying copies patiently await until reaching the destination.

4. Routing Protocols Integrated with Cybersecurity and Blockchain Technologies

In this section, we explore various routing protocols that are seamlessly integrated with cybersecurity and blockchain technologies, introducing enhanced capabilities to optimize communication within OppNets. Each protocol harnesses unique features to address specific challenges and improve the efficiency of message delivery.

a. *Blockchain-Assisted Epidemic Routing:* This approach uses a decentralized ledger to optimize message replication strategies. Smart contracts play a crucial role in governing the dissemination process, effectively reducing redundancy and improving delivery rates [23].

b. *Proof-of-Delivery (PoD) Routing:* Leveraging the transparency of blockchain, PoD routing ensures reliable message delivery. Through smart contracts, successful message reception is validated, triggering incentives for relaying nodes and thereby enhancing overall message delivery efficiency [24].

c. *Consensus-Based Routing with Blockchain:* Consensus-based routing algorithms incorporate blockchain consensus mechanisms, such as Proof of Work and Proof of Stake, to validate routing decisions. The immutable nature of blockchain records enhances trust in 251 consensus outcomes, ensuring both secure and efficient message forwarding [25].

d. *Blockchain-Powered Predictive Routing:* Predictive routing algorithms leverage historical encounter data stored on the blockchain to predict future node interactions. The execution of smart contracts facilitates the implementation of predictive algorithms, ultimately enhancing the accuracy of encounter-based routing strategies [26].

5. Challenges and Opportunities

The integration of cybersecurity and blockchain technology with OppNets brings forth both challenges and opportunities that require attention for the improvement of efficiency, reliability, and security in data exchange.

Scalability: Blockchain's inherent scalability challenges pose issues in resource-constrained OppNets. Research focuses on lightweight consensus algorithms and off-chain solutions to enhance scalability, while maintaining security [27].

Security and Privacy: Ensuring secure and private transactions, while preserving blockchain's transparency is a significant challenge. Advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, are explored to enhance security and privacy in blockchain-integrated OppNets [28].

Incentive Mechanisms: Designing efficient incentive mechanisms using blockchain is crucial for encouraging active participation in routing. Smart-contract-based incentive models, combined with game-theoretic approaches, are proposed to encourage cooperation among nodes [29].

In [30], the authors address the challenges faced in OppNets, provide insights into protocol implementation, and conduct evaluations. By examining these aspects, the paper offers a comprehensive understanding of the complexities involved in routing within OppNets, shedding light on practical implementations and their evaluations.

The authors in [31] propose a novel OppNet routing method designed for campus environments. Their approach is grounded in an improved Markov model, a probabilistic system that enables a more efficient and context-aware routing strategy. By leveraging this model, the paper introduces an innovative routing method tailored for campus-based OppNets, enhancing the network's reliability and performance. In [32], a new routing algorithm is proposed for sparse OppNets. The algorithm's foundation lies in considering node intimacy, highlighting the importance of social aspects in opportunistic networking scenarios. By incorporating this element, the proposed algorithm optimizes routing decisions, addressing the challenges posed by sparse connectivity. The paper's findings contribute to enhancing the efficiency and effectiveness of OppNet communication in scenarios where nodes are sparsely distributed.

As a result, the integration of blockchain technology with innovative routing protocols holds immense promise for enhancing the efficiency, reliability, and security of data exchange in OppNets. While challenges such as scalability, security, and incentive mechanisms persist, ongoing research efforts are focused on addressing these issues.

6. Our Approach: Proposed Model

In our approach, we introduce a proposed model that operates on a two-layer protocol framework, each layer serving a distinct yet interconnected purpose. At its foundational stratum, the first layer is intricately crafted for the establishment of a secure protocol. This layer not only capitalizes on the decentralized and tamper-proof nature of blockchain but also acts as the bedrock for elevating the overall reliability of the proposed model. Concurrently, the second layer of the framework is tailored for the seamless execution and implementation of the novel routing protocol. By encapsulating these two layers, the model aspires to create a harmonious synergy, blending the security advantages of blockchain with the dynamic functionality of the routing protocol to address the unique challenges and requirements of OppNets.

6.1. Layer 1: FT-OLSR Protocol

The Fuzzy-Logic-based Trusted Optimized Link State Routing (FT-OLSR), a detection method designed to identify blackhole nodes, was introduced in [33]. This technique involves examining various communication links to identify nodes that drop HELLO and TC messages [34]. Once a blackhole node is pinpointed, any messages received from it are disregarded and not processed. Consequently, these nodes are disqualified.

The FT-OLSR protocol operates on a fuzzy logic framework [35]. Given the context of cybersecurity, precise trust computation is crucial. Therefore, we opted for a fuzzy logic approach to assess trust levels. Fuzzy logic offers distinct advantages in this context:

- It allows for more precise trust computation, enhancing our ability to assess trust levels accurately.
- By leveraging fuzzy logic, we can consider nuanced factors that might not fit well into traditional binary trust models, thus providing a more comprehensive evaluation of trustworthiness.

The development of a reliable scheme for detecting and isolating misbehaving OppNets necessitates the achievement of several key objectives [35,36]:

Distributed Management: Trust evaluation of nodes must occur in a decentralized manner, meaning that trust values should be calculated and evaluated at the individual node level, ensuring mutual assessment among nodes.

Reliability and Availability Requirements: Each node should maintain a trust table to evaluate neighboring nodes, enabling the selection of optimal nodes for seamless data transfer.

Security and Privacy: Enhanced information exchange in the network raises concerns about user vulnerability and potential exploitation by attackers. Without cooperation among OppNet components, attackers can target various nodes repeatedly. Protocols must incorporate trust requirements to mitigate these security risks.

Scalability: Nodes face challenges in management and limited bandwidth. In this resource-constrained environment, it is advisable to adopt a simpler method with a certain level of security, rather than a more complex approach that demands intricate mechanisms and consumes additional resources. Prioritizing simplicity ensures a practical balance between security and resource conservation. To achieve our objectives, we isolated malicious nodes detected by FT-OLSR. By enhancing cooperation among components in a dynamic environment with limited resources, we streamlined the process, eliminating the need for intricate calculations. The proposed system, illustrated in Figure 1, can be segmented into components tailored to the specific requirements of OppNets.

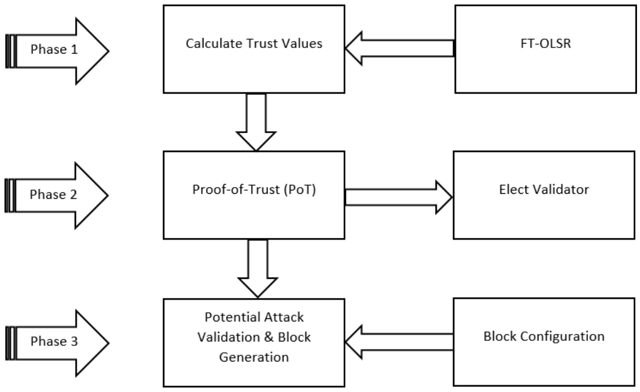


Figure 1. Proposed FT-OLSR scheme.

Trust Value Computation

In the FT-OLSR protocol, the trustworthiness assessment of neighboring nodes relies on the analysis of exchanged control messages, namely HELLO and TC. If a node's trust value equals or exceeds the predefined trust threshold, it qualifies as a potential candidate for transmitting packets. To accommodate the newly introduced modules, modifications will be made to the neighbor list. This enhanced list will not only contain neighbor IDs but also include the count of messages received from each neighbor and their respective trust levels. These parameters will be dynamically updated each time HELLO or TC messages are received. Our proposed detection system operates on fuzzy logic, comprising three core modules: the Extraction of Fuzzy-Based Parameters, the Fuzzy Inference Module, and the Fuzzy Decision Module. This approach allows for a nuanced evaluation of trust values, enabling accurate identification of suitable MPR candidates and enhancing the overall reliability of the FT-OLSR protocol.

Consensus Algorithm (Proof of Trust)

In the context of our study, the trust value assumes a pivotal role in identifying nodes to be isolated and subsequently incorporated into blocks. Given the decentralized nature of OppNets and the absence of centralized management, the consensus process must occur at the individual node level. While various consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), are prevalent in the literature, neither PoW, reliant on computational capacity, nor PoS, favoring the wealthiest node, is ideally suited for OppNets with their inherent limitations in computational resources. In our work, we introduce the Proof-of-Trust (PoT) consensus algorithm tailored specifically for highly dynamic and resource-constrained environments. In the PoT algorithm, the node with the highest trust value assumes the role of the validator. For a node to be eligible as a validator, its trust value must surpass a predetermined threshold, the smallest value determined through multiple simulations, signifying the minimum level of trustworthiness.

Block Generation Process

In the event of detecting a malicious node via FT-OLSR, it is permanently isolated from communication by incorporating its details into the shared blockchain. The detection process relies on potential attacker messages sent by nodes to validators following an attack incident. However, there exists a possibility of erroneous transmission, where a node might mistakenly include the information of a reliable node in its potential attacker message. To address this concern, an attack claim transaction necessitates confirmation by neighbors before a validator can generate a block based on the claim. To prevent potential attackers from isolating trustworthy nodes by maliciously sending potential attacker messages, a validation mechanism is in place. If the majority of neighboring nodes include the same node's information in their HELLO messages, the transaction is considered validated. Once a transaction is validated, determined by the number of nodes voting for it, the validator generates and disseminates an encrypted block containing the attacker's information.

6.2. Layer 2: Proposed Routing Protocol

In a real OppNet involving human activity where mobile nodes are carried by humans, the mobility is not truly random. Human activity imposes patterns on the mobility that has a characteristic time interval, depending on what the human is doing. The proposed routing approach partially depends on the probability that the current node will encounter the destination node based on the last meeting time. Moreover, the new model depends on an acknowledgment table to remove the acknowledged messages from the network. To overcome high overhead, the protocol efficiently detects which messages should be deleted from the buffer upon congestion.

6.2.1. Protocol Requirements

The routing protocol requires the presence of the two tables shown in Figure 2 to be present in the memory of each mobile node.

The "Acked Messages table" is used to save the IDs of all messages that are acknowledged, their acknowledgment time, and their time to live (TTL). The flowchart presented in Figure 3 illustrates the periodic process ensured by the table.

To prevent the table from becoming too large, a periodic check on the table tests whether the time since the message was acknowledged is greater or equal to the TTL; if true, the message will be dropped from the table. This means that all the copies of the message are dropped from the network due to their TTL expiration. The second table, "Hosts table", saves the ID of each node encountered by the current node and the last time those nodes met. Another requirement for the algorithm is the addition of a new integer header, "Number of Copies", and a new entry, "Time Received", in each message. The "Number of Copies" header is used to control the number of messages spread in the network to reduce the overhead and increase the delivery probability. Figure 4 shows the message overhead where the dashed parts represent the new added fields.

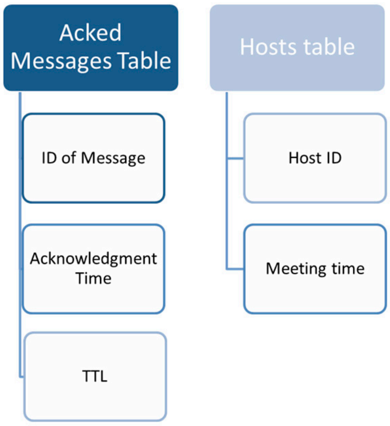


Figure 2. Schematic of two required tables.

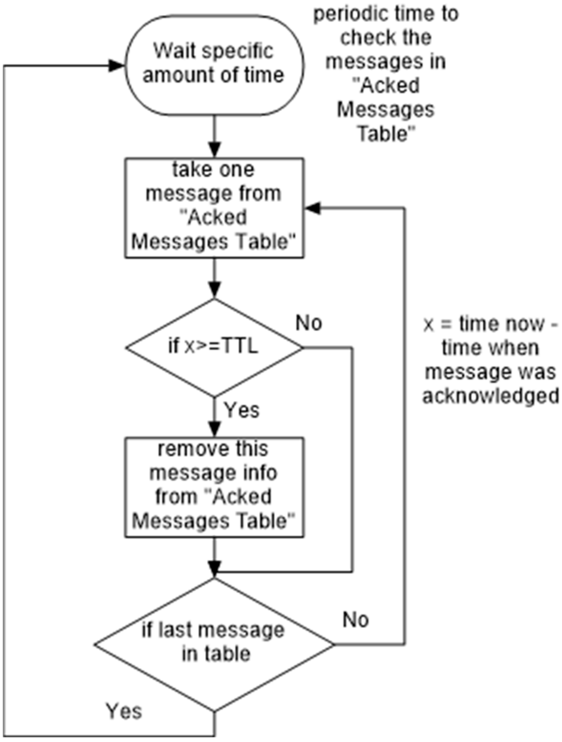
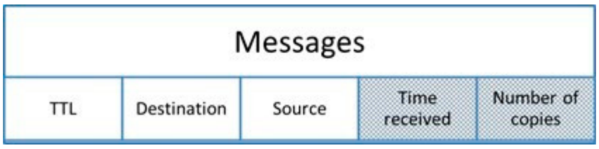

Wait specific amount of time
periodic time to check the messages in "Acked Messages Table"
take one message from "Acked Messages Table"
if x>=TTL
No
Yes
x = time now - time when message was acknowledged
remove this message info from "Acked Messages Table"
if last message in table
No
Yes

Figure 3. Acked Messages table flowchart.



Messages

TTL	Destination	Source	Time received	Number of copies

Figure 4. Message overhead.

6.2.2. Protocol Phases

The operational framework of the proposed model unfolds through a structured sequence of five essential phases, each designed and intricately interconnected. These phases, presented in the remainder of this section, delineate the systematic progression of the protocol, outlining key stages that contribute to the overall functionality and efficacy of the model.

- ***Phase 1: Initialization Phase***

When the connection between two nodes is established, this phase starts. It aims to delete all the acknowledged messages from the buffer of both connecting nodes and update their meeting time. Deleting acknowledged messages will reduce the dropping of undelivered messages from the buffer to make room for new received messages (as we will see in phase 5) and to avoid useless transfer of messages that are already delivered, thus preventing wastage of transmitting and processing time and energy on already delivered messages. As shown in Figure 5, when the connection is established, both nodes exchange their "Acked Messages tables", add to their tables the delivered messages present in the received "Acked Messages table", and then delete the delivered messages that are present in their own buffer. Note that saving the IDs of delivered messages in a table and exchanging this table when any connection is established is much more efficient than flooding the network with an "Ack" message for each delivered message. This will reduce the overhead, the buffer overflow, and the energy. Moreover, the node that has sent the message will be able to detect whether the message is delivered to the destination using this acknowledgment table. After deleting acknowledged messages, both nodes test whether the other node is present in their "Hosts table"; if so, they update their meeting time, otherwise the node will be added to the table as well as its meeting time. Once this phase is over, the routing protocol will start the next phase.

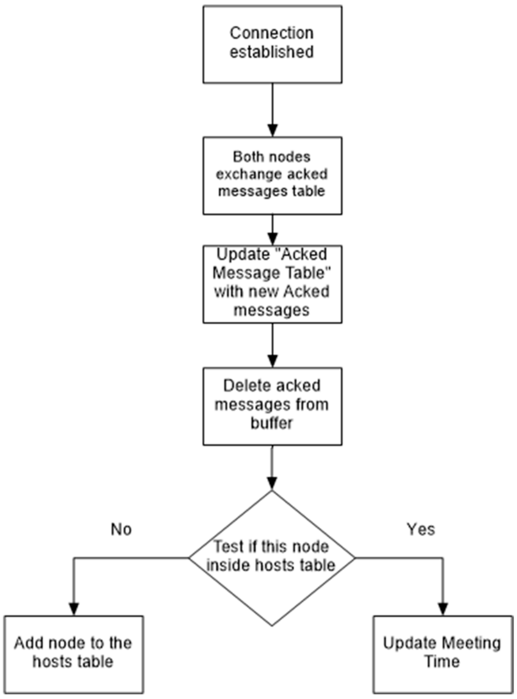

Connection established
Both nodes exchange acked messages table
Update "Acked Message Table" with new Acked messages
Delete acked messages from buffer
Test if this node inside hosts table
No
Yes
Add node to the hosts table
Update Meeting Time

Figure 5. Phase 1 functionality.

- ***Phase 2: Exchange Deliverables Phase***

The main role of this phase is to ensure that messages whose destination is the connected node (deliverable messages) are exchanged first. As the buffer contains deliverable messages, and other messages whose final recipients are other nodes in the network, it is important to first exchange the deliverable messages and then start trying to send other messages. This will ensure that the nodes with low power will act as direct delivery nodes (this is shown in phase 5), and if the connection between the nodes is closed suddenly, due to the speed of the nodes or any other malfunctioning, the deliverable messages will be delivered, thus increasing the delivery probability. As shown in Figure 6, the deliverable messages are accumulated at both nodes and then exchanged. Each node updates its "Acked Messages table" with the newly delivered messages, and then, if the energy is greater than the threshold energy, the routing protocol moves to the next phase, which illustrates the procedure to deal with other messages in the buffer. Otherwise, the connection is closed to preserve the node's energy, and thus the node acts as a direct delivery node.

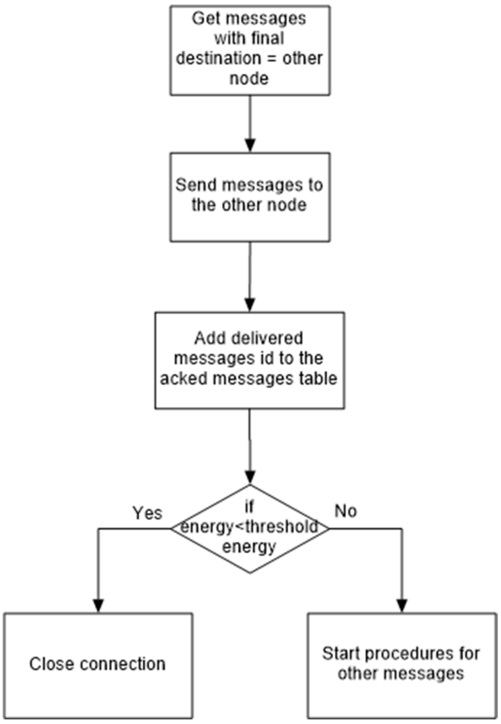

Get messages with final destination = other node
Send messages to the other node
Add delivered messages id to the acked messages table
if energy<threshold energy
Yes
No
Close connection
Start procedures for other messages

Figure 6. Phase 2 functionality.

- ***Phase 3: Procedures for Non-Deliverable Messages***

This phase is considered as the core phase of the new routing protocol. Note that at this point, the message buffer contains only non-deliverable messages, "messages with a final destination other than the connected node". The main goal of this phase is to accumulate messages that will be suggested to be sent to the other node in a temporary output buffer. Choosing messages that will be put in the output buffer depends on specific criteria shown in Figure 7. The first block in Figure 6 is labeled "for each message in the buffer" because this phase could be implemented in a way such that all the messages are processed at the same time. However, the implementation performed in the simulator is not multithreading; it just tests each message at a time. First, we start with the case when at least one of the nodes does not meet the destination. Note that x is the time since the current node meets the destination node and y is the time since the other node meets the destination node. If the current node does not meet the message's destination node, while the other node does, the message will be copied to the output buffer. If the current node does meet the message's destination, while the other node does not, the message will not be copied to the output buffer. However, when both nodes have already met the destination, if the current node's meeting time with the destination is earlier that the other node, and the message will not be copied to the output buffer; otherwise, the message will be copied. This is shown in the flowchart in the case while testing if $x < y$. The simulation results of the proposed approach show that the new routing protocol, in the early phases of the simulation, acts as direct delivery. That is the case when both nodes do not meet the message's destination node. This results in increased latency. To overcome this problem, in the case when both nodes have not met the message's destination node yet, a Spray and Wait logic is followed. However, the implementation of Spray and Wait here is different than the traditional one. This is why we add a message header field "Number of Copies". In case both nodes have not met the message's destination node, the protocol tests whether the number of copies in the message header is greater than zero. A zero value indicates that the message will not be copied to the output buffer. If "Number of Copies" is greater than zero, it is set to Floor (*old Number of Copies/2*), that is, if the "Number of Copies" is 3, it will become 1. And then, the message will be copied to the output buffer. This will result in spreading the message in the network in a controlled way, not like Epidemic, thus increasing the delivery probability, especially in the early phases of the simulation.

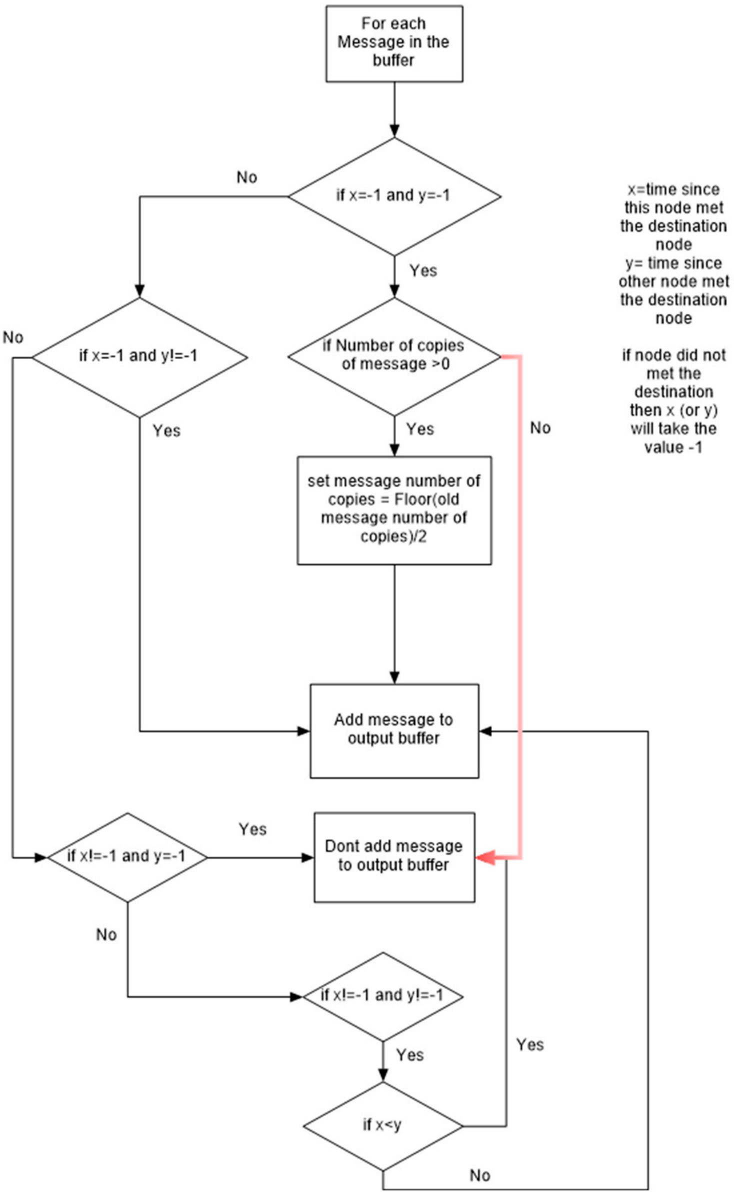

For each Message in the buffer
if x=-1 and y=-1
No
Yes
x=time since this node met the destination node
y= time since other node met the destination node
if node did not met the destination then x (or y) will take the value -1
if x=-1 and y!=-1
No
Yes
if Number of copies of message >0
Yes
No
set message number of copies = Floor(old message number of copies)/2
Add message to output buffer
if x!=-1 and y=-1
Yes
No
Dont add message to output buffer
if x!=-1 and y!=-1
Yes
if x<y
Yes
No

Figure 7. Phase 3 functionality.

- ***Phase 4: Send Messages Accepted by the Receiver***

This phase and the next one run at the same time, but this phase runs at the sender side and the next one at the receiver. The sender first accumulates the metadata of all messages in the output buffer in one message and sends them to the receiver. The metadata contain the ID of the message and its size. And then, the sender waits for the receiver to send it a reply for each message. Depending on this reply, the sender decides whether to send the message or to delete it from the output buffer. Note that the receiver replies for each message based on specific criteria discussed in the fifth phase. As shown in Figure 8, the sender waits for a reply from the receiver. Each reply message contains RCV_OK or DENIED_LOW_RESOURCES, and the ID of the message the receiver replies for. If the receiver replies with RCV_OK, the sender sends a message from the output buffer whose

ID is in the reply message and then returns to the waiting state. However, if the reply is DENIED_LOW_RESOURCES, the connection between the sender and the receiver is closed.

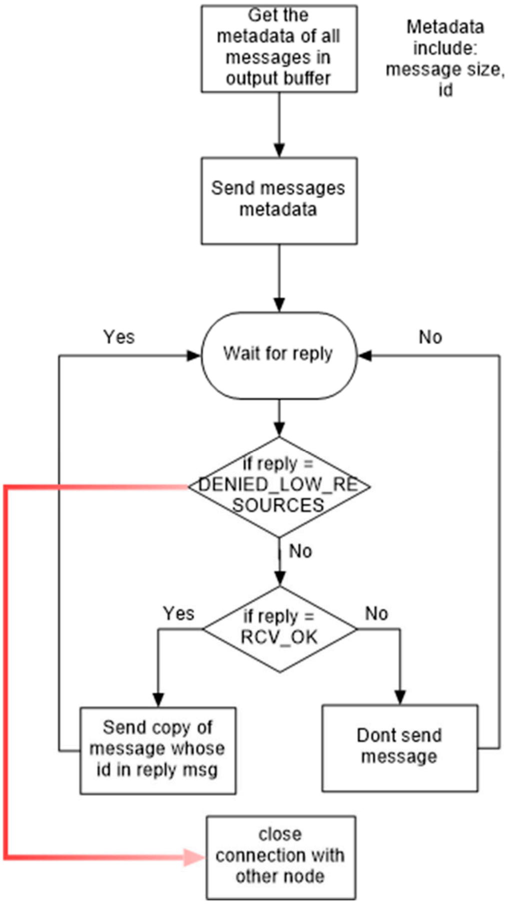

Get the metadata of all messages in output buffer
Metadata include: message size, id
Send messages metadata
Yes
Wait for reply
No
if reply = DENIED_LOW_RESOURCES
No
Yes
if reply = RCV_OK
No
Send copy of message whose id in reply msg
Dont send message
close connection with other node

Figure 8. Phase 4 functionality.

- ***Phase 5: Message Acceptance Criteria***

This phase occurs at the receiver's side when it receives metadata sent by the sender in the fourth phase. If the receiver's node energy is below the minimum threshold, it replies with DENIED_LOW_RESOURCES to the sender and the connection is terminated. Otherwise, the receiver follows specific criteria to choose messages to be relayed in its buffer. If the receiver has enough energy and the message is not in the buffer, a check is performed regarding the message size. If the size of the message is greater than the buffer size, the message will not be accepted. If the free buffer size is greater than or equal to the message size, the message is accepted. If the free buffer size is less than the message size, the receiver keeps deleting the oldest message in the buffer until the free buffer size is greater than or equal to the message size; then, it accepts the message.

The message is accepted by replying to the sender with a RCV_OK packet containing the ID of the message.

7. Performance Evaluation

The simulator used in the proposed work is an opportunistic network environment (ONE) simulator. Unlike other DTN simulators, which only simulate routing protocols, we combined the simulation mobility modeling and DTN routing. Connectivity between the nodes is based on their location, communication range, and bit rate. The simulations contain different types of groups (cars, pedestrians, etc.), and each one has a set of parameters, such as the message buffer size, radio range, and mobility model.

7.1. Simulation Scenario

To simulate the proposed model, two simulation scenarios have been proposed. The first one is the default scenario of the ONE simulator, and the second one is the DakNet scenario, which simulates three villages connected with each other. In all simulations, the focus is on three parameters: delivery probability, overhead ratio, and latency. The proposed algorithm is compared to the most important DTN routing algorithms implemented in the ONE simulator, which are: Spray and Wait, Prophet, Epidemic, and Fresh. The ping–pong application can be configured to send pings with a fixed interval or to only answer pings it receives. When the application receives a ping, it sends a pong message in response. In the simulation scenario, all the nodes are considered to be mobile. The nodes communicate with each other using the Bluetooth interface at a 250 KB/s data rate and a 10 m radio range. This scenario includes a part of the Helsinki downtown area (4500 × 3400 m). The total number of nodes is divided into three main groups. Group 1 and group 3 nodes are pedestrians who move at random speeds in the range of 0.5–1.5 m/s, which is the typical walking speed, with pause times between 0 and 120 s. Group 2 nodes are cars moving at the speeds of 2.7–13.9 m/s (10–50 km/h), with pause times between 0 and 120 s. Group 4 nodes are trams that move at the speeds of 7–10 m/s with pause times between 10 and 30 s. Groups 1, 2, and 3 consist of 40 nodes each, while group 4 only consists of 6 nodes. Group 1, 2, and 3 nodes have up to 20 MB of free buffer space, while group 4 nodes have 50 MB of free space for relaying and forwarding messages. Note that the group 4 communication interface has a data rate of 10 MB/s and a transmission range of 1000 m. A new message is generated on average every 25 to 35 s. The message size varies between 500 KB and 1 MB, with the time to live set to 300 min. Each simulation runs for 43,200 s (12 h).

7.2. Simulation Results

7.2.1. Layer 1 Simulation Results

In this experiment, we conducted a comparison between the detection time achieved by our proposed system and that of FT-OLSR. Figure 9 illustrates the time taken to isolate attackers from communication with other nodes, with respect to the percentage of attackers within the OppNet. As indicated in [37], the fuzzy logic system operates with two inputs and three fuzzy sets for each input, using 10 discretization levels for the universe of discourse. Based on these parameters, the fuzzy logic system involves approximately 9127 operations. Assuming the implementation of our FT-OLSR in hardware with a CPU clocked at 700 MHz and an average instruction execution time of 10 clocks, a single inference requires approximately 0.13 ms.

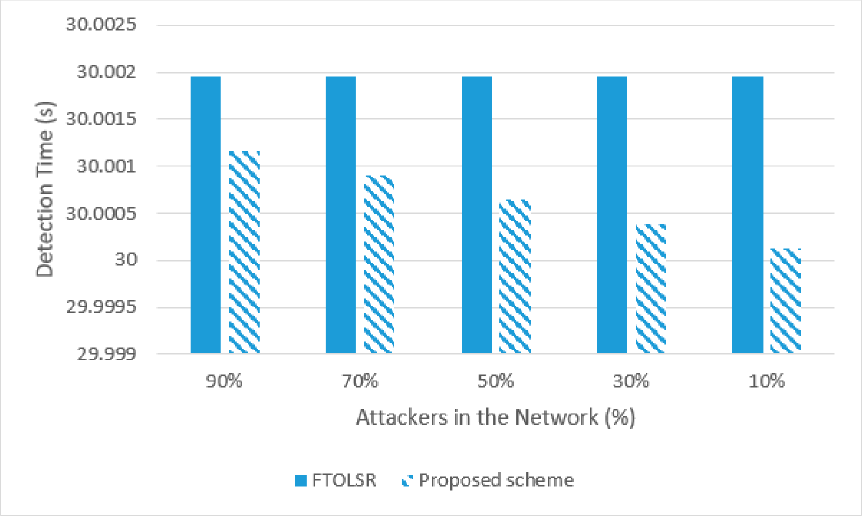
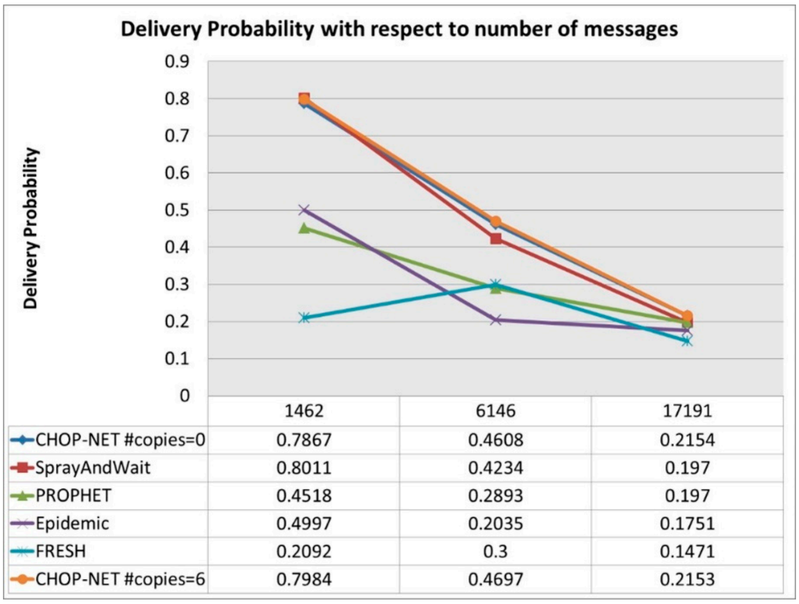


Figure 9. Detection time.

7.2.2. Layer 2 Simulation Results

a. **Varying the number of messages:** increase the number of messages from 1462 to 6146 to 17,191.

In this scenario, the behavior of the routing protocols under heavy load is studied: 17,191 messages each with size between 500 KB and 1 MB. Figure 10 shows that increasing the number of messages in the network will increase the number of dropped messages in the buffer and thus decrease the delivery probability. The proposed algorithm ensures the best delivery probability, while the number of messages increases. Figure 11 shows that when the number of messages increases from 1462 to 6146, the overhead ratio decreases from 14.54 to 7.46 (case number of copies = 0). Note that the Spray and Wait algorithm has a less overhead ratio. Beyond this point, when the number of messages increases from 6146 to 17,191, the algorithm approximately maintains the same overhead and has less overhead than the Spray and Wait algorithm. Figure 12 shows that increasing the number of messages will lead to a slight increase in the latency from 6704 s (1462 messages) to 7418 s (6146 messages). However, increasing the number of messages to 17,191 will decrease the latency to 4608. The fact that increasing the number of messages leads to decreasing the latency is because increasing the number of messages will increase the number of messages dropped in the buffer. This is because the buffer has to accept new messages, and thus, the messages cannot traverse several hops without being dropped and only messages with a destination near the source will be delivered, and thus, the latency decreases.

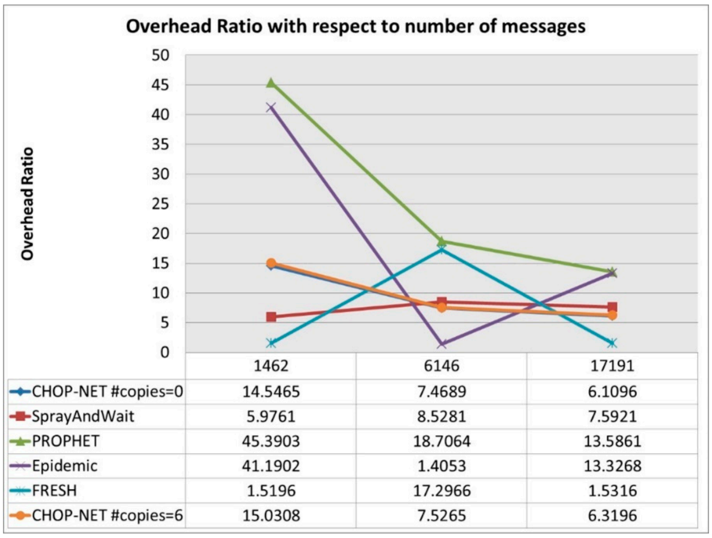


	1462	6146	17191
CHOP-NET #copies=0	0.7867	0.4608	0.2154
SprayAndWait	0.8011	0.4234	0.197
PROPHET	0.4518	0.2893	0.197
Epidemic	0.4997	0.2035	0.1751
FRESH	0.2092	0.3	0.1471
CHOP-NET #copies=6	0.7984	0.4697	0.2153

Figure 10. Delivery probability with respect to the number of messages.

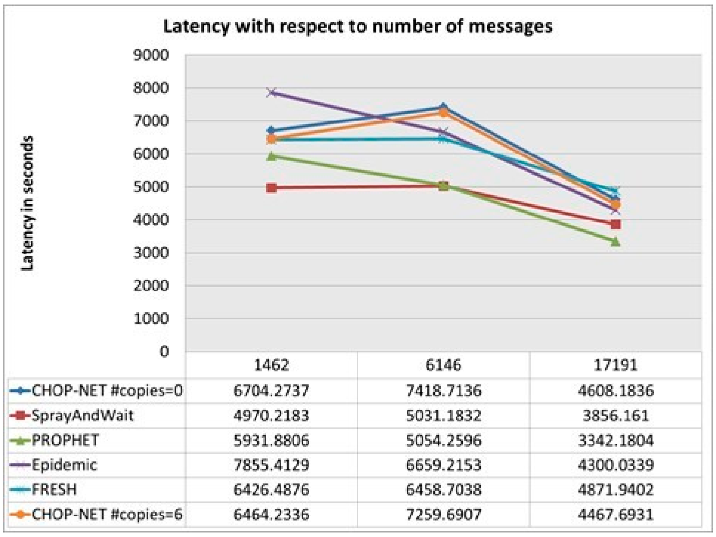
b. **Varying the number of users:** increase the number of nodes from 125 to 185 to 245.

Increasing the number of users means that the number of message carriers will increase, and this has a good effect on the algorithm. Figure 13 shows that increasing the number of users in the network has a good effect on the delivery probability, which increases to 0.9 in case we have 245 users, which is a considerable rate compared to other algorithms. The overhead ratio increases but remains challenging compared to other protocols. As shown in Figure 14, the overhead value is acceptable when compared to other routing algorithms, where the overhead ranges between 208 for Prophet (case 245 users) and 5.8 for Spray and Wait. The latency decreases as the number of users increases, and the proposed algorithm achieves low and challenging latency when compared to other algorithms, as shown in Figure 15.



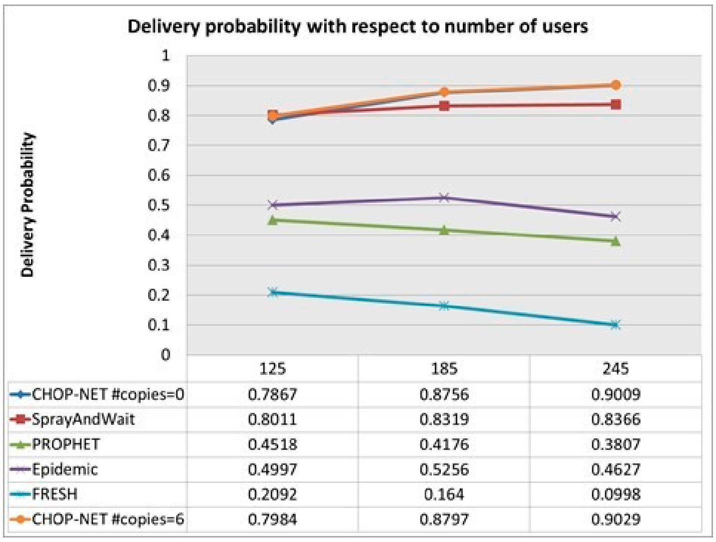
	1462	6146	17191
CHOP-NET #copies=0	14.5465	7.4689	6.1096
SprayAndWait	5.9761	8.5281	7.5921
PROPHET	45.3903	18.7064	13.5861
Epidemic	41.1902	1.4053	13.3268
FRESH	1.5196	17.2966	1.5316
CHOP-NET #copies=6	15.0308	7.5265	6.3196

Figure 11. Overhead ratio with respect to the number of messages.



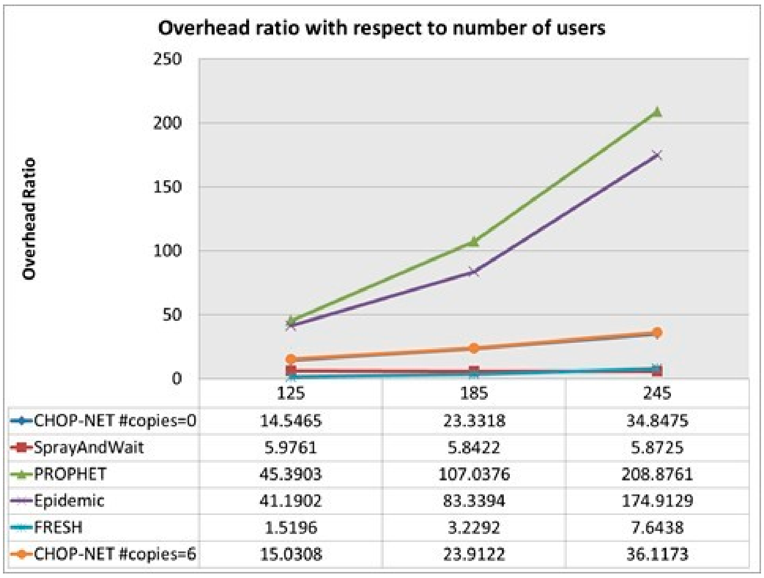
	1462	6146	17191
CHOP-NET #copies=0	6704.2737	7418.7136	4608.1836
SprayAndWait	4970.2183	5031.1832	3856.161
PROPHET	5931.8806	5054.2596	3342.1804
Epidemic	7855.4129	6659.2153	4300.0339
FRESH	6426.4876	6458.7038	4871.9402
CHOP-NET #copies=6	6464.2336	7259.6907	4467.6931

Figure 12. Latency with respect to the number of messages.



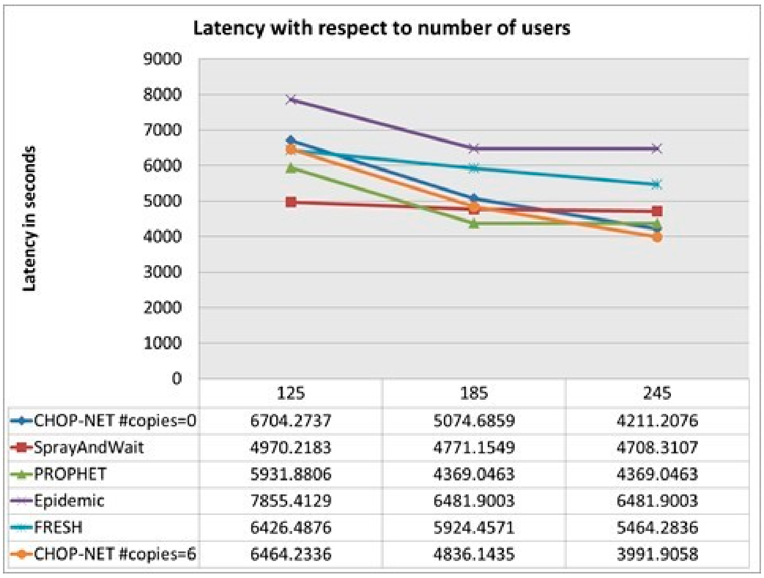
	125	185	245
CHOP-NET #copies=0	0.7867	0.8756	0.9009
SprayAndWait	0.8011	0.8319	0.8366
PROPHET	0.4518	0.4176	0.3807
Epidemic	0.4997	0.5256	0.4627
FRESH	0.2092	0.164	0.0998
CHOP-NET #copies=6	0.7984	0.8797	0.9029

Figure 13. Delivery probability with respect to the number of users.



	125	185	245
CHOP-NET #copies=0	14.5465	23.3318	34.8475
SprayAndWait	5.9761	5.8422	5.8725
PROPHET	45.3903	107.0376	208.8761
Epidemic	41.1902	83.3394	174.9129
FRESH	1.5196	3.2292	7.6438
CHOP-NET #copies=6	15.0308	23.9122	36.1173

Figure 14. Overhead ratio with respect to the number of users.

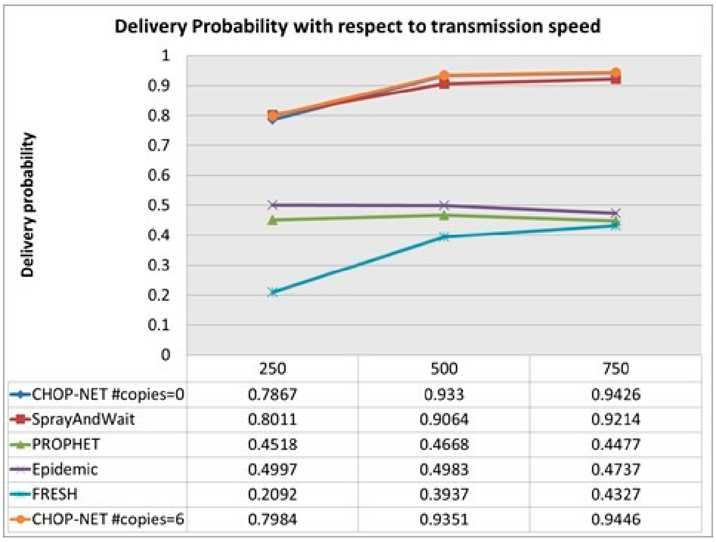


	125	185	245
CHOP-NET #copies=0	6704.2737	5074.6859	4211.2076
SprayAndWait	4970.2183	4771.1549	4708.3107
PROPHET	5931.8806	4369.0463	4369.0463
Epidemic	7855.4129	6481.9003	6481.9003
FRESH	6426.4876	5924.4571	5464.2836
CHOP-NET #copies=6	6464.2336	4836.1435	3991.9058

Figure 15. Latency with respect to the number of users.

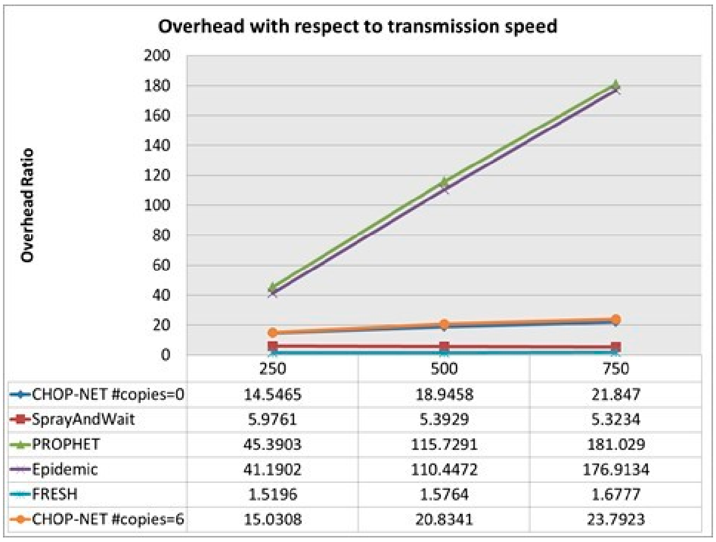
c. **Varying the transmission speed:** increase the transmission speed from 250 to 500 to 750 KB/s.

When the distance between two connected nodes becomes larger than the transmission range of the wireless network interface, 10 m in the simulation, the connection will be terminated. Increasing the transmission speed will decrease the time of phases 1, 2, 4, and 5 of the algorithm, and thus, the number of message exchanged between any connected nodes will increase before the connection is terminated. This will lead to an increase in the delivery probability, as shown in Figure 16. The proposed protocol maintains the best delivery probability and the lowest latency (when the transmission speed increases to 500 and 750 KB/s). Figure 17 shows that the protocol maintains an acceptable overhead, while increasing the transmission speed. At 750 KB/s speed, the proposed protocol has an overhead ratio of 21.84 (case number of copies = 0) and 23.79 (when number of copies = 6). The range of overhead varies between 181 (for Prophet) and 1.67 (for Fresh). Thus, the overhead ratio of the proposed protocol is considered acceptable. We notice also a decrease in the latency (Figure 18).



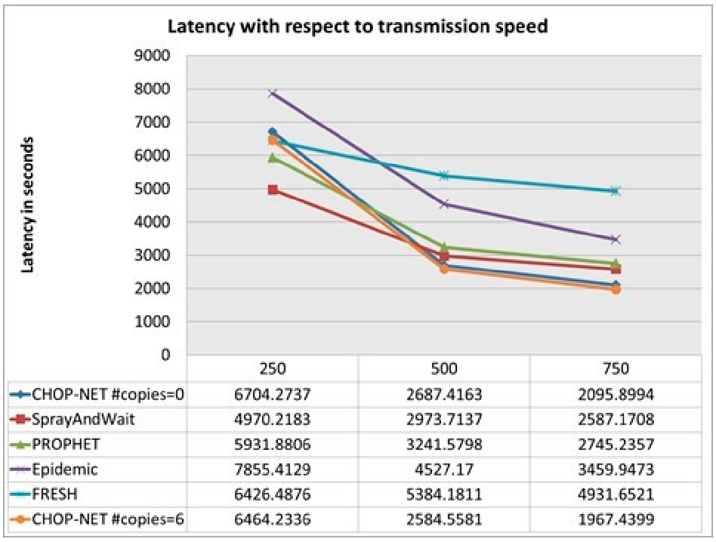
	250	500	750
CHOP-NET #copies=0	0.7867	0.933	0.9426
SprayAndWait	0.8011	0.9064	0.9214
PROPHET	0.4518	0.4668	0.4477
Epidemic	0.4997	0.4983	0.4737
FRESH	0.2092	0.3937	0.4327
CHOP-NET #copies=6	0.7984	0.9351	0.9446

Figure 16. Delivery probability with respect to the transmission speed.



	250	500	750
CHOP-NET #copies=0	14.5465	18.9458	21.847
SprayAndWait	5.9761	5.3929	5.3234
PROPHET	45.3903	115.7291	181.029
Epidemic	41.1902	110.4472	176.9134
FRESH	1.5196	1.5764	1.6777
CHOP-NET #copies=6	15.0308	20.8341	23.7923

Figure 17. Overhead ratio with respect to the transmission speed.

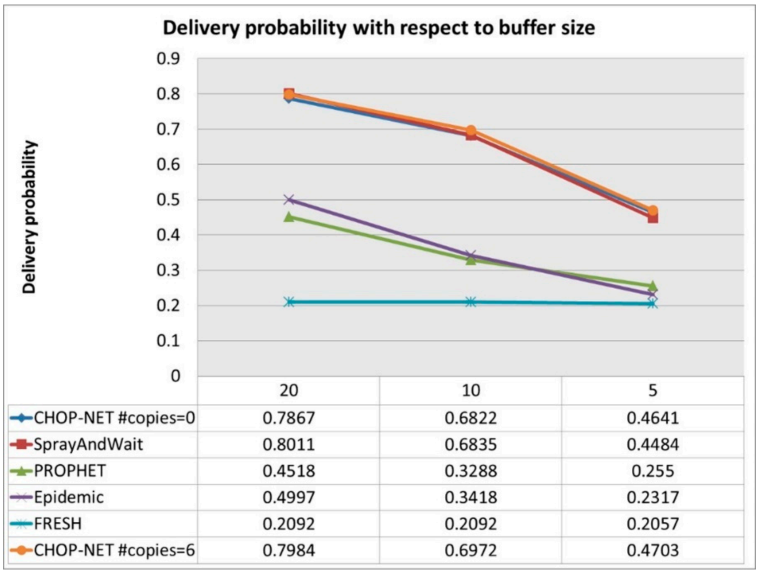


	250	500	750
CHOP-NET #copies=0	6704.2737	2687.4163	2095.8994
SprayAndWait	4970.2183	2973.7137	2587.1708
PROPHET	5931.8806	3241.5798	2745.2357
Epidemic	7855.4129	4527.17	3459.9473
FRESH	6426.4876	5384.1811	4931.6521
CHOP-NET #copies=6	6464.2336	2584.5581	1967.4399

Figure 18. Latency with respect to the transmission speed.

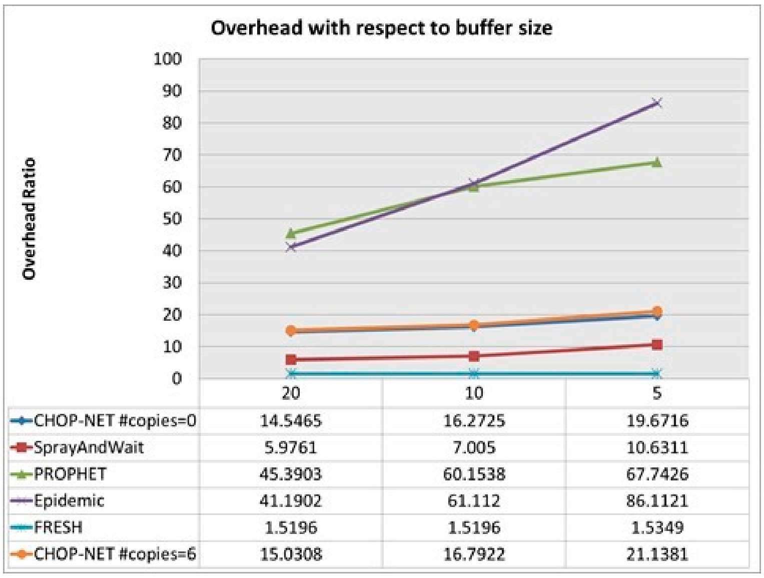
d. **Varying the buffer size:** decrease the buffer size from 20 to 10 to 5 MB.

This scenario studies the effect of decreasing the buffer size in a situation in which the mobile device has limited memory capability. Decreasing the buffer size will decrease the number of messages carried by each node; this will consequently decrease the delivery probability. This is demonstrated in Figure 19, where the delivery probability decreases, while the buffer size decreases. However, the proposed routing algorithm maintains high delivery probability with respect to other algorithms. Figure 20 shows that the overhead decreases, while the buffer size decreases. The proposed algorithm shows acceptable overhead when compared to other algorithms. Figure 21 shows that decreasing the buffer size leads to a decrease in the delay; this is because the buffer will drop more packets when its size decreases, and thus, the packets will not be routed through many hops.



	20	10	5
CHOP-NET #copies=0	0.7867	0.6822	0.4641
SprayAndWait	0.8011	0.6835	0.4484
PROPHET	0.4518	0.3288	0.255
Epidemic	0.4997	0.3418	0.2317
FRESH	0.2092	0.2092	0.2057
CHOP-NET #copies=6	0.7984	0.6972	0.4703

Figure 19. Delivery probability with respect to the buffer size.

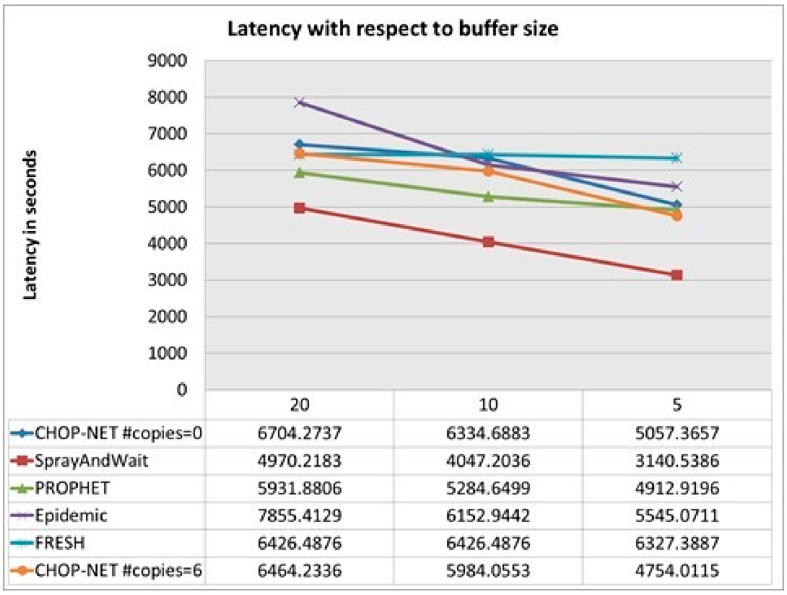


	20	10	5
CHOP-NET #copies=0	14.5465	16.2725	19.6716
SprayAndWait	5.9761	7.005	10.6311
PROPHET	45.3903	60.1538	67.7426
Epidemic	41.1902	61.112	86.1121
FRESH	1.5196	1.5196	1.5349
CHOP-NET #copies=6	15.0308	16.7922	21.1381

Figure 20. Overhead ratio with respect to the buffer size.

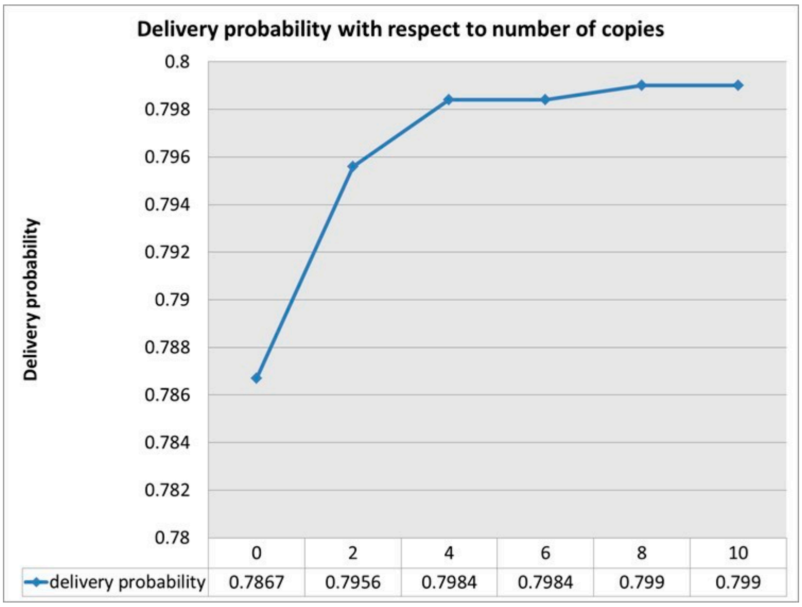
e. **Varying the number of copies**

This scenario shows the routing protocol behavior upon changing the number of message copies. Increasing the number of message copies will increase the chance of the message to arrive at the destination node, and thus, the delivery probability increases (Figure 22). The overhead ratio will surely increase because we are adding more overhead messages for each single message, and this is shown in Figure 23. Again the latency decreases (Figure 24).



	20	10	5
CHOP-NET #copies=0	6704.2737	6334.6883	5057.3657
SprayAndWait	4970.2183	4047.2036	3140.5386
PROPHET	5931.8806	5284.6499	4912.9196
Epidemic	7855.4129	6152.9442	5545.0711
FRESH	6426.4876	6426.4876	6327.3887
CHOP-NET #copies=6	6464.2336	5984.0553	4754.0115

Figure 21. Latency with respect to the buffer size.



	0	2	4	6	8	10
delivery probability	0.7867	0.7956	0.7984	0.7984	0.799	0.799

Figure 22. Delivery probability with respect to the number of copies.

f. **Ping–pong application**

As shown in Figure 25, the proposed algorithm has the highest ping delivery probability and a high pong delivery probability. Notice that increasing the number of message copies to six has a remarkable effect in the application where we obtain the highest ping/pong success probability.

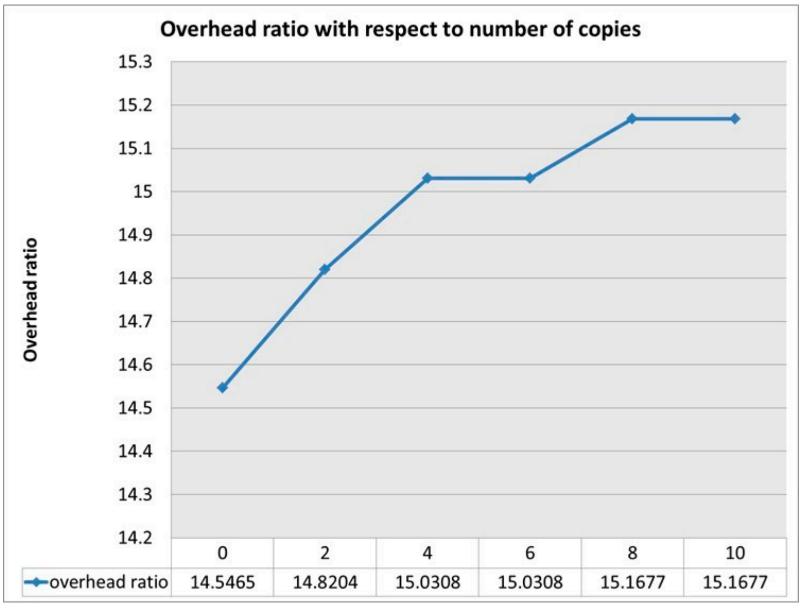


Figure 23. Overhead ratio with respect to the number of copies.

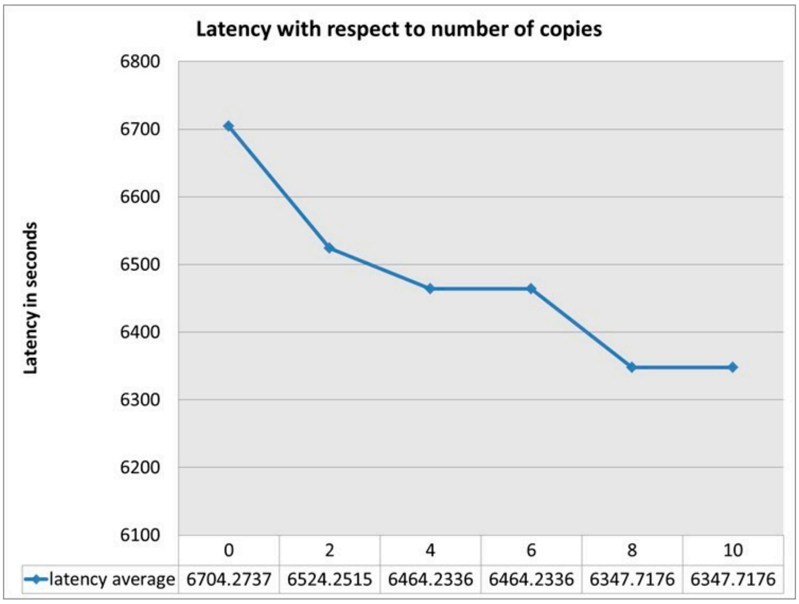


Figure 24. Latency with respect to the number of copies.

g. **WiFi-Direct scenario:** transmission speed 5 MB/s, transmission range 30 m, and buffer size 20 MB.

This scenario replaces the Bluetooth radio interface with a WiFi-Direct interface having the above-mentioned characteristics. As shown in Figure 26, in this scenario, the proposed algorithm gets a high delivery probability (0.959), and it is the highest among the other algorithms. Figure 27 shows that the proposed algorithm overhead ratio is low (between 26 and 30). Figure 28 shows that the proposed algorithm has the lowest latency among other algorithms (between 1477 and 1616). This scenario shows how the proposed algorithm maintains its highest delivery probability with the development of network interfaces. Notice that we obtain a significant improvement in latency.

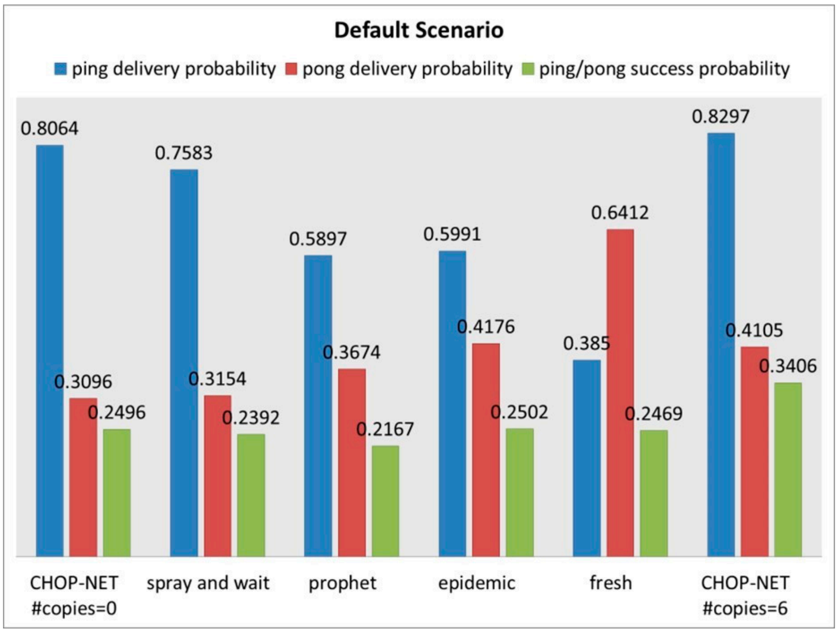


Figure 25. Ping–pong application probability results.

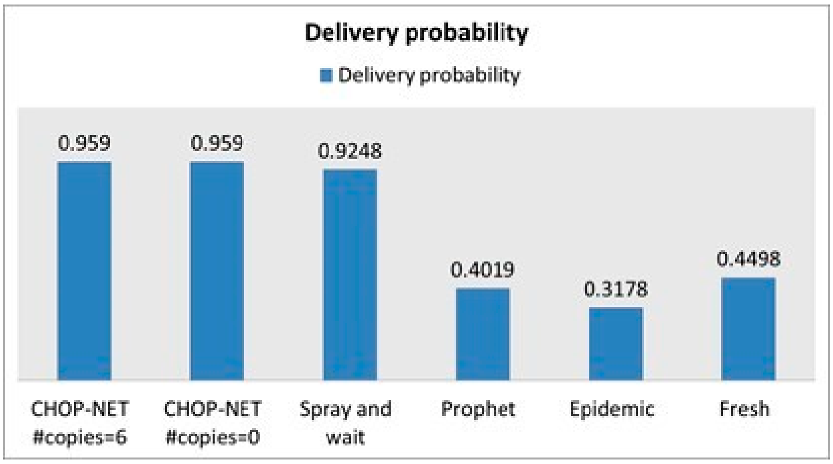


Figure 26. Delivery probability WiFi-Direct case.

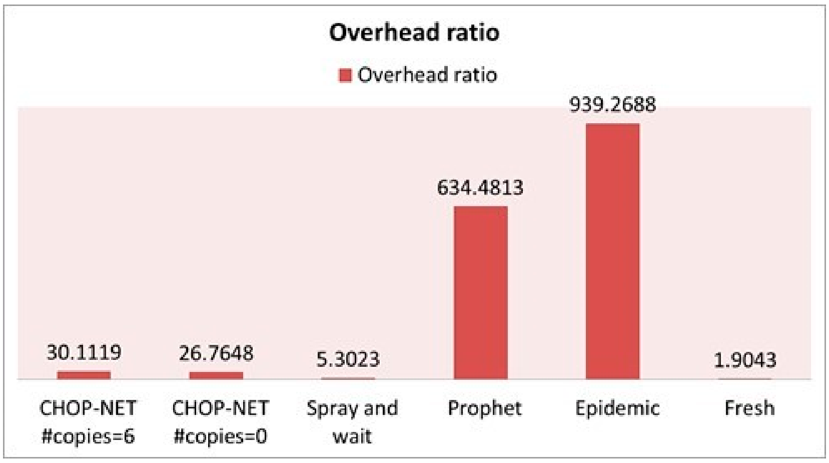


Figure 27. Overhead ratio WiFi-Direct case.

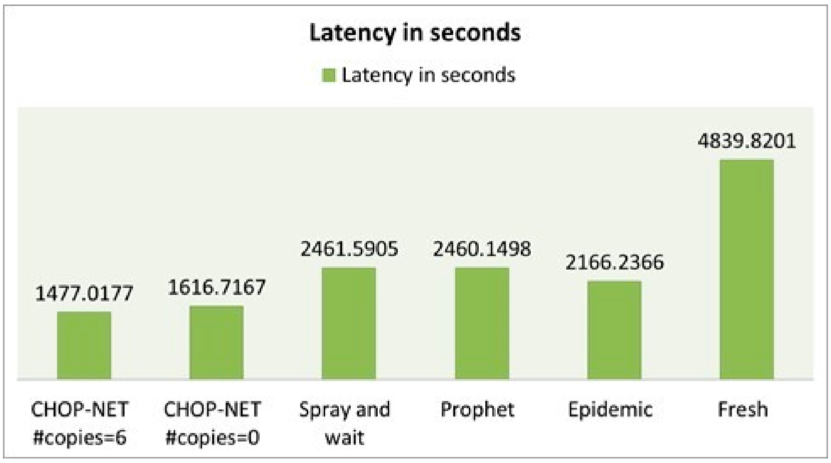


Figure 28. Latency WiFi-Direct case.

8. Conclusions

In conclusion, the fusion of cybersecurity technology with opportunistic networks in the proposed model represents a significant leap forward in the realm of wireless communications. The proposed two-layer approach, combining security protocols with an innovative routing protocol, successfully addresses the distinctive challenges posed by opportunistic networks.

The first layer, anchored by the FT-OLSR protocol, showcases the effectiveness of employing fuzzy logic for trust computation and a Proof-of-Trust consensus algorithm. The decentralized trust evaluation and the isolation of misbehaving nodes contribute to a robust and secure network environment. The proposed system not only meets the distributed management, reliability, security, and scalability requirements but also streamlines the process, avoiding intricate calculations and conserving resources. The second layer introduces a novel routing protocol meticulously designed for opportunistic networks. The protocol's efficiency is demonstrated through distinct phases, optimizing message exchange, handling non-deliverable messages, and implementing smart criteria for message acceptance. This approach significantly improves key performance metrics, ensuring superior delivery probability, reduced overhead, and minimized communication latency.

The extensive simulation results across various scenarios validate the model's performance and versatility. The proposed solution consistently outperforms established DTN routing algorithms under different conditions, emphasizing its adaptability to diverse network scenarios. Whether in a DakNet environment or a WiFi-Direct scenario, the model proves its robustness, offering superior delivery probability, low overhead, and reduced latency.

In essence, this research paper paves the way for the integration of cybersecurity into opportunistic networks, offering a holistic solution that not only fortifies security but also optimizes routing for enhanced efficiency and sustainability. The proposed model emerges as a beacon in wireless communications, especially in scenarios where traditional networking infrastructures face limitations, ensuring seamless and timely information exchange in dynamic and resource-constrained settings. As the digital landscape evolves, the paradigm introduced here holds promise for shaping the future of wireless communication systems.

Author Contributions: Conceptualization, A.K. and B.Z.; methodology, A.K. and B.Z.; software, A.K. and B.Z.; validation, B.Z. and A.K.; formal analysis, B.Z. and A.K.; investigation, A.K. and B.Z.; resources, B.Z. and A.K.; data curation, A.K. and B.Z.; writing—original draft preparation, A.K. and B.Z.; writing—review and editing, A.K. and B.Z.; visualization, A.K. and B.Z.; super-vision, B.Z. and A.K.; project administration, B.Z. and A.K.; funding acquisition, B.Z. and A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

OppNets	opportunistic networks
DTN	delay-tolerant network
TCP/IP	Transmission Control Protocol/Internet Protocol
Prophet	Probabilistic Routing Protocol using History of Encounters and Transitivity
Fresh	FResher Encounter SearcH
Meed	minimum estimated expected delay
PoD	Proof of Delivery
PoW	Proof of Work
PoS	Proof of Stake
FT-OLSR	Fuzzy-Logic-based Trusted Optimized Link State
PoT	Proof of Trust
TC messages	topology control messages
TTL	time to live
RCV_OK	receive return value for OK

References

1. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; HN Publishing: Storstrom, Denmark, 2008.
2. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
3. Doe, J.; Smith, A. Cybersecurity Measures for Critical Infrastructure Protection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 532–545.
4. Ruoti, S.; Rodrigues, B.; Gkantsidis, C. Identity, Identification, and Identifiability: The Language of Self-Sovereign Identity. *arXiv* **2018**, arXiv:1802.05262.
5. Alajeely, M.; Doss, R.; Ahmad, A. Security and Trust in Opportunistic Networks—A Survey. *IETE Tech. Rev.* **2015**, *33*, 256–268. [CrossRef]
6. Mohan, S.; Qu, G.; Mili, F. Security Analysis of Opportunistic Networks Using Complex Network Properties. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Orlando, FL, USA, 25–30 March 2012.
7. Muñoz, A.; Ríos, R.; Román, R.; López, J. A survey on the (in)security of trusted execution environments. *Comput. Secur.* **2023**, *129*, 103180. [CrossRef]
8. Muñoz, A.; Gago, C.F.; López-Villa, R. A Test Environment for Wireless Hacking in Domestic IoT Scenarios. *Mob. Netw. Appl.* **2022**, 1–10. [CrossRef]
9. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Wattenhofer, R. On Scaling Decentralized Blockchains. In Proceedings of the International Conference on Financial Cryptography and Data Security, Church, Barbados, 22–26 February 2016; pp. 106–125.
10. Pass, R.; Seeman, L.; Shelat, A. Analysis of the Blockchain Protocol in Asynchronous Networks. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 30 April–4 May 2017; pp. 643–673.
11. Bonneau, J.; Narayanan, A.; Miller, A.; Clark, J.A.; Kroll, J.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121.
12. Camenisch, J.; Lysyanskaya, A. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001; pp. 93–118.
13. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
14. Micali, S.; Lehman, A.; Lipton, R.J. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, 28 October 2017; pp. 51–68.
15. Camp, T.; Boleng, J.; Davies, V. A survey of mobility models for ad hoc network research. *Wirel. Commun. Mob. Comput.* **2002**, *2*, 483–502. [CrossRef]
16. Boudguig, M.; Abdali, A. New predictability concept for routing in DTN: Comparison between different routing protocols. In Proceedings of the IEEE International Multimedia Computing and Systems (ICMCS), Tangiers, Morocco, 10–12 May 2012.
17. Socievole, A.; De Rango, F.; Coscarella, C. Routing Approaches and Performance Evaluation in Delay Tolerant Networks. In Proceedings of the IEEE Wireless Telecommunications Symposium (WTS), New York, NY, USA, 13–15 April 2011.

18. Zhang, Z. Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 24–37. [CrossRef]
19. Gui, J.; Wu, Y.; Pan, C.; Zou, F.; Xie, Y. Cost-Based Routing in Delay Tolerant Networks. In Proceedings of the IEEE Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, NSW, Australia, 9–12 September 2012.
20. Boldrini, C.; Conti, M.; Jacopini, J.; Passarella, A. HiBOp: A History Based Routing Protocol for Opportunistic Networks. In Proceedings of the IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM), Espoo, Finland, 18–21 June 2007.
21. Neena, V.; Rajam, V. Performance Analysis of Epidemic Routing Protocol for Opportunistic Networks in Different Mobility Patterns. In Proceedings of the IEEE International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 4–6 January 2013.
22. Spyropoulos, T.; Psounis, K.; Raghavendra, C.S. Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-copy Case. *IEEE/ACM Trans. Netw.* **2008**, *16*, 77–90. [CrossRef]
23. Iqbal SM, A. Multischeme Spray and Wait routing in Delay Tolerant networks exploiting nodes delivery predictability. In Proceedings of the IEEE International Conference on Computer and Information Technology (ICCIT), Chittagong, Bangladesh, 22–24 December 2012.
24. Li, X.; Jiang, P.; Chen, T. Blockchain-Assisted Epidemic Routing in Delay Tolerant Networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 537–545.
25. Ma, Z.; Chang, Z.; Wu, D.; Wang, Y. PoD: A Blockchain-Enabled Proof of Delivery Routing Protocol for Opportunistic Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 14673–14683.
26. Xu, J.; Zou, J.; Jiang, P. Consensus-Based Routing with Blockchain in Delay Tolerant Networks. *IEEE Trans. Netw. Sci. Eng.* **2018**, *5*, 204–213.
27. Wang, H.; Wang, Y.; Zhao, L. Blockchain-Powered Predictive Routing in Opportunistic Networks. *IEEE Internet Things J.* **2021**, *9*, 7858–7867.
28. Zohrevand, A.H.; Shafagh, H. Towards Scalable Blockchain Using Sharding. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019.
29. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
30. Mohanta, S.R.; Chowdhury, C.; Jana, P.K. Game Theoretic Analysis of Incentive Mechanism for Blockchain-Enabled Vehicular Delay Tolerant Network. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrück, Germany, 14–17 October 2019; pp. 90–97.
31. Cao, Y.; Li, P.; Liang, T.; Wu, X.; Wang, X.; Cui, Y. A Novel Opportunistic Network Routing Method on Campus Based on the Improved Markov Model. *Appl. Sci.* **2023**, *13*, 5217. [CrossRef]
32. Xu, G.; Wang, X.; Zhang, N.; Wang, Z.; Yu, L.; He, L. A Routing Algorithm for the Sparse Opportunistic Networks Based on Node Intimacy. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6666211. [CrossRef]
33. Inedjaren, Y.; Zeddini, B.; Maachaoui, M.; Barbot, J.P. Securing intelligent communications on the vehicular adhoc networks using fuzzy logic based trust OLSR. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–6.
34. Ross, T.J. *Fuzzy Logic with Engineering Applications*; John Wiley Sons: Hoboken, NJ, USA, 2005.
35. Inedjaren, Y.; Maachaoui, M.; Zeddini, B.; Barbot, J.-P. Blockchain-based distributed management system for trust in VANET. *Veh. Commun.* **2021**, *30*, 100350. [CrossRef]
36. Clausen, T.; Jacquet, P. RFC3626: Optimized Link State Routing Protocol (OLSR). 2003. Available online: https://datatracker.ietf.org/doc/rfc3626/ (accessed on 7 January 2024).
37. Kim, Y.H.; Ahn, S.C.; Kwon, W.H. Computational complexity of general fuzzy logic control and its simplification for a loop controller. *Fuzzy Sets Syst.* **2000**, *111*, 215–224. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.