Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777868

OPPORTUNISTIC NETWORKS: CONCEPTS, OPPORTUNITIES AND RESEARCH CHALLENGES IN SECURITY AND QOS

Mansi Mathur*
Dept. Of Computer Engineering, J.C. Bose University of Science & Technology, YMCA
Haryana, India, mansimathur66@gmail.com

Dr. Jyoti Verma
Dept. Of Computer Engineering, J.C. Bose University of Science & Technology, YMCA
Haryana, India, justjyoti.verma@gmail.com

Dr. Poonam
Dept. Of Computer Engineering, J.C. Bose University of Science & Technology, YMCA
Haryana, India, poonamgarg1984@gmail.com

Abstract— This paper provides an in-depth analysis of opportunistic networks (OppNets), focusing specifically on the aspects of security and quality of service (QoS). OppNets are characterized by their dynamic and ad hoc nature, presenting unique challenges and opportunities for communication. The paper examines the fundamental concepts underlying opportunistic networks and highlights the potential benefits they offer in various domains such as disaster management, vehicular networks, and rural communication. Moreover, the review identifies the key research challenges associated with security and QoS in opportunistic networks, including trust establishment, data privacy, routing protocols, and resource management. The paper also explores existing approaches and solutions proposed in the literature to address these challenges. By shedding light on the research gaps and future directions, this review aims to inspire further advancements in security and QoS aspects of opportunistic networks, ultimately contributing to their practical deployment in real-world scenarios.

Keywords— OppNet, Ad-hoc Network, Routing, Security, QoS, Machine Learning

1 INTRODUCTION

An Opportunistic Network (OppNet) is an advancement over ad-hoc networks, where the existence of a complete path between two nodes for communication cannot be assumed. In OppNets, the messages are sent opportunistically when a node encounters another node. These networks are highly mobile, with no prior knowledge of the next possible node or the final destination. They utilize a store-carry-forward policy, allowing nodes to store and carry information until they encounter the intended node or destination, enabling message forwarding. The primary advantage of OppNets is their ability to store messages without imposing time limits, ensuring successful communication with intermediate nodes [1][2]. Figure 1 illustrates the store-carry-forward model. OppNet stands out from other network techniques because of this characteristic.

OppNets emerged as an innovative network framework building upon ad-hoc networks, which allow packet transfer through intermediate hops while nodes are on the move, eventually

reaching the destination node in a fragmented network setting [3]. The term "contact" refers to the connection between two nodes, established when they are within the same communication domain. Communication occurs during this link, while it ends or is disrupted when one node leaves the domain. OppNets can be broadly classified into two types: 1) Infrastructure-based, where information about working nodes is initially used to identify potential nodes leading to the destination [5]; and 2) Infrastructure-less, designed for ad-hoc networks categorized as Vehicle Ad-hoc Networks (VANETS) [28] and Mobile Ad-hoc Networks (MANETS) [16], depending on their underlying infrastructure [6].

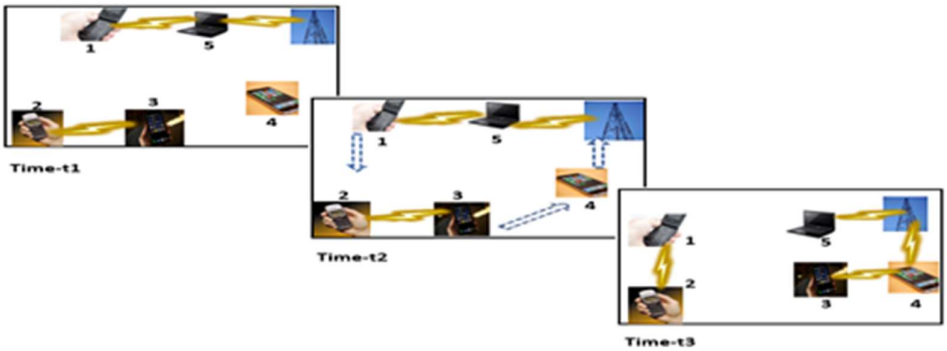

Figure 1 Store-carry-forward Technique

In Figure 1, shows there is no such fixed route for a message to reach from the source to the destination. So, the Node 1 delivers the message to Node 5 and carries till time interval t2 and then deliver to the Node 4. Finally, until time interval of t3, Node 5 and the destination Node 3 move to the same communication area.

OppNets serve as a network framework in various application domains, such as VANETS, mobile computing sharing, mobile data offloading, and more [7][8]. OppNets offer the advantages of low cost and easy deployment, enabling these applications to thrive. Regardless of the underlying infrastructure, OppNets facilitate functions like message sharing, content distribution, and resource sharing [9][10]. This versatility makes OppNets a valuable framework for achieving diverse communication and collaboration tasks, further enhancing their relevance across different domains.

The dynamic nature of OppNets poses a challenge in determining the forwarding path for message transmission. To enhance transmission performance, OppNets employ multiple copies of messages and select the most suitable next hop based on utility criteria. Routing algorithms in OppNets are categorized based on their routing behavior and the availability of the nodes in the network. Figure 2 illustrates the movement of nodes in an OppNet environment, showcasing how nodes navigate and interact within the network. These strategies aim to optimize routing and improve overall performance in OppNets.

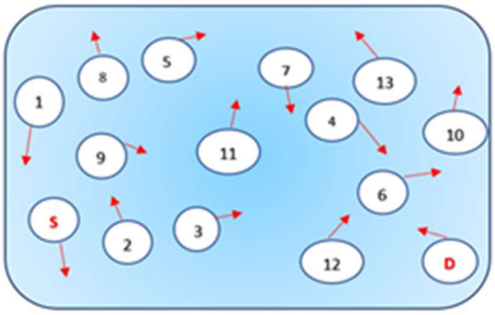

Figure 2 Working of nodes in OPPNET

In Figure 2, this is an example of how the nodes work in an opportunistic network environment. There are 15 nodes, among them one is the source node 'S' (message bearer) and the other one is the destination node 'D' (message receiver). The nodes other than these two nodes are used opportunistically in message transmission and communication. 'S' can only connect with either the 'D' directly or the adjacent nodes based on many factors like: - Connection durability, node's energy, connection history [12], delivery probability [21], trustworthiness of the next node [17][18][24][27] etc. There are many attacks exists which can breach the communication in and make the network insecure [25].

In various situations, achieving efficient and secure communication in OppNets can be quite challenging. Nodes face the task of making optimal message forwarding decisions, taking into consideration the trustworthiness of other nodes. This trustworthiness factor plays a critical role in ensuring secure transmission of data. Striking a balance between efficient and secure communication is a key objective in OppNets, and it requires careful consideration and decision-making on the part of individual nodes.

1.1 Motivation

The growing interest in opportunistic networks stems from their ability to support communication in challenging and dynamic environments, where traditional network infrastructure is limited or unavailable. These networks offer promising prospects for diverse domains, including disaster response, remote regions, and mobile ad-hoc networks. However, ensuring the security and QoS in opportunistic networks poses significant hurdles. This review paper aims to delve into the concepts, opportunities, and research challenges pertaining to security and QoS in opportunistic networks. Through an in-depth analysis of existing literature and identification of research gaps, this review aims to provide valuable insights and guide future research directions. Ultimately, the findings will contribute to the advancement of secure and reliable communication protocols in opportunistic networks.

1.2 Our Contribution

The main contributions of this paper are: -

- Analysis of various QoS parameters involved in routing techniques of existing opportunistic network.
- A detailed survey of the existing techniques proposed by various scholars for the secured transmission of messages in an opportunistic network environment.
- Identified gaps within the current proposed outcomes that can serve as valuable points of reference for researchers in developing future solutions.

1.3 Paper Organization

The rest of the paper is structured as follows: Section 2 offers an overview of routing techniques that researchers have employed to enhance quality of service and security aspects in opportunistic networks. Section 3 outlines the research methodology employed during the literature review. Section 4 elucidates key terms relevant to Opportunistic Networks. Finally, in Section 5, we summarize this review paper.

2 LITERATURE REVIEW

2.1 Existing routing techniques used by researchers for improving QoS parameters

Till now, various routing techniques have been proposed by researchers for improving the quality-of-service parameters for efficient routing in the OppNet environment. In [3], author presented an analysis of an adaptive-ranking-based energy-efficient opportunistic routing scheme. The paper proposed a mechanism that dynamically adjusts the ranking of nodes based on their energy levels and opportunistic encounters. Through simulations, the paper demonstrated that the proposed scheme achieved improved energy efficiency by effectively utilizing opportunistic encounters, enhanced the overall performance of opportunistic routing in wireless networks.

In [5], author presented an analysis of a routing protocol designed for secure and energy-efficient communication in underwater acoustic sensor networks. The protocol incorporates void avoidance techniques to mitigate the challenges posed by void regions in underwater environments. The authors also evaluated the proposed protocol through simulations, demonstrating its effectiveness in achieving secure and energy-efficient routing in underwater acoustic sensor networks.

In [6], they presented an analysis of a routing algorithm specifically designed for sparse opportunistic networks. The algorithm leverages the concept of node intimacy to prioritize message forwarding among closely related nodes. Through simulations and comparisons with existing algorithms, the paper demonstrated the proposed algorithm achieved improved routing performance in terms of average delay and delivery ratio, particularly in sparse opportunistic network scenarios.

In [7], they presented an analysis of energy balancing techniques for mobile opportunistic networks with wireless charging. The paper proposed single and multi-hop approaches to distribute energy efficiently among nodes in the network. Through simulations and comparisons, the authors demonstrated that the proposed approaches effectively balance energy levels, prolonged network lifetime, and improved the overall energy efficiency in mobile opportunistic networks with wireless charging.

In [10], author presented an effective communication scheme specifically designed for BLE i.e., Bluetooth Low Energy in large-scale applications. A novel protocol that optimizes data transmission, reduces energy consumption, and improves network scalability. The paper gave the comprehensive evaluation of the proposed scheme through simulations, demonstrating its effectiveness in achieving efficient communication in BLE-based large-scale applications.

In [11], the author presented an analysis of a fair energy-efficient scheduler for wireless networks. Proposed a scheduler algorithm that aims to balance energy efficiency and system capacity by intelligently allocating resources to users. The author evaluates the proposed

scheduler through simulations, demonstrating its ability to provide fair resource allocation, improved energy efficiency, and achieved high system capacity in wireless networks.

In [16], they presented an analysis of a delay-aware and cost-efficient probabilistic transmission scheme for OppNets. Proposed a mechanism that considers both delay constraints and transmission costs to optimize message delivery. Through simulations, the paper demonstrated that the proposed scheme effectively improves message delivery rates while minimizing transmission costs, making it suitable for opportunistic networks.

In [20], the author presented an analysis of an energy-efficient forwarding scheme for opportunistic networks. The scheme utilizes location prediction to optimize data packet forwarding and reduce energy consumption. Through simulations and comparisons with existing schemes, the paper demonstrated that the proposed scheme achieves significant energy savings while maintaining high delivery rates. The findings contributed to the development of energy-efficient forwarding mechanisms in resource-constrained opportunistic networks.

In [25], author presented an analysis of an energy-aware-routing scheme for promoting green communication in OppNets. They proposed a routing algorithm that considered energy consumption and network conditions to optimize route selection. Through simulations and comparisons, the authors demonstrated that the proposed scheme achieved energy efficiency, reduced carbon footprint, and improved the overall performance of opportunistic networks with reduced energy consumption.

In [35], author proposed a novel forwarding scheme which utilizes location prediction to efficiently forward data packets, thereby reducing energy consumption. They evaluated simulations and compares it with existing forwarding schemes. The results achieved significant energy savings while sustaining high delivery rates.

Table 1 provides the summarization of the existing work performed by the researchers related to the QoS parameters in opportunistic networks. It mainly focusses on the contribution made by the author and the limitations in their work.

TABLE 1 EXISTING RESEARCH RELATED TO QOS PARAMETERS IN OPPORTUNSTIC NETWORK

Reference	Year	Contribution	Limitation(s)
Satya J. Borah et al. [35]	2018	ELPFR-MC- Energy-efficient- Location-Prediction-based-Forwarding using Markov Chain	Proposed ELPFR-MC outperforms DEEP when no. of nodes are changed but missed the real-trace mobility models.
Ashkan Moradi [43]	2019	MSN, opportunistic network, selfish nodes, content dissemination	Results represented that the proposed algorithm to observe the optimal selfishness vector can further develop the organization

			execution by diminishing the forwarding delay.
Ankur Lohachab et al. [1]	2019	Opportunistic IoT network architecture	Results obtained using three protocols- PRoPHet, Epidemic and MaxProp and among them MaxProp was most efficient except for average hop count parameter was more in epidemic in two scenarios.
Premkumar Chithaluru et al. [3]	2019	Energy optimization, Adaptive ranking	Adaptive-ranking based energy-efficient opportunistic routing protocol was proposed which was computationally oriented but still time consuming.
Sanjay K. Dhurandher et al. [25]	2019	energy- aware routing, OppNet, green communication	With rise in no. of nodes there will be more message drops. In this paper the authors took increasing no. of nodes to check the evaluation parameters for four routing techniques.
JIANQUN CUI et al. [32]	2019	Connection strength, spray & wait, QoN, message handling capacity.	The QoN-ASW improved the distribution rate and cut the average delay and achieved comparatively low overhead but couldn't adapt to the changing buffer size of network.
Xiaomei Zhang and Shuyun Luo [12]	2019	Mobile opportunistic network, on-demand data forwarding, backbone- based approach	Ignored information's heterogeneous delay limitations that may ineffectually allocate resources, resultant inadequate data forwarding.
Wenyu Zheng et al. [13]	2019	Greedy approach, Node classification, opportunistic social network, task allocation, cooperative mechanism	Message carriers being usually limited in computing power will most likely be unable to rapidly track down the reasonable relay hub, bringing about network overhead and higher network latency.
S. Jagan [9]	2019	Throughput, Overload and Packet Delivery Ratio, Node	The network overhead increases due to the traffic flow of data in the network.

		Density, Epidemic Routing, Source Encoding	
Varun Menon [5]	2020	Energy-efficient and secure data transmission protocols, encryption	The proposed way needs to be verified in a real-time underwater setting.
Halikul Lenando et al. [8]	2020	MIWS- Mutual information-based weighting scheme	High load of specific attribute suggests a correspondingly high effect in accomplishing proficient information forwarding.
Maciej Nikodem et al. [10]	2020	Bluetooth Low energy, opportunistic sensing, active scanning, energy efficiency	The Bluetooth low energy nodes operated in large area are dependent on one central server.
Cédric Gueguen et al. [11]	2020	Energy consumption, Opportunistic scheduling, Cross-layer design.	Fairness, Energy efficiency and high system Capacity called FEC scheduler was proposed.
Jun Li et al. [14]	2020	Delay-aware, cost-effective, energy efficient, transmission delay	Proposed a cost-productive and delay-aware probabilistic transmission strategy to determine apt. relay nodes but used so many values of hop-count & delay thresholds.
Weifeng Sun et al. [4]	2021	Software defined network, Data flow classification	An information stream classification strategy called MACCA2 RF is proposed, to recognize the information stream classification and get the QoS prerequisites.
Gang Xu et al. [6]	2021	Node intimacy method, Time series, parameters- average buffer time, average latency, success delivery rate, average hop count of messages	The proposed ONBTM algorithm achieved higher message distribution quality with low resource utilization than epidemic and Prophet but not than spray and wait.
Aashish Dhungana et al. [7]	2021	Energy loss minimization, Mixed integer linear programming, load balancing	The relation of energy balancing and network lifetime has not been elaborated. Considered only single hop balancing.

On the basis of this literature survey, the below taxonomy of 'what' and 'how' approaches of improving Quality of Service parameters in opportunistic networks can be determined in figure 3. In the former approach the objective analysis has been carried out which includes the analysis of the current problems and their solutions in the area.

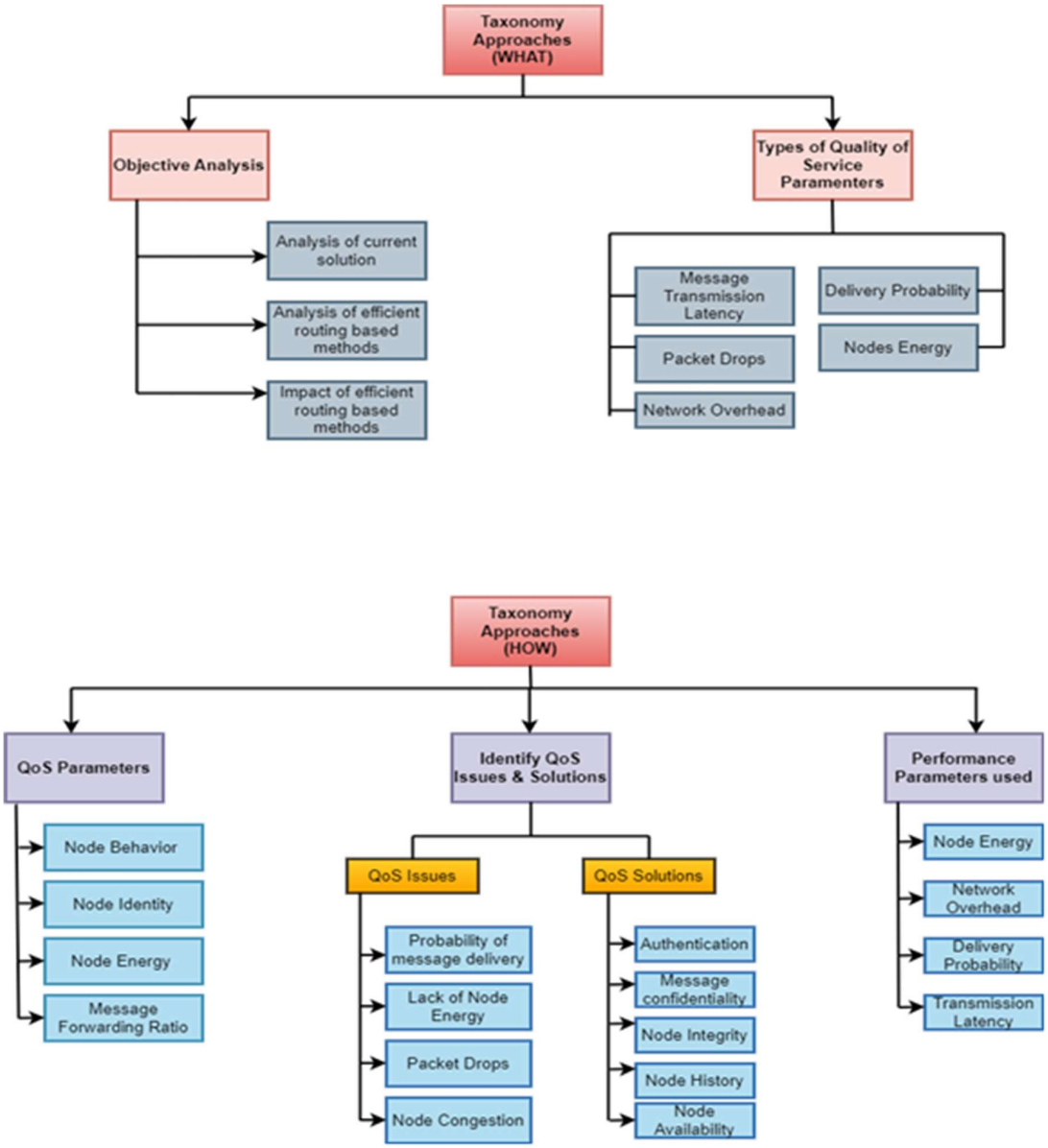

Figure 3 Taxonomy on QoS of OppNets to define solutions to the problems

2.2 Existing routing techniques used by researchers for improving security parameters

At present various existing routing methods have been proposed by the researchers to improve and also increase the security of these types of networks, as there exists non-connected and decentralised environments [18][22]. Due to this scattered nature, it is not probable to utilise matured security mechanisms such as cryptography that entails centralised trusted authorities which results in insecure communication [23].

To maintain the security of the network, there are various methods which are included in previous researches. [60] uses node trust model which generally uses pruning and filtering ways to get rid of threats in the network as shown in Figure 4. Their technique was able to reduce the interference of mean nodes to the network enhancing the performance of the system. Whereas [61] used the concept of PFM as in positive feedback message which sends a positive acknowledgement of current forwarder node to the previous node whenever a node receives or forwards a message to the next hop. Some researchers in [62] used trust-aware opportunity routing protocol in which their selection of next hop is based on trust level calculated by the fellow nodes who plays part in data packets communication. The methods discussed in [60][61][62] only solved the detection of malicious nodes but do not inculcate collision behaviour in such nodes.

To cope-up with the above issues, the researchers used a context-based-risk assessment method [63] which provides a safe and much reliable environment due to its approach to sensitivity of the data. Usually, these types of networks are more prone to various attacks such as man-in-the-middle attack [61], sybil attack [61], black hole attack [61] and denial of service attack [62] etc.

Su et. al. [64] used node trust model which generally uses pruning and filtering ways to get rid of threats in the network. Their calculation is based on dynamic weighting. Then they combined this method by ETC i.e., expected transmission count and calculated trust values of nodes. Their technique was able to reduce the interference of mean nodes to the network enhancing the system performance.

Singh et al. [65] proposed a novel jamming attack detection technique by using a statistical process approach to reduce overhead in the network. They ensured that the packet delivery ratio should increase.

Wang et. al. [66] ensured personal privacy and boost transmission effectiveness, opportunistic Cloud of Things was given a privacy-preserving message forwarding structure. To increase the efficiency of communication for terminal clients, they initially built up a cloud server with a two-layer architecture. They constructed a trait-based cryptosystem to protect information security at the expense of adequate resource utilization.

Kumar et. al. [67] used trust-aware opportunity routing protocol in which their selection of next hop is based on trust level calculated by the fellow nodes who plays part in data packets communication. The methods discussed in [1][11][12] only solved the detection of malicious nodes but do not inculcate collision behavior in such nodes.

Therefore, network security is crucial in terms of achieving higher probability of message delivery, legitimate packet delivery, lower value of latency in packet delivery and lower count of dropped messages. Table 2 provides the summarization of the work performed by researchers based on security parameters of the opportunistic network in the order of technique used and the limitations in their work.

TABLE 2 SUMMARIZATION OF SECURITY PARAMETERS USED BY RESEARCHERS IN OPPORTUNISTIC NETWORK

Reference	Year	Technique Used	Limitation(s)

Xiaojie Wang et al. [20]	2018	Opportunistic networking, Privacy-preserving message forwarding framework	Constructed a trait-based cryptosystem to protect information security at the expense of adequate resource utilization.
Satya J. Borah et al. [21]	2018	E-PRoWait, E-Prophet, DEEP, E-EDR	ELPFR-MC, in which the following best jump choice of a message relies upon the use of the hub's extra energy and its location in light of delivery probability.
Sameh Zakhary et al. [49]	2018	Distributed computing, Anonymity, Location privacy	Worked on transmission capacity and energy of the nodes.
Ngoc T. Luong et al. [16]	2019	Request route flooding attack, MANET, ML, AODV, B-ODV, FAPRP	Proposed a ML approach to flooding attacks prevention routing protocol in MANET.
Nisha Kandhoul, S. K dhurander et al. [18]	2019	Network Security, OppIoT, OppNet, IoT, Routing Protocols-SHBPR, RSASec and ATDTN	T_CAFE protocol enhanced the security of network and outperformed some routing protocols.
Nisha Kandhoul et al. [19]	2019	OppIoT, RSA, Secure prediction-based scheme	Secured messages with RSA and performed routing by foreseeing node's upcoming location utilizing Markov chain.
Cossi Blaise Avoussoukpo et al. [15]	2020	Mutual Authentication, OppNets, Opportunistic Communication, Privacy Protection	Comprehensive overviewed on user's Mutual Authentication in OppNets from one viewpoint and Location, social connections protection and identity inside OppNets then other.
Nisha Kandhoul et al. [22]	2021	Green Forwarding ratio, content-based routing, RSA based secure routing protocol	Covered only two security threats-Blackhole and packet fabrication. And no security scheme for identity of the nodes.
Cossi Blaise Avoussoukpo et al. [23]	2021	IoT, OPN Security, OPN Privacy Protection, Seed OppNet, Communication	Reviewed about only the main challenges of OppNets and the

			unusual knowledge of the network's topologic evolution.
R. Lavanya [24]	2021	IoT, Multicast Routing, Elephant Herding Optimization (EHO)	The proposed convention recognized an ideal way for directing by figuring costs including blockage and lifetimes of nodes.
Samaneh Rashidibajgan et al. [26]	2021	Sharing public key approach	Algorithm chose the best available node for message forwarding on its own. Provides identity and location privacy to nodes.

On the basis of this literature survey, the below taxonomy of 'what' and 'how' approaches of maintaining security in opportunistic networks can be determined in figure 4. In the former approach the objective analysis has been carried out which includes the analysis of the current problems and their solutions in the area. Then comes the trust-based solution analysis and what kind of impact it reflects on the situation. In the same, the types of attacks on the network security has been displayed.

The taxonomy approach of 'How' or the latter approach has the parameters to measure whether the trust of network or the trust level of a node. Alongside the trust issues and their solutions are displayed and discussed in the next section. To determine these trust-based solutions for carefree message forwarding among the nodes, some performance parameters are needed which are for example the identity of nodes can be snatched by the malicious node or an attacker which can impose itself as healthy node in the network to hamper the flow of packet delivery, another is node privacy and etc. Furthermore, the OppNet uses wireless technology such as WiMAX, IEEE 802.11 for wireless LAN, encompassing MAC and Physical layer specifications, IEEE 802.15 in WPAN for Wireless Personal Area Network, IEEE 802.16 in Wireless MAN for Wireless Metropolitan Area Network, and IEEE 802.17 in RPR access for Resilient Packet Ring, among others.

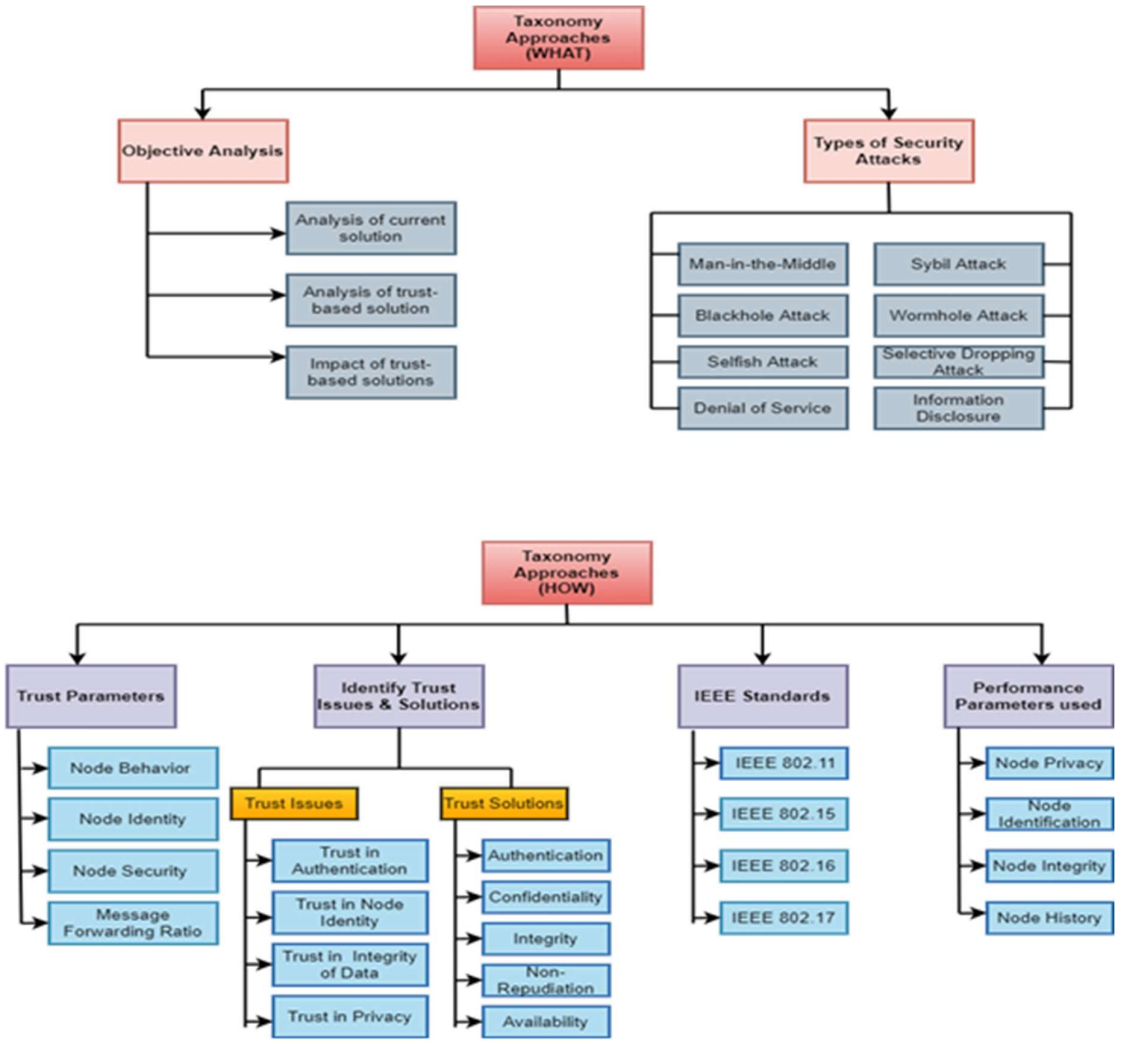

Figure 4 Taxonomy on Trust Management in OppNets to define solutions to the problems

2.3 Existing routing techniques used by researchers for improving QoS and security parameters using ML algorithms

Machine learning [71][72] plays a crucial role in addressing a wide range of challenges, such as enhancing quality of service and addressing various concerns including scalability, security, privacy, power efficiency, long-range communication, network management, heterogeneity, interoperability, mobility, network congestion, QoS, & coverage. These aspects require careful attention and machine learning offers its benefits in supporting network evolution while avoiding unexpected issues. For instance, security is a primary concern that needs continuous updates with technological advancements.

Machine learning provides effective solutions to boost the secure environment of linked devices by identifying malicious code attacks, ensuring privacy protection to prevent unauthorized identification and tracking, power analysis, intrusion detection systems, and more.

In [28] presented an analysis of utilizing unsupervised machine learning techniques to enhance routing in opportunistic communication networks of vehicles. The author proposed a methodology that leverages machine learning algorithms to autonomously learn and adapt

routing decisions based on the network's dynamic conditions. Through simulations and evaluations, the paper demonstrated the effectiveness of the proposed approach in improving routing efficiency and reliability in opportunistic networks of vehicles.

In [29], author presented an analysis of a machine learning-based approach for achieving optimal routing in opportunistic IoT networks. The author proposed a methodology that utilizes classifier cascades to classify network nodes and select the most suitable route for data transmission. Through experiments and evaluations, the paper demonstrated that the proposed approach achieved improved routing efficiency and minimizes transmission delay in opportunistic IoT networks.

In [30], the author presented an analysis of a routing algorithm based on Double Q-Learning for DTNs to make routing decisions by considering the network's delay and connectivity characteristics. Through simulations and evaluations, the paper demonstrated that proposed algorithm effectually improves message delivery rates and reduces transmission delays in DTNs.

In [31], the author proposed a method that utilizes fuzzy logic to determine the importance of various network parameters and incorporates double Q-Learning to make routing decisions based on learned Q-values. Through simulations and evaluations, the paper demonstrated that the proposed algorithm improves message delivery rates and reduces transmission delays in DTNs.

The author proposed a method that utilizes a deep reinforcement learning model to make routing decisions based on the dynamic conditions of the network. Through simulations & evaluations, the paper demonstrated that the proposed scheme achieves improved performance in terms of throughput, delay, and energy efficiency compared to traditional routing approaches [38].

In [39], the author focused on addressing the challenge of high latency in such networks by proposing a routing algorithm that leverages reinforcement learning techniques. The paper provides an explanation of the key components and mechanisms involved in the proposed scheme, including the use of Markov Decision Processes (MDPs) and Q-Learning. Additionally, the paper discusses the evaluation of the algorithm through simulations, highlighting its effectiveness in reducing latency and improving the overall routing performance in opportunistic networks.

In [45], the author addressed the challenge of efficient routing in opportunistic networks by proposing a protocol that utilizes K-means clustering to organize nodes into clusters. The paper provides a detailed explanation of the protocol's key components, including cluster formation, cluster head selection, and data forwarding mechanisms. Additionally, the paper discusses the evaluation of KROp through simulations, demonstrating its effectiveness in achieving improved routing efficiency and reduced overhead in opportunistic networks.

In [53], they presented a fuzzy routing-forwarding algorithm that utilizes comprehensive node similarity in Opportunistic Social Networks. The paper demonstrated the effectiveness of the algorithm in improving message delivery rates and reducing delays compared to existing approaches. The use of fuzzy logic and comprehensive node similarity enhances the efficiency and effectiveness of routing and forwarding in Opportunistic Social Networks.

In [57], the author proposed a mechanism that forms clusters of nodes to minimize energy consumption during data forwarding. Through simulations and evaluations, the paper demonstrated that the proposed mechanism achieves significant energy savings compared to traditional forwarding methods. The findings contributed to the development of energy-efficient strategies for data transmission in opportunistic networks, improving their overall performance and prolonging network lifetime.

In [59], the author proposed a method that leverages location-based routing to make forwarding decisions based on the geographical proximity of nodes. The paper demonstrates the effectiveness of cascade learning in optimizing route selection and improving message delivery rates in opportunistic networks. The findings contributed to the development of efficient routing strategies in OppNets by considering location-based information and employing cascade learning techniques and also to the development of intelligent and adaptive routing mechanisms for dynamic IoT networks, optimizing various objectives simultaneously.

Table 3 provides the summarization of existing routing techniques used for improving QoS and security parameters using machine learning algorithms followed by the limitations in their work.

Table 4 describes the common parameters taken by the researchers in opportunistic network environment which are necessary to carry out for the successful message transmission.

TABLE 3 SUMMARIZATION OF EXISTING ROUTING TECHNIQUES USED FOR IMPROVING QOS AND SECURITY PARAMETERS USING ML ALGORITHMS

Reference	Year	Technique Used	Limitation(s)
Ladislava Smıtkova Janku and Katerina Hyniov´ [28]	2019	Unsupervised learning, Cluster analysis, K-means, Euclidean distance	Machine Learning is used to improve routing in cluster OPN.
Vidushi Vashishth et al. [29]	2019	Routing Protocols-MLProph & KNNR, ML, NN, Cascade Learning, Logistic Regression	Cascade learning is used - NN classifier & Logistic Regression in order to simplify routing in MLProph. Used so in input to low computational complexity
Fan Yuan et al. [30]	2019	Double Q-learning Routing, Reinforcement Learning	DQLR convention is proposed, which examines the routing selection of the following hop in a circulated way and takes care of the overestimation issue.
Vidushi Vashishth et al. [36]	2019	ML, Gaussian mixture model, soft clustering mechanism	Proposed method combines both context-free and context-aware routing protocols.
Deepak kumar sharma et al. [39]	2020	Reinforcement Learning, Opportunistic Networks	A novel approach for calculating the average delay between any pair of nodes, which is employed in conjunction with reinforcement

			learning to progressively learn the relationships between nodes.
Mohammed S. Al-kahtani et al. [40]	2020	Packet-loss ratio, density clustering, energy efficient, throughput, disaster routing	Introduced an energy-efficient and reliable routing protocol based on opportunistic density clustering, which intelligently conveys data using a density-clustering approach in emergency and disaster scenarios.
Yongjie Lu et al. [41]	2020	Q-learning, depth-based routing, EDORQ	Suggested an energy-efficient depth-based opportunistic routing algorithm for Underwater Wireless Sensor Networks (UWSNs), which incorporates Q-learning to ensure efficient and reliable information transmission while conserving energy.
Seifeddine Messaoud et al. [37]	2020	ML, IoT	Challenges like adaptability, security and protection, power saving, interoperability and heterogeneity, network the executives, network clog and over-burden, long-range organization, QoS, and network versatility and inclusion.
Nisha Kandhoul et al. [27]	2021	Fuzzy logic, trust based routing	The protocol determines the belief of nodes in the organization utilizing four fuzzy properties: Amiability, Forwarding Ratio, Unfabricated Packet Ratio, and Encounter Ratio.
Peizhuang Cong et al. [38]	2021	Deep Q network, Deep reinforcement learning, multi-optimality criteria	Designed, executed both incorporated and disseminated Reinforcement Learning-based Routing plans joined with multi-optimality directing models (RLR-M).

TABLE 4 SUMMARY OF SOME COMMON PARAMETERS OF OPPNETS REVIEWED

Parameters ☞ Authors ☜	**OPN Security**	**Node Security**	**Packet Delivery Ratio**	**Task Allocati-on**	**Data Forwardi-ng**	**Message Handling Capacity**	**Connecti--on Strength**	**Residual Energy of Nodes**	**Energy Optimizat-ion**
S. J. Borah et al., 2018					✓	✓		✓	✓

S. Zakhary et al., 2018								✓	✓
P. Chithaluru et al., 2019			✓						✓
S.Dhurandher et al.,2019						✓			✓
M. S. Al-kahtani et al., 2020				✓					✓
Y. Lu et al., 2020			✓						✓
J. Cui et al., 2019						✓	✓		
V. Menon, 2020							✓		
X. Wang et al., 2018					✓	✓			
N. Kandhoul et al., 2019					✓	✓			✓
S.Rashidibajgan et al., 2021						✓			
W. Zheng et al., 2019				✓					
S. Jagan, 2019			✓						
P. Kuchhal et al., 2019	✓	✓							
R. Lavanya, 2021	✓	✓					✓		
C.Avoussoukpo et al.,2021	✓	✓					✓		
X. Zhang, 2019					✓				
S. Luo, 2019			✓		✓				
A. Moradi, 2018					✓		✓		

H. Lenando et al., 2020			✓		✓				
W. Sun et al., 2021					✓				

3 RESEARCH METHODOLOGY

This review follows a deliberate methodology (See Figure 5) to finish the research cycle. We utilised an overall methodology that is Planning, Conducting, and Report writing. The means of the procedure utilised here are given underneath:

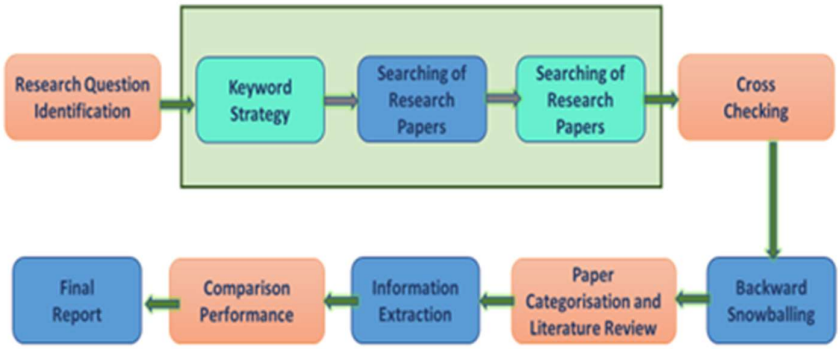

Figure 5 Research Methodology Overview

In the principal stage, Research questions are characterised to play out in this review. In the second stage, OppNet security and efficient routing techniques related research and review papers are searched using special keywords and catchphrases. Utilising explicit catchphrases is to keep up with the consideration and avoidance of applicable and non-significant research papers. Accordingly, order of security, QoS and ML in OppNets research papers is completed. Then in the last stage an extensive taxonomy is written in subsections of four.

3.1 Research Questions

This survey tries to achieve these subsequent research questions:

Research Question 1: What are the issues and limitations of current secure routing solutions in addressing the security parameter of an opportunistic network?

Research Question 2: What can be the mechanism for establishing secure communication through trusted nodes and what kind of procedures and issues are there in integration of security and QoS parameters?

Research Question 3: What is the effect of an integrated approach to support secure QoS routing in Opportunistic Networks?

3.2 Strategy of searching Research Paper

Observing the relevant research distributions is a huge task to isolate the right information for survey research [74]. In this subsection, keywords and techniques are picked and used in this review for keeping right and finding critical research publication.

Search Keywords: With the assistance of research questions, we settled significant keywords which are identified with OppNet, QoS, and Trust Management. In case we sum up

our inquiry string, then, at that point, it very well may be the mix of combination and incoherence of various associated substring catchphrases. A rundown of keywords utilised by us is specified in table 5.

TABLE 5 SEARCH KEYWORDS

String	Keywords
X1	Opportunistic Network, OppNet, Opportunistic network environment
X2	Quality of service, QoS
X3	Trust, peer nodes, secure, trust management

S = x1 AND x2 AND x3 or (1)

S = x1 OR x2 OR x3, where x1, x2, x3 are the different keywords (2)

Exclusion Criteria: In spite of the fact that we looked through utilising explicit catchphrases to track down significant papers, indexed lists had a broad number of distributions and among many of them, many are as yet inappropriate for us. Thus, we utilise some rejection/exclusion techniques. These techniques are:

First, out of research papers available in numerous languages, we consider only those that were written in English language in light of the fact that the vast majority of the logical research papers are available in English.

Secondly, focus only on detailed information related to the topic. Short papers with 6–8 pages are barred by us on the grounds that a large portion of such papers are expansions of their fundamental papers.

Third, we attempted to keep away from copy papers utilising a procedure like contrasting the authors, title, and conceptual text/abstract.

Backward Snowballing and Cross checking: The principal objective of Backward Snowballing and cross-checking is to find those conceivable lost important papers which might not have been looked through utilising our search keywords. In this cycle, we looked in the references of our fundamental looked through papers.

Paper Categorization and Literature Review: In the wake of tracking down appropriate papers, the following stage is to group papers dependent on trust in the executives' procedures that talked about OppNet security and those that don't. After it, an itemised writing survey of these research and review papers is performed.

Information Extraction: From the prior work mentioned in literature review, we additionally remove data to distinguish tended to security and trust boundaries and to quality of service of the network. These boundaries are the fundamental mainstays of our analogy among research papers.

Comparison Performed and final report: In the subsequent stage, a comparison dependent on trust, security and quality of service parameters are performed among the executives' methods proposed by research papers shortlisted for writing surveys. At long last, in view of the correlation outcomes, a report is ready and examined.

4.3 Statistics of examined publications

Subsequent to finishing the course of research papers search, we tracked down almost 200 publications. Subsequent to applying prohibition and Backward Snowballing procedures, we shortlisted 70 research papers that fit this study paper. After studying them, we arranged these shortlisted papers in three classes such the first is QoS parameters for efficient routing in an opportunistic network, second is on Security parameters and third on existing routing techniques used by researchers for improving QoS and security parameters using machine learning algorithms.

Figure 6 & Figure 7 shows the conveyance of chosen research papers dependent on publication year and Database respectively. We consider almost 58% of published papers from the year 2018 to 2022. Also, assuming that we talk about Databases, the vast majority of the papers are from Elsevier, Springer and IEEE.

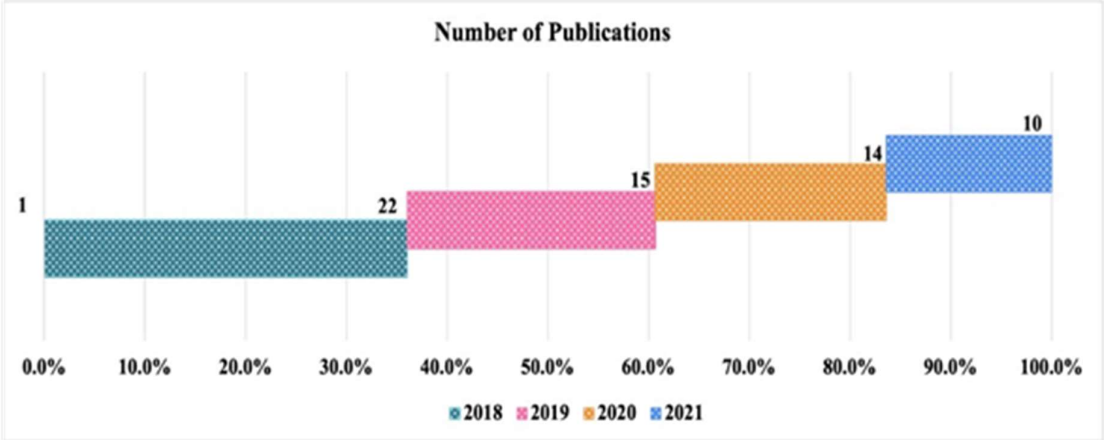

Figure 6 Distribution of papers according to year publication year

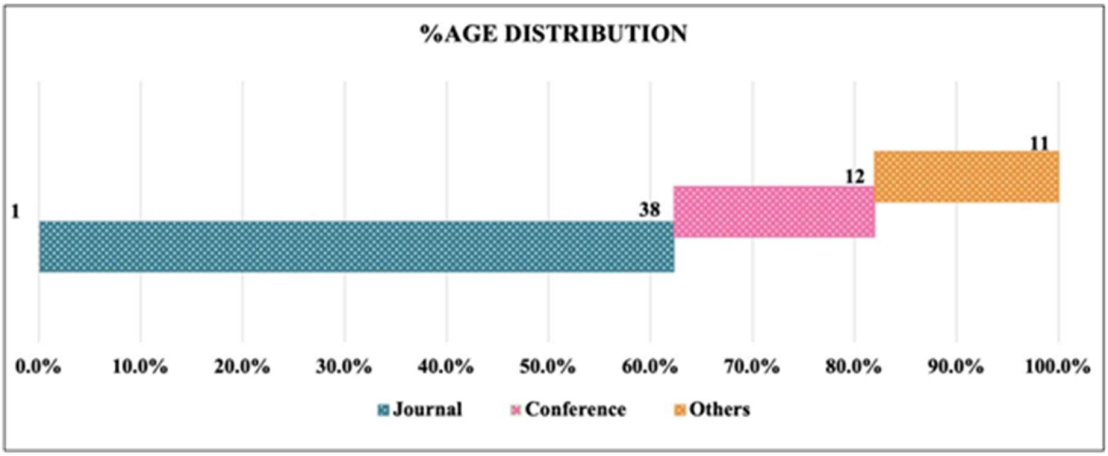

Figure 7 Distribution of papers based on their type

Figure 8(a) shows the word cloud of keywords of selected articles of all which are comprised in this survey. We can analyse from the cloud representation that opportunistic network, efficient routing, machine learning and security are the primary catchphrase for looking through writing over the all vaults like Elsevier, Springer IEEE, and so forth.

As far as we could possibly know, we observed all applicable distributions utilising appropriate watchword determination, prohibition technique, and Backward Snowballing. Similarly Figure 8(b) represents the word cloud of titles of selected articles.

Figure 8 (a) Word cloud of keywords of selected articles

Figure 8 (b) Word cloud of titles of selected articles

4 TAXONOMY

OppNets aim to handle the unpredictable nature of information exchange. In these networks, messages are stored at intermediate nodes without relying on a direct forwarder. This store-carry-forward approach helps overcome challenges such as unpredictable availability, indirect paths, high-error rates, and delays in network. Nodes carrying information navigate the environment to find a suitable data forwarding node or hub. By employing this method, OppNets aim to effectively address the uncertainties and limitations inherent in the network, ensuring reliable and efficient data transmission.

This review examines various routing protocols and mobile opportunistic network models, as well as simulation tools available for studying these environments. It also discusses challenges such as energy requirements and constraints [40], trust among peer nodes [26], and secure data forwarding [41][75]. The paper introduces several applications, including real-time contextual analysis. Based on the review, future directions are explored to address the challenges faced in the current scenario. Additionally, It has been noted that a significant number of researchers have concentrated their efforts on epidemic [9][33], spray and wait [32], and ProPHET [21][35] protocols as the basis for their studies in routing protocols.

4.3 Evolution of OppNets

The evolution of OppNets, can be traced back to the development of MANETs [16]. However, OppNets emerged as a solution to overcome the limitations of MANETs reliance on continuous end-to-end connectivity. In this section, we explore the historical progression and key advancements that have shaped OppNets.

Initially rooted in MANETs, OppNets introduced the concept of operating in an interruption-tolerant mode, where nodes function independently of fixed infrastructure or docking stations. Instead, they rely on opportunistic encounters to exchange information and share content.

OppNets can be classified as a subset of DTNs [30][31], recognizing the intermittent nature of communication opportunities. Unlike traditional networks, OppNets embrace the challenges posed by infrequent or non-existent end-to-end paths between nodes. These strategies address the challenges of variable latencies, high error rates, and the absence of continuous paths.

Dynamic connectivity is a defining characteristic of OppNets, with nodes constantly moving and changing network associations. This dynamic nature presents challenges in routing, resource allocation, and maintaining network connectivity.

Security [73] is a critical concern in OppNets, as they often operate in environments with limited physical security. Protecting against malicious attacks and unauthorized access requires robust security mechanisms and privacy-preserving techniques.

The evolution of OppNets has been driven by the need to enable communication in scenarios where traditional networks fail. Advances in routing algorithms, data dissemination techniques, and resource management strategies have contributed to their growth and potential applications in various domains. Figure 9 illustrates the evolution of opportunistic networks.

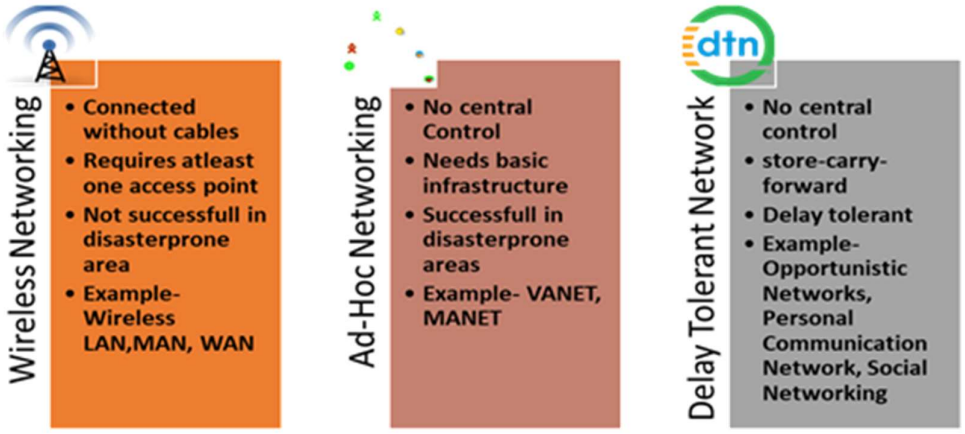

Figure 9 Evolution of OppNets

4.3 Routing techniques in OppNets

Routing in OppNets is composed of two factors:

- For route discovery: In opportunistic networks, there is no predefined route between the source and destination; instead, dynamic paths are formed using intermediate nodes.
- Finding the next forwarding node: Identifying a suitable helper node that can efficiently forward data to the destination as quickly as possible.

In this section we have discussed possible routing techniques in OppNets. Figure 10 illustrates the various types of routing protocols [68][69] that are used in OppNets to make the process efficient and the transmission successful.

In flooding-based routing protocol [16], the node generally floods the information to be sent among the neighbour's nodes. It gives the highest overhead ratio and due to this the performance of the network also gets degraded as it grows. Since it is easy to understand and execute, it is widely used. Spray-and-Wait routing protocols [32] and Epidemic routing protocol [9][33] are some examples of flooding-based routing techniques.

In the Forwarding-based routing protocol [12], nodes transmit the required data once a specific condition is met. This category typically has the fewest hops, but it comes with a lower delivery success rate and higher latency. Routing protocols like the direct delivery protocol and first contact protocol fall into this category.

To overcome the high delays and to increase the delivery probability, the probability-based routing protocol follows the probability concept. In this the desired information advances to just those hubs having high probability for effective delivery [10][11][21][34][35], that is why it requires extra memory for putting away probability values. The widely used protocol-PRoPHET [21][35][44] is a probability-based routing mechanism and MaxProp also comes under the same.

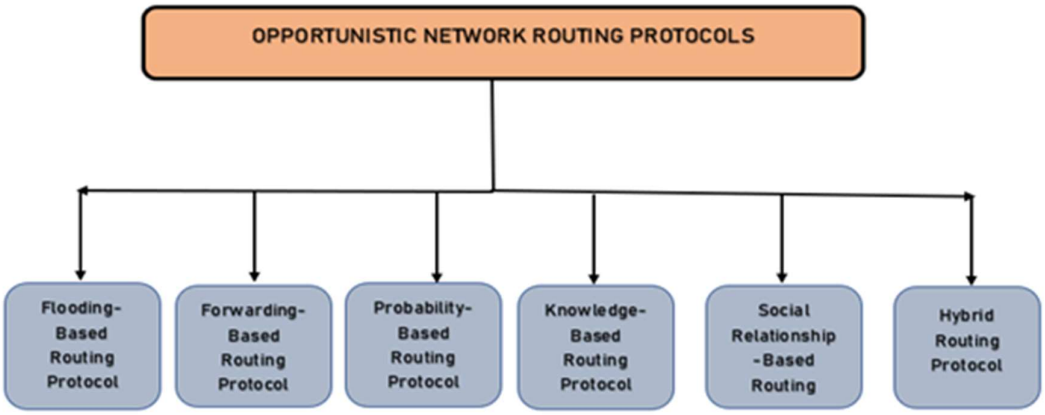

Figure 10 Types of Routing protocols used in Opportunistic Networks

Another type of routing technique related to OppNet is knowledge-based routing protocol [23], in which every single node keeps a data set about the information on neighbour hubs for information spread. It consumes a large amount of memory for keeping a knowledge database. Epidemic Oracle protocol is an example of such techniques but are not generally used due to high overhead and delays.

Further in social relationship-based routing protocols [48], the dissemination of the wanted data to the transitional hub as per the social-relationship factor. Nodes that are associated with countless nodes will get more opportunities to go about as halfway. The advantage of using this protocol is its smallest delay and reduced message drops. Example is- FRESH protocol.

The last category of the routing techniques is hybrid routing protocol which includes RAPID protocol and follows the method of more than one category of OppNet protocols [46][58][60]. The execution relies upon the similarity of the protocols to be used.

4.3 Common Parameters used in OppNets

In Opportunistic Networks (OppNets), maintaining security and Quality of Service (QoS) are crucial factors for network performance. However, the decentralized architecture of

OppNets poses challenges in establishing trust among peer nodes, leading to a less secure environment for message transmission [17][18]. The distributed nature of OppNets restricts the use of traditional security systems, such as centralized trusted authorities and cryptography. Therefore, network security [18] becomes even more critical, alongside QoS parameters like reliable packet delivery, increased message delivery probability, minimal message drops, and reduced packet delivery latency. Figure 11 illustrates the QoS parameters in OppNets.

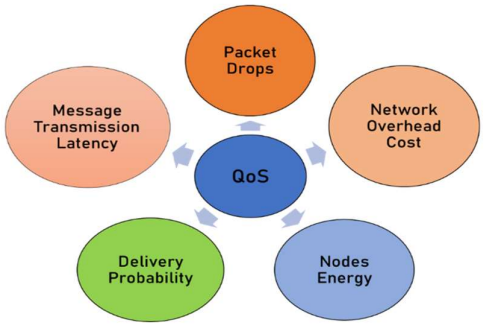

Figure 11 Quality of Service parameters in OppNets

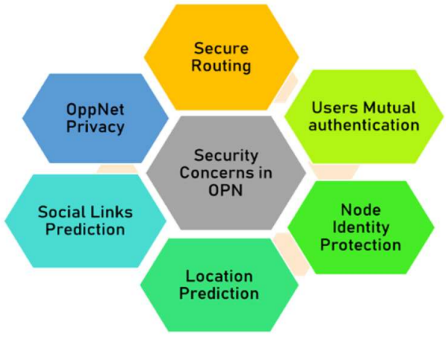

Figure 12 Security Concerns in OPN

In Figure 12, shows the parameters related to security of the OppNet. To ensure secure routing in OppNets [64-67], it is essential to address these parameters. Firstly, mutual authentication among users within the network is crucial. The preservation of node identity, whether disclosed or undisclosed to other peer nodes, is important to prevent malicious attackers [65][7] from introducing fake nodes into the network. Additionally, the intentional dropping of packets by malicious nodes should be minimized to avoid disrupting communication and increasing network overhead.

An efficient routing technique [57] should also incorporate node location prediction. Predicting the social links between nodes enhances the selection of nodes for effective communication. The better nodes can interact and collaborate, the more efficient they become in transmitting messages and packets.

Lastly, OppNet privacy [66] presents a constant challenge due to the network's uncertain topology and intermittent connectivity. Safeguarding privacy within this networking environment remains a significant concern.

5 CONCLUSION

This paper presents a comprehensive review focusing on three types of research papers related to opportunistic network routing techniques. Firstly, it explores the QoS parameters essential for efficient routing in opportunistic networks. Secondly, it delves into the security parameters that contribute to secure communication within these networks. Lastly, it examines the existing routing techniques employed by researchers to enhance QoS and security parameters using machine learning algorithms.

Considering the increasing significance of distributed routing architecture in opportunistic networks, there is a growing need for in-depth surveys and studies in this field. Figure 13 provides a knowledge map visualization of the opportunistic network environment, highlighting its diverse applications in our daily lives. The review also addresses the underlying

technologies used in these networks and emphasizes the importance of studying their architecture for effective implementation and evaluation, focusing on specific parameters of interest.

6 DISCUSSIONS AND FUTURE SCOPE

The discussion of QoS parameters has revealed the importance of factors such as packet delivery, message latency, and dropped message count in ensuring efficient routing in opportunistic networks. Additionally, the examination of security parameters has underscored the need for mutual authentication, preservation of node identity, and prevention of malicious attacks to maintain a secure communication environment. The review has also highlighted the use of machine learning algorithms in routing techniques, particularly in predicting node locations and selecting nodes for positive communication.

In conclusion, this review paper has provided an extensive analysis of opportunistic network routing techniques, with a particular focus on QoS and security parameters. The study has highlighted the significance of distributed routing in opportunistic networks and emphasized the need for further research in this field. The discussion has explored various routing approaches and their potential for enhancing QoS and security through the utilization of machine learning algorithms. The knowledge map presentation has illustrated the wide-ranging applications of opportunistic networks in our daily lives.

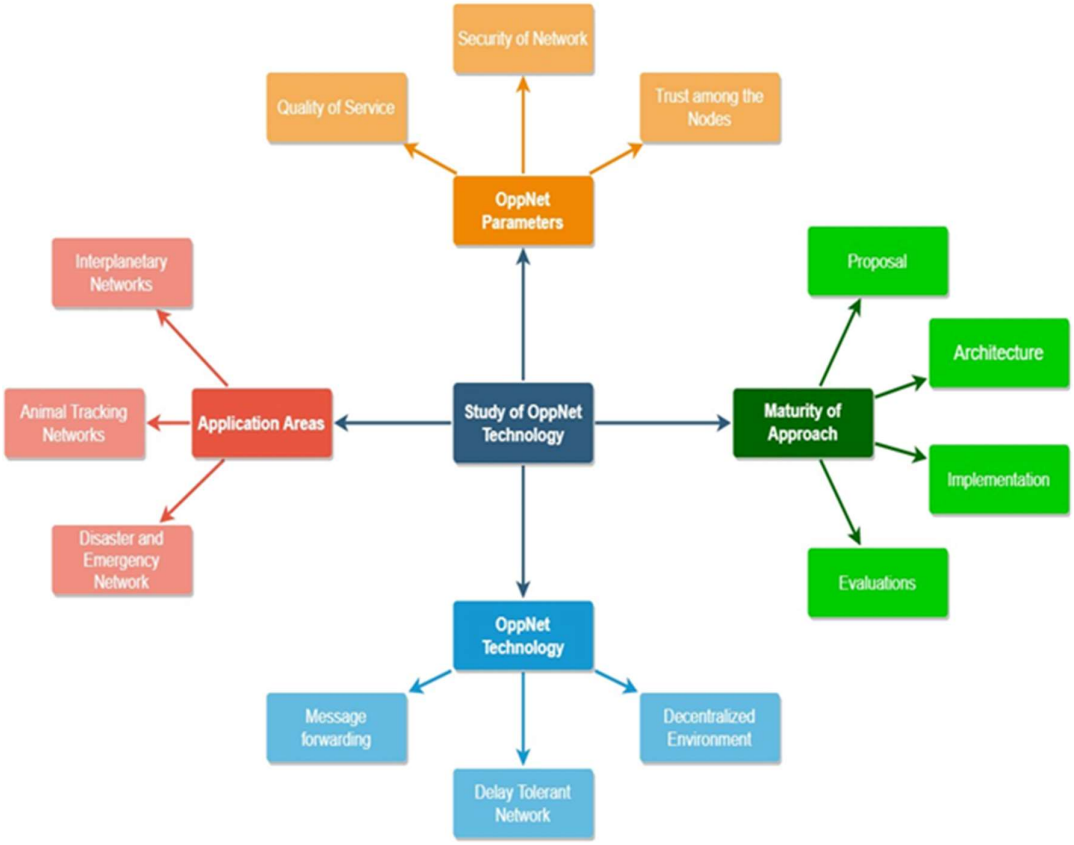

Figure 13 Knowledge Map of OppNet applications

Moving forward, further research is warranted in the field of opportunistic network routing. Future studies could explore novel approaches for enhancing QoS and security parameters, including the integration of advanced machine learning techniques. Additionally, the

development of efficient routing techniques that consider the uncertain topology and sporadic connectivity of opportunistic networks would be valuable. Furthermore, the evaluation of these techniques using specific parameters of interest and real-world scenarios would provide practical insights. Finally, the exploration of emerging technologies, such as blockchain and edge computing, in the context of opportunistic networks could open up new avenues for research and innovation.

The paper begins by presenting an iteratively refined classification framework that aids in comprehending the opportunistic network environment. It provides a comprehensive analysis of the existing literature, primarily focusing on routing techniques proposed by previous researchers between the years 2018 and 2022. By examining these studies, valuable insights into the current state of routing in opportunistic networks can be gained.

REFERENCES

[1] Lohachab, A., & Jangra, A. (2019, March). Opportunistic Internet of Things (IoT): Demystifying the Effective Possibilities of Opportunistic Networks Towards IoT. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 1100-1105). IEEE.

[2] Kandhoul, N., & Dhurandher, S. K. (2018, August). An asymmetric RSA-based security approach for opportunistic IoT. In the International Conference on Wireless Intelligent and Distributed Environment for Communication (pp. 47-60). Springer, Cham.

[3] Chithaluru, P., Tiwari, R., & Kumar, K. (2019). AREOR–adaptive ranking based energy efficient opportunistic routing scheme in Wireless Sensor Network. Computer Networks, 162, 106863.

[4] Sun, W., Wang, Z., & Zhang, G. (2021). A QoS-guaranteed intelligent routing mechanism in software-defined networks. Computer Networks, 185, 107709.

[5] Menon, V., Midhunchakkaravarthy, D., John, S., Jacob, S., & Mukherjee, A. (2020). A secure and energy-efficient opportunistic routing protocol with void avoidance for underwater acoustic sensor networks. Turkish Journal of Electrical Engineering & Computer Sciences, 28(4), 2303-2315.

[6] Xu, G., Wang, X., Zhang, N., Wang, Z., Yu, L., & He, L. (2021). A Routing Algorithm for the Sparse Opportunistic Networks Based on Node Intimacy. Wireless Communications and Mobile Computing, 2021.

[7] Dhungana, A., & Bulut, E. (2021). Energy balancing in mobile opportunistic networks with wireless charging: Single and multi-hop approaches. Ad Hoc Networks, 111, 102342.

[8] Lenando, H., Kurd Ali, A. H., Chaoui, S., & Alrfaay, M. (2021). Innovative mutual information-based weighting scheme in stateless opportunistic networks.

[9] Jagan, S. Efficient Source Balanced Routing Protocol To Enhance QoS Factors In Disruption Tolerant Networks.

[10] Nikodem, M., Slabicki, M., & Bawiec, M. (2020). Efficient communication scheme for Bluetooth low energy in large scale applications. Sensors, 20(21), 6371.

[11] Gueguen, C., & Merlhe, C. (2020). Fair energy efficient scheduler providing high system capacity for wireless networks. SN Applied Sciences, 2(12), 1-15.

[12] Zhang, X., & Luo, S. (2019). On-demand data forwarding in mobile opportunistic networks: backbone-based approach. IET Communications, 13(19), 3336-3343.
[13] Zheng, W., Chen, Z., Wu, J., & Liu, K. (2020). Cooperative-routing mechanism based on node classification and task allocation for opportunistic social networks. IET Communications, 14(3), 420-429. doi:10.1049/iet-com.2019.0756
[14] Li, J., He, X., Zhao, D., Yang, G., He, D., & Chan, S. (2020). Delay-aware and cost-efficient probabilistic transmission for opportunistic networks. IET Networks, 9(6), 372-377. doi:10.1049/iet-net.2020.0082
[15] Avoussoukpo, C. B., Xu, C., & Tchenagnon, M. (2020). Ensuring Users Privacy and Mutual Authentication in Opportunistic Networks: A Survey. Int. J. Netw. Secur., 22(1), 118-125.
[16] Li, J., He, X., Zhao, D., Yang, G., He, D., & Chan, S. (2020). Delay-aware and cost-efficient probabilistic transmission for opportunistic networks. IET Networks, 9(6), 372-377. doi:10.1049/iet-net.2020.0082
[17] Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C. (2021). TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network. Security and Communication Networks, 2021, 1-9. doi:10.1155/2021/5521713
[18] Kandhoul, N., Dhurandher, S. K., & Woungang, I. (2019). T_CAFE: A Trust based Security approach for Opportunistic IoT. IET Communications, 13(20), 3463-3471. doi:10.1049/iet-com.2019.0657
[19] Kandhoul, N., & Dhurandher, S. K. (2019). An Asymmetric RSA-Based Security Approach for Opportunistic IoT. Lecture Notes on Data Engineering and Communications Technologies 2nd International Conference on Wireless Intelligent and Distributed Environment for Communication, 47-60. doi:10.1007/978-3-030-11437-4_5
[20] Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Hu, B., . . . Guo, Y. (2018). A Privacy-Preserving Message Forwarding Framework for Opportunistic Cloud of Things. IEEE Internet of Things Journal, 5(6), 5281-5295. doi:10.1109/jiot.2018.2864782
[21] Borah, S. J., Dhurandher, S. K., Woungang, I., Kandhoul, N., & Rodrigues, J. J. (2018). An Energy-Efficient Location Prediction-Based Forwarding Scheme for Opportunistic Networks. 2018 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2018.8422305
[22] Kandhoul, N., & Dhurandher, S. K. (2021). An Efficient and Secure Data Forwarding Mechanism for Opportunistic IoT. Wireless Personal Communications, 118(1), 217-237. doi:10.1007/s11277-020-08010-w
[23] Avoussoukpo, C. B., Ogunseyi, T. B., & Tchenagnon, M. (2021). Securing and Facilitating Communication Within Opportunistic Networks: A Holistic Survey. IEEE Access, 9, 55009-55035. doi:10.1109/access.2021.3071309
[24] Lavanyaa, R. (2021). Energy Efficient with Trust and Qos-Aware Optimal Multipath Routing Protocol Based on Elephant Herding Optimization for Iot Based Wireless Sensor Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 979-990.

[25] Dhurandher, S. K., Woungang, I., Singh, J., & Borah, S. J. (2019). Energy aware routing for efficient green communication in opportunistic networks. IET Networks, 8(4), 272-279. doi:10.1049/iet-net.2018.5106

[26] Rashidibajgan, S., Hupperich, T., Doss, R., & Förster, A. (2021). Secure and privacy-preserving structure in opportunistic networks. Computers & Security, 104, 102208. doi:10.1016/j.cose.2021.102208

[27] Kandhoul, N., & Dhurandher, S. K. (2020). Fuzzy Trust Based Secure Routing Protocol for Opportunistic Internet of Things. Advances in Intelligent Systems and Computing International Conference on Innovative Computing and Communications, 749-755. doi:10.1007/978-981-15-5148-2_65

[28] Janků, L. S., & Hyniová, K. (2019). Improvement of Routing in Opportunistic Communication Networks of Vehicles by Unsupervised Machine Learning. Engineering Applications of Neural Networks Communications in Computer and Information Science, 412-423. doi:10.1007/978-3-030-20257-6_35

[29] Vashishth, V., Chhabra, A., & Sharma, D. K. (2019). A Machine Learning Approach Using Classifier Cascades for Optimal Routing in Opportunistic Internet of Things Networks. 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). doi:10.1109/sahcn.2019.8824952

[30] Yuan, F., Wu, J., Zhou, H., & Liu, L. (2019). A Double Q-Learning Routing in Delay Tolerant Networks. ICC 2019 - 2019 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2019.8761526

[31] Wu, J., Yuan, F., Guo, Y., Zhou, H., & Liu, L. (2021). A Fuzzy-Logic-Based Double Q -Learning Routing in Delay-Tolerant Networks. Wireless Communications and Mobile Computing, 2021, 1-17. doi:10.1155/2021/8890772

[32] Cui, J., Cao, S., Chang, Y., Wu, L., Liu, D., & Yang, Y. (2019). An Adaptive Spray and Wait Routing Algorithm Based on Quality of Node in Delay Tolerant Network. IEEE Access, 7, 35274-35286. doi:10.1109/access.2019.2904750

[33] Dhurandher, S. K., Singh, J., Obaidat, M. S., Woungang, I., Srivastava, S., & Rodrigues, J. J. (2020). Reinforcement Learning-Based Routing Protocol for Opportunistic Networks. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). doi:10.1109/icc40277.2020.9149039

[34] Kandhoul, N.Dhurandher, S. K., & Woungang, I. (2021). Random forest classifier-based safe and reliable routing for opportunistic IoT networks. International Journal of Communication Systems, 34(1), e4646.

[35] Borah, S. J., Dhurandher, S. K., Woungang, I., Kandhoul, N., & Rodrigues, J. J. (2018). An Energy-Efficient Location Prediction-Based Forwarding Scheme for Opportunistic Networks. 2018 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2018.8422305

[36] Vashishth, V., Chhabra, A., & Sharma, D. K. (2019). GMMR: A Gaussian mixture model based unsupervised machine learning approach for optimal routing in opportunistic IoT networks. Computer Communications, 134, 138-148. doi:10.1016/j.comcom.2018.12.001

[37] Messaoud, S., Bradai, A., Bukhari, S. H., Quang, P. T., Ahmed, O. B., & Atri, M. (2020). A survey on machine learning in Internet of Things: Algorithms, strategies, and applications. Internet of Things, 12, 100314. doi:10.1016/j.iot.2020.100314

[38] Cong, P., Zhang, Y., Liu, Z., Baker, T., Tawfik, H., Wang, W., . . . Li, F. (2021). A deep reinforcement learning-based multi-optimality routing scheme for dynamic IoT networks. Computer Networks, 192, 108057. doi:10.1016/j.comnet.2021.108057

[39] Sharma, D. K., Gupta, S., Malik, S., & Kumar, R. (2020). Latency-aware reinforced routing for opportunistic networks. IET Communications, 14(17), 2981-2989. doi:10.1049/iet-com.2020.0149

[40] Al-Kahtani, M., Karim, L., & Khan, N. (2020). Efficient Opportunistic Routing Protocol for Sensor Network in Emergency Applications. Electronics, 9(3), 455. doi:10.3390/electronics9030455

[41] Lu, Y., He, R., Chen, X., Lin, B., & Yu, C. (2020). Energy-Efficient Depth-Based Opportunistic Routing with Q-Learning for Underwater Wireless Sensor Networks. Sensors, 20(4), 1025. doi:10.3390/s20041025

[42] Garg, P., Dixit, A., Sethi, P., & Pinheiro, P. R. (2020). Impact of Node Density on the QoS Parameters of Routing Protocols in Opportunistic Networks for Smart Spaces. Mobile Information Systems, 2020. https://link.gale.com/apps/doc/A639994217/AONE?u=anon~ee625161&sid=googleScholar&xid=6437c159

[43] Moradi, A., & Shah-Mansouri, V. (2019). Opportunistic content dissemination in mobile social networks via adjustment of user selfishness. IET Networks, 8(2), 126–137. https://doi.org/10.1049/iet-net.2018.5013 Lindgren, A., Doria, A., Schelén, O.: 'Probabilistic routing in intermittently connected networks', Sigmob. Mob. Comput. Commun. Rev., 2003, 7, (3), pp. 19–20.

[44] Du, P., Yoo, S., Zhao, Q., Chen, M., & Gerla, M. (2018). Towards Opportunistic Resource Sharing in Mobile Social Networks. Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. doi:10.1145/3209582.3225201

[45] Sharma, D. K., Dhurandher, S. K., Agarwal, D., & Arora, K. (2018). KROp: K-Means clustering based routing protocol for opportunistic networks. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1289-1306. doi:10.1007/s12652-018-0697-3

[46] Kosmides, P., & Lambrinos, L. (2018). Intelligent Routing in Mobile Opportunistic Networks. 2018 Global Information Infrastructure and Networking Symposium (GIIS). doi:10.1109/giis.2018.8635592

[47] Borrego, C., Borrell, J., & Robles, S. (2019). Hey, influencer! Message delivery to social central nodes in social opportunistic networks. Computer Communications, 137, 81-91. doi:10.1016/j.comcom.2019.02.003

[48] Zakhary, S., & Benslimane, A. (2018). On location-privacy in opportunistic mobile networks, a survey. Journal of Network and Computer Applications, 103, 157-170. doi:10.1016/j.jnca.2017.10.022

[49] Dhungana, A., & Bulut, E. (2019). Loss-Aware Efficient Energy Balancing in Mobile Opportunistic Networks. 2019 IEEE Global Communications Conference (GLOBECOM). doi:10.1109/globecom38437.2019.9014073

[50] Xu, G., Xu, Z., He, Y., Zhou, J., Guo, Y., & Guo, X. (2018). Opportunistic Networks Routing Algorithm Based on the Uncertain Social Relationship. 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)). doi:10.1109/cscwd.2018.8465201

[51] Nigam, R., Sharma, D. K., Jain, S., Gupta, S., & Ghosh, S. (2019). Bonding Based Technique for message forwarding in Social Opportunistic Network. Scalable Computing: Practice and Experience, 20(1), 1-15. doi:10.12694/scpe.v20i1.1469

[52] Dhurandher, S. K., Borah, S. J., Woungang, I., Tibarewal, S., & Barolli, L. (2018). DEEP: Distance and encounter based energy-efficient protocol for opportunistic networks. Journal of High Speed Networks, 24(2), 119-131. doi:10.3233/jhs-180585

[53] Liu, K., Chen, Z., Wu, J., & Wang, L. (2018). FCNS: A Fuzzy Routing-Forwarding Algorithm Exploiting Comprehensive Node Similarity in Opportunistic Social Networks. Symmetry, 10(8), 338. doi:10.3390/sym10080338

[54] Liu, K., Chen, Z., Wu, J., Xiao, Y., & Zhang, H. (2018). Predict and Forward: An Efficient Routing-Delivery Scheme Based on Node Profile in Opportunistic Networks. Future Internet, 10(8), 74. doi:10.3390/fi10080074

[55] Chancay-Garcia, L., Hernandez-Orallo, E., Manzoni, P., Calafate, C. T., & Cano, J. (2018). Evaluating and Enhancing Information Dissemination in Urban Areas of Interest Using Opportunistic Networks. IEEE Access, 6, 32514-32531. doi:10.1109/access.2018.2846201

[56] Borah, S. J., Dhurandher, S. K., Woungang, I., Kumar, V., & Barolli, L. (2017). A multi-objectives based technique for optimized routing in opportunistic networks. Journal of Ambient Intelligence and Humanized Computing, 9(3), 655-666. doi:10.1007/s12652-017-0462-z

[57] Santos, G., Soares, D., Carvalho, C., & Mota, E. (2021). An Energy-Saving Forwarding Mechanism Based on Clustering for Opportunistic Networks. Sensors, 21(22), 7427.

[58] Galarza, C. E., Palma, J. M., Morais, C. F., Utria, J., Carvalho, L. P., Bustos, D., & Oliveira, R. C. (2021). A Novel Theoretical Probabilistic Model for Opportunistic Routing with Applications in Energy Consumption for WSNs. Sensors, 21(23), 8058.

[59] Singh, J., Obaidat, M. S., & Dhurandher, S. K. (2021, November). Location based Routing in Opportunistic Networks using Cascade Learning. In 2021 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.

[60] Su, B., Du, C., & Huan, J. (2020). Trusted opportunistic routing based on Node Trust model. IEEE Access, 8, 163077–163090. https://doi.org/10.1109/access.2020.3020129

[61] Opportunistic data forwarding. (2020). Encyclopedia of Wireless Networks, 1043–1043.

[62] Kumar, A., Gupta, N., & Tapwal, R. (2020). Trust aware scheme based malicious nodes detection under cooperative spectrum sensing for Cognitive Radio Networks. https://doi.org/10.36227/techrxiv.12052662

[63] Mantas, N., Louta, M., Karapistoli, E., Karetsos, G. T., Kraounakis, S., & Obaidat, M. S. (2017). Towards an incentive-compatible, reputation-based framework for stimulating

cooperation in opportunistic networks: A survey. IET Networks, 6(6), 169–178. https://doi.org/10.1049/iet-net.2017.0079

[64] Su B., Du C.,, & Huan J. (2020). Trusted opportunistic routing based on Node Trust model. IEEE Access. vol. 8. pp. 163077–163090.

[65] Singh J., Woungang I., Dhurandher S. K., Khalid K. (2022). A jamming attack detection technique for opportunistic networks. Internet of Things. vol. 17. p. 100464.

[66] Wang X., Ning Z., Zhou M. C., Hu X., Wang L., Hu B., Kwok R. Y., Guo Y. (2018). A privacy-preserving message forwarding framework for Opportunistic cloud of things. IEEE Internet of Things Journal. vol. 5. no. 6. pp. 5281–5295.

[67] Kumar A., Gupta N., Tapwal R. (2021). Trust aware scheme based malicious nodes detection under cooperative spectrum sensing for Cognitive Radio Networks.

[68] Mangla, M., Sharma, N., & Mittal, P. (2021). A fuzzy expert system for predicting the mortality of COVID'19. Turkish Journal of Electrical Engineering and Computer Sciences, 29(3), 1628-1642.

[69] Poonam, & Nagpal, C. K. (2018). A game theory based solution for security challenges in CRNs. 3D Research, 9, 1-24.

[70] Aggarwal, R., Verma, J., & Siwach, M. (2022). Small files' problem in Hadoop: A systematic literature review. Journal of King Saud University-Computer and Information Sciences, 34(10), 8658-8674.