Received March 8, 2021, accepted March 25, 2021, date of publication April 6, 2021, date of current version April 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071309

Securing and Facilitating Communication Within Opportunistic Networks: A Holistic Survey

COSSI BLAISE AVOUSSOUKPO[1], TAIWO BLESSING OGUNSEYI[1], (Member, IEEE), AND MARIUS TCHENAGNON[2]

[1]International Faculty of Applied Technology, Yibin University, Yibin 644000, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Cossi Blaise Avoussoukpo (omramson@yahoo.fr)

This work was supported by the Yibin University.

ABSTRACT Opportunistic Networks is a new concept that is increasingly gaining ground since it appears as a concrete example of the Internet of Things, Internet of Vehicles, Industrial Internet of Things, and the Internet of Everything with Mobile ad hoc Networks' characteristics. An Opportunistic Network starts with a Seed OppNet that sets up the network; expands from the Seed OppNet to an extended Seed OppNet through devices' discovery. The characteristics of Opportunistic Networks make OppNets more challenging than any other networks. So, a deep understanding of OppNets' characteristics and demands is an unavoidable precondition before proposing any OppNets related scheme. However, under OppNets' constraints, the relevance of the Opportunistic Networks related articles in literature is yet to be established. Also, most surveys tackling Opportunistic Networks do not give a complete insight into what Opportunistic Networks stand for. This work reviews state of the art on Opportunistic Networks providing three main contributions. First, resorting to the primary definition of Opportunistic Networks, it elucidates what OppNets are, pointing out the particularities of an OppNet, its domains of applications, and challenges. Second, it provides a comprehensive review that encompasses most Opportunistic Networks' research areas: routing, intrusion detection, authentication, privacy protection, data aggregation, and the technology for OppNets, organising them in a taxonomy. Third, it evaluates the role of the Seed OppNet in Opportunistic Networks related schemes. Any proposed OppNets related scheme, to be relevant to OppNets' research, should include OppNets' characteristics and demands.

INDEX TERMS Internet of Things (IoT), opportunistic networks security, opportunistic networks privacy protection, Seed OppNet, communication.

I. INTRODUCTION

The statistic reveals significant changes for the year 2023 as far as Internet users, devices connections, Internet of Things' applications, and mobility growth are concerned [1]. The Internet users that were 3.9 billion in 2018 will become 5.3 billion (about 66 per cent of the world inhabitants). Also, the number of devices connected to the Internet might triple the global population, taking machine-to-machine connections and connected Things' applications to an unprecedented rate. Moreover, mobile connectivity will increase significantly. The various breakthrough in Technology in general, and in Communications, in particular, has given rise to many concepts. The concept of the Internet of Things (IoT) [2] came as a new beau ideal that is supposed to integrate several complex technologies. As devices get smarter and connected to the Internet, from the concept of the Internet of Things, emerged; the concept of the Internet of Vehicle (IoV) [3], the concept of Industrial Internet of Things (IIoT) [4] that should provide connectivity to machines, robots, and sensors, and finally the concept of the Internet of Everything which is Everything connected in a vast distributed Network. On the other hand, the advances in wireless and infrastructure-less networks birthed Mobile ad hoc Networks [5] followed by the advent of Delay Tolerant Networks, Unstructured Networks, and Self-Configured Networks. The Internet of Things, the Internet of Vehicle, the Industrial Internet of Vehicle, the Internet of Everything (IoE) [7], and the Mobile

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenhui Yuan.

ad hoc Networks, all together, fathered Opportunistic Networks(OppNets) [8], [9]. Opportunistic Networks classified as Self-Configured Networks came as a natural evolution of research on Mobile ad hoc Networks. OppNets with users as vital components rely upon devices' discovery. An OppNet's life starts and ends with a Seed OppNet which defines the Opportunistic Networks' mission. To achieve its mission, the Seed OppNet invites other nodes called Helpers. The Seed OppNet and Helpers formed an extended or expanded Seed OppNet where all resources are put together to complete a pre-defined goal. After the completion of the Seed OppNet's mission, Helpers are released. So, Opportunistic Networks are temporary networks. The characteristics of Opportunistic Networks make OppNets more challenging than any other networks. Therefore, a deep understanding of OppNets' characteristics and demands is an unavoidable precondition before proposing any OppNets related scheme. Although Opportunistic Networks is a relatively new area of research, it is increasingly capturing the attention of researchers such that there are more and more articles addressing OppNets' issues. Researchers tackle topics across; routing, authentication, privacy protection, intrusion detection, the technology for OppNets, and data aggregation. However, despite the attention that the area of OppNets is gaining within the research community, schemes proposed for Opportunistic seem not to include OppNets' characteristics and demands, and most importantly, the Seed OppNet which is of cardinal importance for any OppNet is barely discussed. A Seed OppNet sets up an OppNet, defines its mission, and plays a vital role in its transition from Seed OppNet to extended or expanded Seed OppNet [10]. With the assumption that Opportunistic Networks (OppNets) have an explicit definition and operate under specific constraints with a Seed OppNet as its nucleus element, this paper aims to study the relevance of the Opportunistic Networks proposed articles under OppNets' constraints. More precisely, considering the domains of intrusion detection, authentication, routing, privacy protection, data aggregation, and the technology for OppNets, this paper studies the role or the degree of involvement of the Seed OppNet in OppNets related articles with the following contributions: First, for the sake of dispelling confusion, this article characterises Opportunistic Networks, points out its particularities, domains of applications, and challenges. Second, it summarises the contributions of the existing survey, in literature, and proves the need for a holistic survey. Third, it presents a concise and succinct comprehensive review of Opportunistic Networks related schemes. Finally, it evaluates the role of the Seed OppNet in Opportunistic Networks related schemes.

As depicted with the roadmap in Fig. 1, this paper's remainder is outlined as follows: Section 2 discusses notions or definitions required to better understand this paper. Section 3 is all about the concept of Opportunistic Networks, its definition, particularities, applications and challenges. Section 4 discusses the existing surveys to show the uniqueness and importance of this paper; Securing and Facilitating Communication within Opportunistic Networks: A Holistic Survey (SFCON). Section 5 provides a brief, comprehensive, and critical review of OppNets related articles and studies the relevance of the articles proposed for Opportunistic Networks under OppNets' constraints. Section 6 concludes the paper with a discussion and future work.

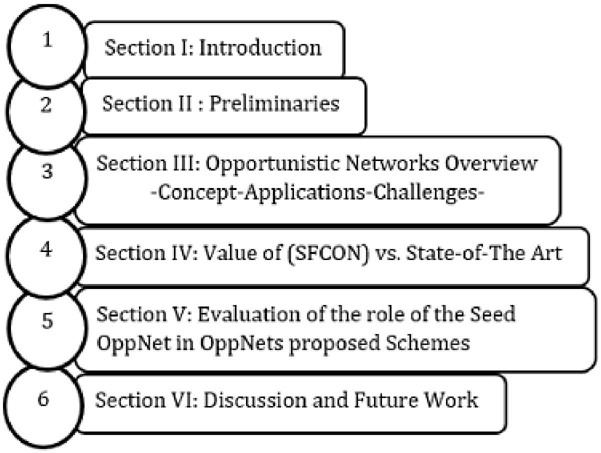

1
Section I: Introduction
2
Section II : Preliminaries
3
Section III: Opportunistic Networks Overview
-Concept-Applications-Challenges-
4
Section IV: Value of (SFCON) vs. State-of-The Art
5
Section V: Evaluation of the role of the Seed
OppNet in OppNets proposed Schemes
6
Section VI: Discussion and Future Work

FIGURE 1. Article roadmap.

II. PRELIMINARIES

This paper depends on many concepts, and the understanding of those concepts could help better understand the various ideas discussed herein. So, this section aims to present an overview of some of these paramount core notions.

A. MULTIDIMENSIONAL SCALING, BLOOM FILTER, DYNAMIC CLUSTERING, AND ONTOLOGY

Multidimensional scaling (MDS) is a method that examines the similarity, sameness, or distance between two objects (data) presented in a low dimensional space, reducing large and complex data into easy to understand and visualise structure. It is via data visualisation that MDS reveals the hidden structure in data [11].

Burton H. Bloom conceived Bloom filters [12] in 1970. View as particular hash tables; Bloom filters are probabilistic and space-efficient data structures that verify whether an element is a member of a set. Bloom filters' raison d'être is that; they are more space-efficient than hash tables, super fast insert, and super fast lookups. Bloom filters allow false positive but do not concede false negative. For Broder and Mitzenmacher [13], on any occasion, a list or set is used, and space is case-sensitive, one can resort to Bloom filters if there is a way to deal with the critical matter of false positive.

Clustering, critical in data or knowledge's discovery, is used in unsupervised learning to differentiate between similar and dissimilar datasets, dividing the dataset into groups. In dynamic clustering [14], clusters are formed, and cluster heads are selected; a notable difference between dynamic clustering and static clustering. Although the concept of Ontology originated from Philosophy, other disciplines such as Computer Science and Information Science do have their definitions of Ontology. In Computer Science and Information Science, sharing is of cardinal importance to the notion of Ontology [15]. The main idea behind the concept of Ontology in Computer Science is creating common vocabularies that are logically well defined which can be used to tag data coming from different sources so that the data become integrated and the sources uninterruptible.

B. OPPORTUNISTIC NETWORK CONTACT GRAPHS, K-ANONYMITY, MARKOV MODELS

A contact graph reveals sensitive pieces of information about social links. Two elements characterise the contact graph G : $G = \{V, E\}$. V is a set of nodes or users, and E is a set of edges [16].

K-Anonymity is a technique that aims to protect data. It relies on the principle that if at least K people share the same quasi-identifiers in the same table, no individual can be individually tracked [17].

The Markov model relies on the Markov process, which is a memoryless chain of events. The next event depends on the current event, not the past event. A set of states forms the Markov model. Fig. 2 is a basic but classic example of a Markov model with the states *Happy* and *Sad*. Assuming that a person can be either Happy or Sad, the Markov model in Fig. 2 describes the random process of feelings over multiple days. If one is Happy today; tomorrow, there is 0.9 probability and 0.1 probability to be Happy and Sad, respectively. And, if one is Sad today; tomorrow, there is 0.6 probability and 0.4 probability to be Sad and Happy, respectively. The probabilities that define a Markov Model can be summed up in a matrix called Transition Matrix, generally, notated Q. In the example of Fig. 2, $Q = \begin{bmatrix} 0.9 & 0.1 \\ 0.4 & 0.6 \end{bmatrix}$. Markov chains have specific applications, among others:

- Market prediction
- Markov text generator
- Customer behaviour prediction
- Individuals genetics
- Music composition algorithm
- Web page ranking.

Therefore, Markov models could be of use when designing Opportunistic Networks related schemes.

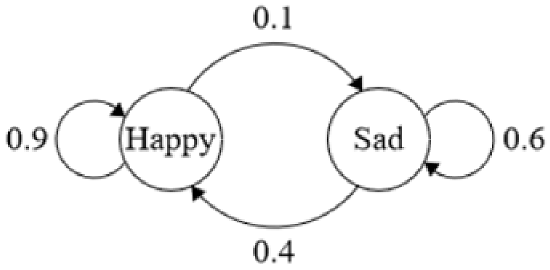


FIGURE 2. Markov Model.

C. NOTIONS OF NEGLIGIBLE FUNCTION, GROUP, BILINEAR MAP

$\mathbb{N}$ is the positive integers' domain and $\mathbb{R}$ is the real numbers' domain. A function

$$F : \mathbb{N} \rightarrow \mathbb{R}$$

is negligible if $\forall\ \epsilon \in \mathbb{N}$, $\exists\ t_\epsilon \in \mathbb{N}$ such that $F(t) \leq t^{-\epsilon}$ for all $t \geq t_\epsilon$; meaning that F approaches zero faster than the reciprocal of any polynomial. 2^{-t}; $2^{-sqrt(t)}$; t^{-logt} are examples of negligible functions.

G is a set and $(\star)$ a binary operation. The couple $(G, \star)$ is a group if and only if the following conditions are satisfied

- $\forall\ \alpha, \beta \in G$,$\alpha \star \beta \in G$. This condition is know as *closure* axiom.
- $\forall\ \alpha, \beta, \gamma \in G, \alpha \star (\beta \star \gamma) = (\alpha \star \beta) \star \gamma$. This condition is known as *Associative* axiom.
- $\exists\ e \in G$ such that $\forall\ \alpha \in G, \alpha \star e = e \star \alpha = \alpha$. From this condition, e is called *Identity element*.
- $\forall\ \alpha \in G, \exists\ \beta \in G$ such that $\alpha \star \beta = \beta \star \alpha = e$. From this condition β is called *Inverse*.

G is an abelian or commutative group if $\forall\ \alpha, \beta \in G, \alpha \star \beta = \beta \star \alpha$

The couple $(\mathbb{Z}, +)$ is an example of an abelian group. For a group can be finite or infinite, the order of a finite Group G is the number of elements in G. In case, group G is infinite, group G is said to be of infinite order. A group G is referred to as a cyclic group if G is generated by a single element x. Then G can be written $G =< x >$, where $x \in G$, and x is called generator of G.

G and G' are two groups. A function λ is a group homomorphism from G to G' if $\lambda(a + b) = \lambda(a) + \lambda(b)$ where a, $b \in G$. And λ is called isomorphism if $G = G'$.

G_1, G_2, and G_3 are three cyclic groups of the same order. A map e: $G_1 \times G_2 \rightarrow G_3$ is a bilinear map if: $\forall\ u \in G_1, v \in G_2$,$\alpha$,$\beta \in \mathbb{Z}$, $e(u^\alpha, v^\beta) = e(u, v)^{\alpha\beta}$.
For e associate pairs of elements from G_1, G_2 respectively with elements in G_3, e is also called Pairing.

D. FUNDAMENTAL CRYPTOGRAPHIC DEFINITIONS

In Cryptography, symmetrical encryptions algorithms also called private key cryptography are old techniques that use a single shared key to cipher and decipher data, messages, or information [18]. In other words, a sender and a receiver use the same key. Symmetrical encryptions are simple, easier to use, fast but can not guarantee PAIN (Privacy, Authenticity, Integrity, and Non-repudiation). AES-128, AES-192, and AES-256 are the most well-known and widely used symmetrical key encryption algorithms. Fig. 3 illustrates a symmetrical encryption key algorithm.

In Cryptography, asymmetrical key encryptions also called public key cryptography, relatively new as compared to symmetrical encryptions, came up to solve the need to share the secret key problem of symmetric key encryption algorithms. Asymmetric encryptions are relatively slower than symmetric encryptions. Asymmetrical key encryption algorithms use

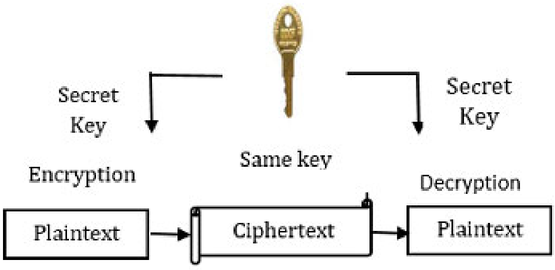


FIGURE 3. **Symmetrical key encryption algorithm.**

two key pairs (public key, private key). The public key is available to anyone who wants to send a message, and the private key is used to decipher a message encrypted with the public key [18]. Elgamal, RSA, DSA, Elliptic Curve techniques, are the most popular asymmetric key encryption algorithms. Fig. 4 is an illustration of an asymmetric key algorithm.

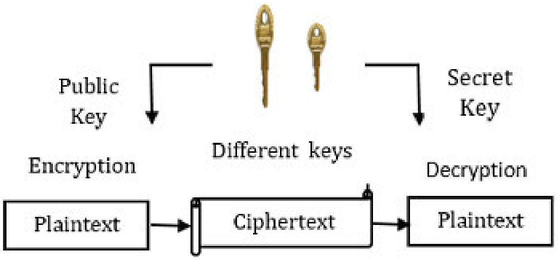


FIGURE 4. **Asymmetric key encryption algorithm.**

Based on asymmetric cryptography's principles, digital signatures are essential cryptographic primitives that help verify the authenticity of digital data. Valid digital signatures are supposed to provide authenticity, non-repudiation, and data integrity. Fig. 5 is a brief illustration of digital signatures. Digital signatures are so significant that if valid, they have the following properties:

- Time saving
- Assurance of security
- Legal and future validity
- Cost, workflow, and business efficiency
- Better customer service experience

1) DECISIONAL BILINEAR DIFFIE-HELLMAN PROBLEM

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p; g a generator of $\mathbb{G}$, and e a bilinear map, $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let $x, y, z, c \in \mathbb{Z}_p$ be randomly chosen. The Decisional Bilinear Diffie-Hellman (DBDH) assumption [19] holds in $\mathbb{G}$ if no probabilistic polynomial-time algorithm can distinguish with a non-negligible probability the tuples $(g, g^x, g^y, g^z, e(g, g)^{xyz})$ from the tuple g, g^x, g^y, g^z, g^c.

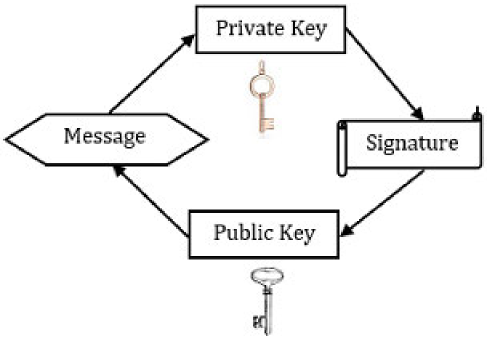


FIGURE 5. **Illustration of digital signatures.**

2) IDENTITY-BASED CRYPTOGRAPHY

A. Shamir [20] was the first person to propose the idea of Identity-Based Cryptography (IBC) in 1984. IBC's main goal was to simplify the certification management of conventional PKI supported security schemes. However, it is until 2001 that Boneh and Franklin introduced the first practical solution of IBC based on the Diffie-Hellman Problem from Weil pairing. An Identity-Based Cryptography scheme is made up of four randomised algorithms [21].

- Setup: Generate the master secret key S and the system parameters.
- Extract: Given a user's identity, generate the corresponding private key by using the master secret key.
- Encrypt: To encrypt a message m for a user, take the user's identity and m as input, and generate the corresponding ciphertext.
- Decrypt: To decrypt a ciphertext c, take the user's private key and c as input, and recover the corresponding message.

3) THRESHOLD SECRET SHARING

A $(k; n)-$threshold secret sharing or threshold secret splitting is a secret keeping method that distributes a secret among a group of participants or users in such a way that only a sufficient number k of users; $(k \leq n)$ together can reconstruct the secret [22].

4) HASH FUNCTIONS

In modern Cryptography, hash functions play a critical role. They are useful for many purposes among others; authentications, encryptions, and digital signatures. Hash functions are particular types of one-way functions that map data, message, or information of an arbitrary length called key or input into data of fixed length called hashes, hash values or checksums [23]. They are supposed to be smaller in size than the input. Hash functions are categorised as follow:

- Non-cryptographic hash functions.
- Cryptographic hash functions:
  1) Keyed cryptographic hash functions.
  2) Unkeyed cryptographic hash functions.

5) THE TIMESTAMP PROTOCOL

Timestamps are of great help in designing users authentications and data integrity algorithms [24]. In effect, a timestamp protocol helps locate in time the existence of a piece of electronic data.

6) MERKLE HASHING TECHNIQUES

Hash functions are particular types of one-way functions use to verify data's integrity. The Merkle hashing techniques, however, introduced by Merkle [24], comes in when one has to deal with large data structures; in other words, many blocks of data, or a big block of data split into many blocks. Sometimes, referred to as a hash tree, a Merkle tree is a particular binary tree that first hashes every packet with a hash function; the resulting hashes of these packets are called the leafs of the tree. Every pair of hashes are then hashed together to form a new hash value; the process continues until only one value remains. The last value is called the root value, or the Merkle root. $H(P0, P1, P2)$ is the Merkle root in Fig. 6. If there is an uneven number of hashes at any level of the tree, the last packet's hash value is concatenated with itself to form a new hash value.

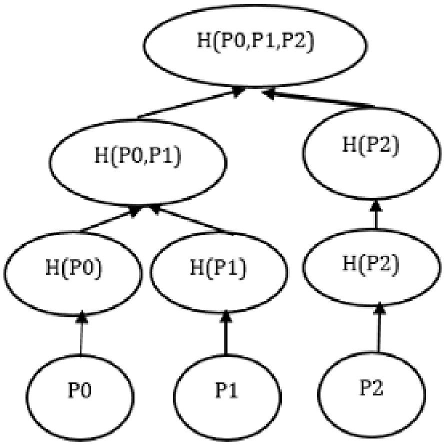


FIGURE 6. Merkle hashing techniques.

E. DENIAL OF SERVICE WITHIN OPPORTUNISTIC NETWORKS, MACHINE LEARNING

In an Opportunistic Network, certain nodes have behaviours that encroach on the proper functioning of the Network. Among other such behaviours, free rider, wormhole attacks, Packet drop attacks, Sybil attacks, and Supernova and Hypernova attacks are the most popular.

- In a Sybil attack, a malignant node introduces fake identities into the network, pretending to be multiple and real nodes.
- Supernova and Hypernova nodes occupy the network's resources and prevent the proper functioning of the network.
- Free rider nodes are selfish nodes.
- A packet dropping attack within Opportunistic Networks is a kind of denial of service attack in which a node often called malicious node in the network, intentionally, for some reasons, instead of forwarding all the packets, drops all the packets or retains a portion of them. A packet faking attack, on the other hand, is an attack where a malicious node not only drops one or more packets but also injects fake, forged packets.
- As far as wormhole attacks are concerned, a malignant user receives packets at one spot, channels the received packets to another spot, and replays the received packets into the network from the new spot.

Machine Learning, first discussed by A.L. Samuel [25], is a branch of artificial intelligence that instead of a human, relies on systems(machines) to study data in order to make decisions, without being explicitly programmed. The widely known Machine Learning algorithms are; Unsupervised Learning, Supervised Learning, Reinforcement Learning, and recommender systems. While Unsupervised Learning and Supervised Learning are used the most.

F. INTERNET OF THINGS, MOBILE AD HOC NETWORKS

D. Evans [2], first coined the concept of the Internet of Things (IoT) when he made a presentation at Procter & Gamble (P&G) in 1999. The topic of the Internet of Things is nowadays at the centre of many types of research for it has become an important technology that enables communication between objects, machines and everything together with people. On the other hand, K.A.M Evans and S.A.A Elmustafa [26] saw the Internet of Things as a system that includes real-world Things and sensors attached to these Things and connected to the Internet via a network structure. E. Fleisch [27] defined IoT as a network of uniquely identifiable and inter-operable objects connected by services over the Internet. On the other hand, I. Lee and K. Lee [28] defined the Internet of Things as a system of the network which generates interaction among physical and virtual Things with the purpose of collecting and sending data by using Information and Communications Technology. Notwithstanding the above definitions, some institutions also defined the Internet of Things. For IERC, IoT is a dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols where physical and virtual Things have identities, physical attributes, and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network [29].The concept of the Internet of Things, despite being a hot area of research has engendered many other concepts such as IoV, IIoT, and IoE, among others. The Internet of Vehicles (IoV), learning from the Internet of Things (IoT), IoV, also referred to as the concept of "Connected Vehicles" came to modernise the traditional transportation system. For the sake of simplifying matters, IoV came to facilitate the pervasive data, message, or information sharing among vehicles with little or no humane collaborations [30]. From the Internet of Vehicles, emerged the concept of Fog Internet of Things (F-IoV). The research for the advances of the field of the Internet of Things also fathered the Industrial Internet of Things (IIoT). Integrating the information technology (IT) and the operation technology in industries or work environments, IIoT uses the Internet of Things' principles and connected Things within an industry's environment not only to provide real-time interconnectivity but also to enable intelligent industrial operations using advanced data analytics for transformational business outcomes [31]. Things formerly unconnected to the Internet are now increasingly connected to the Internet in an unprecedented manner. Also, on the one hand, human beings' awareness on the use of the Internet is soaring, and on the other hand, the capabilities of Things connected today are also improving. So, the Internet of Everything (IoE) came up to combine and take the Internet of Things, the Internet of vehicles, the Industrial Internet of Things to the next level. IoE, as depicted in Fig. 7, aims to bring people, data and process together [7].

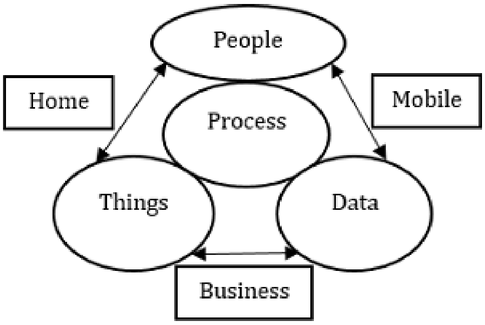


FIGURE 7. Internet of Everything.

Mobile ad hoc Networks also called MANETs are wireless networks with the following characteristics;

- Continuously self-configuring
- Infrastructure-less network
- Freedom of movement of each device
- Each device is a router
- Dynamic topology
- Autonomous topology
- Decentralised networks
- Mobile nodes
- Altruism
- Arbitrary location
- Multi-hop routing
- Light-weight terminals

As research on Mobile ad hoc Networks matures, from Mobile ad hoc Networks' research emerged among others: Vehicular ad hoc Networks (VANETS) that applies Mobile ad hoc's principles to Vehicle-to-Vehicle information or data sharing, Smart Phone ad hoc Network (SPANs), Internet-based mobile ad hoc Network (iMANETs) [5].

Mobile ad hoc Networks have many applications in:

- Business
- Military
- Emergency
- Home, Office, and Education

III. OPPORTUNISTIC NETWORKS OVERVIEW

The relevance of any OppNets related article or scheme relies on how effective the proposed scheme includes OppNets' characteristics and demands. Thus, this section resorts to the pioneers of Opportunistic Networks to present an overview of OppNets. Also, this section's definitions and concepts will serve as the foundation for evaluating Opportunistic Networks' schemes.

A. CONCEPT OF OPPORTUNISTIC NETWORKS

B. Bhargava *et al.* [8] and L. Lilien *et al.* [9], on the one hand, M. Conti and M. Kumar [34] and M. Conti *et al.* [35], on the other hand, had a seminal role in conceptualising Opportunistic Networks or OppNets. Opportunistic Networks appears as the next step of research after research on ad hoc Networks, Mobile ad hoc Networks, the Internet of Things, the Internet of Vehicles, the Industrial Internet of Things, and the Internet of Everything. There are even researchers that do regard OppNets as the natural evolution of Mobile ad hoc Networks. Opportunistic Networks fall in the category of self-configured networks with a reliance on limited or no infrastructure, made of diverse systems, not initially employed as components, which join dynamically to exploit the resources available to achieve a specific mission. Also, when it comes to routing within Opportunistic Networks, the is no notion of an end-to-end path. In effect, an Opportunistic Network's life starts with a Seed OppNet that sets the Opportunistic Networks' mission. The Seed OppNet is a vital part of an OppNet that works for its transition from Seed OppNet to expanded or extended Seed OppNet by inviting "foreign" nodes that may become Helpers. So, an Opportunistic Network has, on the one hand, a Seed OppNet and, on the other hand, Helpers that could be any kinds of devices or systems (users, machines, robots, vehicles, sensors, or Things) equipped with various types of communication media (Bluetooth, wired Internet, wi-fi, ham radio, RFID) or technology. For example, Fig. 8 illustrates a Seed OppNet and Fig. 9 is the resulting expanded Seed OppNet or Opportunistic Network. A "foreign" node can accept or reject an invitation from a Seed OppNet. However, for a Seed OppNet deployed for national interest (life or death situation),

FIGURE 8. Seed OppNet.

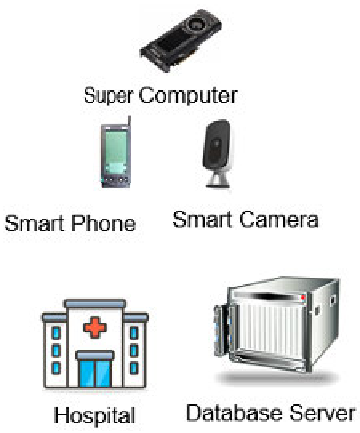


FIGURE 9. Expanded Seed OppNet.

some reluctant nodes might be forced or ordered to join an OppNet. After accepting a Seed OppNet's invitation to join an OppNet, the newly arrived to the OppNet is registered or certified and becomes a Helper. After deployment, discovering and registration of Helpers are the next steps for an OppNet. However, the acceptation of "foreign " nodes to become Helpers is conditioned with the resources they offer. The Seed OppNet and Helpers put their resources together to achieve the Seed OppNet's initial mission. After its mission is completed, the Seed OppNet releases all Helpers, and the Opportunistic Network's life ends. As far as Opportunistic Networks are concerned, the terms; nodes, users, and devices, can be used interchangeably.

B. DIFFERENCES BETWEEN OppNets AND OTHER NETWORKS

First, most researchers mistake Opportunistic Communication in other Networks such as Mobile ad hoc Networks for communication within Opportunistic Networks (OppNets). Although nodes within an OppNet also communicate opportunistically, the "Opportunistic" referred to by other networks is limited. For opportunistic communication to happen within these other networks, devices wait until they are in each other's range. In contrast, OppNets should create a bundle where nodes or users with heterogeneous resources pool their resources. So, OppNets not only grow opportunistically in size but also in resources. Second, Delay Tolerant Networks' routing algorithms, always look for an existing end-to-end route first and only resort to opportunistic communication when there is no end-to-end route. Third, an OppNet's components are not all deployed at once with the network's size; they join dynamically. In other words, Things have little to no idea about the network's topology and routes are built dynamically. Finally, OppNets can be a span among various Things to leverage their resources.

C. APPLICATIONS OF OppNets

Whenever Things get interconnected, anytime, anyplace through any service and network, there is the opportunity to establish temporary networks to achieve specific goals. The goal of OppNets is to take advantage of the wealth of pervasive resources and capabilities within their reach. So, many situations can benefit from OppNets' research. Opportunistic Networks' concepts can be applied in:

- Social-oriented services (Census, crisis management, mobile social networking information)
- Personal and environment services (Pervasive healthcare, environment monitoring)
- Multimedia Services
- Intelligent transportation systems

D. CHALLENGES OF OppNets

Users are critical to Opportunistic Networks because they carry smart devices connected to the Internet, provide the contact opportunity, the bandwidth and produce consumable data. Like most networks, OppNets in particular, due to their characteristics, as summed up in Fig. 10, face many challenges across users' privacy, information routing, authentication, data aggregation, and technology.

As far as users' privacy is concerned, one should consider the Seed OppNet's privacy and the Helpers' privacy. Users' privacy includes location, identity, and social privacy. The location consists of users' geographical location; the place users live, work or the routes users use to commute. The social in social privacy represents social relationships among possible Helpers; friendship relationship, pre-established contacts, the frequency of meeting among contacts, membership of a group. The identity represents the user or the identifier of the device that a user owns.

As far as information routing is concerned; energy constraints, message delivery latency, users' possible selfish behaviour, data integrity, and the scarce knowledge of the network's topological evolution are the main challenges. OppNets rely on users, but devices that users own have limited power resources. Also, a small dysfunctioning of a device can cause message delivery latency. Moreover, coping with users or nodes' selfish behaviour is a significant challenge. Besides, ensuring data integrity is not the least important.

We identified two authentication types as far as users' authentication is concerned, namely; (Helper-Helper) authentication and (Helpers-Seed OppNet) authentication. The (Helper-Helper) authentication is, in effect, mutual authentication between Helpers within an OppNet's environment. In contrast, the (Helpers-Seed OppNet) authentication is an authentication that occurs within an OppNet when Helpers send their share of information to the Seed OppNet. This (Helpers-Seed OppNet) authentication, to work correctly, may need an aggregate-based signatures scheme.

Finally, despite the advances in technology, a breakthrough is still needed to solve latency issues. Also, a breakthrough is needed to help equip devices with a universal aggregator capable of aggregation irrespective of data. Because of the nature of Opportunistic Networks, the proposed protocols that work for other networks do not apply to OppNets.

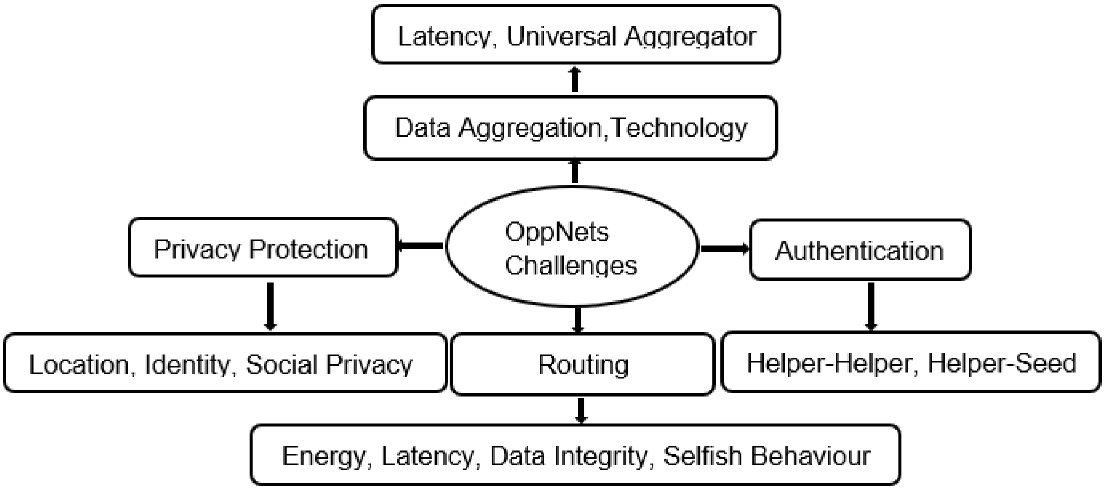

Latency, Universal Aggregator
Data Aggregation,Technology
Privacy Protection
OppNets Challenges
Authentication
Location, Identity, Social Privacy
Routing
Helper-Helper, Helper-Seed
Energy, Latency, Data Integrity, Selfish Behaviour

FIGURE 10. Challenges within an OppNet.

TABLE 1. Existing Survey in Literature and Comparison with (SFCON).

Article and Year	Adressing OppNets Definition	Adressing Schemes Relevance	Adressing Routing or Simulation	Adressing Authentication	Adressing Privacy Protection	Adressing Intrusion Detection	Adressing Data Aggregation	Adressing OppNets Technology
[32]-2008	×	×	✓	×	×	×	×	×
[33]-2009	×	×	✓	×	×	×	×	×
[34]-2010	✓	×	✓	×	×	×	×	✓
[35]-2010	✓	×	✓	×	×	×	×	✓
[36]-2011	✓	×	✓	×	×	×	×	×
[37]-2012	✓	×	✓	×	×	×	×	×
[38]-2013	×	×	✓	×	×	×	×	×
[39]-2013	×	×	✓	×	×	×	×	×
[40]-2013	×	×	✓	×	×	×	×	×
[41]-2014	✓	×	✓	×	✓	×	×	✓
[42]-2014	×	×	✓	×	×	×	×	×
[43]-2015	×	×	✓	✓	✓	✓	×	×
[44]-2016	×	×	✓	×	×	×	×	×
[45]-2016	✓	×	✓	×	✓	✓	×	×
[46]-2017	×	×	✓	×	×	×	×	×
[47]-2017	×	×	✓	×	×	×	×	×
[48]-2017	×	×	✓	×	×	×	×	×
[49]-2018	✓	×	×	×	✓	×	×	×
[50]-2018	✓	×	✓	×	×	×	×	×
[51]-2019	×	×	✓	×	×	×	×	×
[52]-2020	✓	×	×	×	✓	×	×	✓
SFCON-2010	✓	✓	✓	✓	✓	✓	✓	✓

IV. ADDED VALUE OF OUR SURVEY COMPARED TO THE STATE-OF-THE-ART

Survey-type articles proposed for Opportunistic Networks are critical for the advancement of the field of Opportunistic Networks. This section provides a concise review of the main contributions in the survey-type articles proposed to help advance OppNets' research. Also, Table 1 depicts an at-a-glance comparison of our proposed survey; Securing and Facilitating Communication within Opportunistic Networks: A Holistic Survey (*SFCON*) with surveys, in literature, that discussed OppNets related topics. In Table 1, "✓" = Topic addressed and "×" = Topic not addressed.

C.M. Huang *et al.* [32] defined an Opportunistic Network as a subclass of Delay Tolerant Networks and proposed a short survey that discussed some OppNets' challenges. For the authors, energy and storage's matters are the main challenges facing OppNets. Moreover, the authors discussed routing in an Opportunistic Network, mainly forwarding-based and flooding-based approaches.

Acknowledging the challenges that come with routing in an opportunistic network's environment, H. A. Nguyen and S. Giordano [33], proposed a survey that discussed Opportunistic routing protocols. They classified routing protocols into three groups, mainly; context-oblivious, mobility-based, and context-aware routing. Also, they not only evaluated the performance of the three classes but also characterised routing in Sensor Actor Networks (SAN).

M. Conti and M. Kumar [34] with a seminal-type article, combed the domain of Opportunistic Networks with a concise overview that discussed the key challenges, research questions, and applications in the field of Opportunistic Networks. Also, the authors briefly discussed their OppNets-oriented research achievements with the research group Haggle project.

Concerned with how Opportunistic Networks should evolve from OppNets to Opportunistic Computing, M. Conti *et al.* [35], after a thorough breakdown of Opportunistic Networks' definitions and applications, proposed a survey that tackles research and results in Opportunistic Networks based on the European Union Haggle project (EU haggle project). The authors introduced the concept of Opportunistic Computing (OC) and suggested that the experience accumulated from years of research from OppNets will drive OC.

Users are central to Opportunistic Networks, and since within OppNets, users represent devices and vice versa, the mobility of users that are sentient beings is reflected in devices users carry. For mobility is an Opportunity for OppNets, D. Karamshuk *et al.* [36], were interested in human's mobility and its application to OppNets. They considered a spatial, temporal and social dimension of mobility to review the findings as far as Humans' mobility is concerned.

L. Liu and Y. Jing [37] expressed a particular interest in routing in OppNets with the help of social settings that they broke into three groups, namely: community-based, regular mobility pattern-based, and combination of context and social information-based.

I.Woungang *et al.* [38] defined Opportunistic Networks as a generic Mobile ad hoc Network paradigm and wrote a book on routing in Opportunistic Networks that includes a plethora of Opportunistic Networks related topics. To sum up, the authors investigated on mobility-enabled message dissemination and social-aware routing approaches for opportunistic Networks. Also, they elaborated on context information routing protocols and analysed the tradeoff between energy and latency for routing in Opportunistic Networks. What is more, the authors analysed the infrastructure needed for communication in Opportunistic Networks and the connectivity problems in Opportunistic Vehicular ad hoc Networks. Moreover, they elaborated on routing protocols that exploit intermittent communication opportunities for increased data transmission success in Mobile ad hoc Networks.

B. Poonguzharselvi and V. Vetriselvi [39] defined Opportunistic Networks as an evolution of Mobile ad hoc Networks and proposed a survey article that classified routing schemes proposed for Opportunistic Networks based on what the authors call "Forwarding behaviour.".

B. Soelistijanto and M.P. Howarth [40] defined Opportunistic Networks as a class of Mobile ad hoc Networks and proposed a survey article that discussed routing protocols in OppNets. Precisely, the authors reviewed the techniques used for message transfer reliability and the techniques used in congestion control for Opportunistic Networks.

Aware of the challenges that Opportunistic Networks came with, C. Boldrini *et al.* [41] proposed an overview of the research questions in Opportunistic Networks' area of research.

V.F.S. Mota *et al.* [42] characterised Opportunistic Networks, classified OppNets, discussed routing protocols, and simulators for OppNets.

Likening OppNets to Delay Tolerant Networks and Mobile ad hoc Networks, Y. Wu *et al.* [43] proposed a survey that not only elaborated on the security threats and requirements in Opportunistic Networks but also proposed a security architecture for OppNets that encompasses authentication, trust management; cooperation, secure routing, and access control. The authors also provided a comparison of the security and trust solution available in literature.

P. Yuan *et al.* [44] suggested that the selection of a routing mechanism is critical when it comes to transmitting packets in an OppNet's environment. So, classifying the routing mechanism into two main groups, they surveyed opportunistic routing protocols; organising them into a taxonomy. Also, they analysed and evaluated them. Moreover, the authors discussed open research questions.

Unlike surveys that focused on; security threats, architecture, authentication, and access control in Opportunistic Networks, M. Alajeely *et al.* [45], acknowledging that Human is central to OppNets and that trust could play a key role in securing routing in OppNets, provided a detailed overview of the security of trust-based routing protocols.

Similar to P. Yuan *et al.* [44], S.R. Bharamagoudar and S.V. Saboji [46] proposed a survey article that discussed routing for Opportunistic Networks, classifying the routing protocols into two classes; social-zero information schemes and social-aware information schemes. Moreover, the authors elaborated on the evaluation of routing algorithms.

Since a simulation is critical before any real-life project deployment, J. Dede *et al.* [47] aimed at surveying tools and models to help simulate Opportunistic Networks. After a thorough gap analysis of the simulators used for Opportunistic Networks, the authors outlined possible research directions.

N. Mantas *et al.* [48], concerned with the trade off that comes with the use of conventional secure forwarding techniques that involve cryptographically signed certificate exchanges, suggested the use of cooperation enforcement schemes as a lightweight alternative. So, the authors proposed a comprehensive survey of representative cooperation enforcement schemes that exploit a reputation system.

Motivated by privacy concerns in general and location-privacy concerns in particular, S. Zakhary and A. Benslimane [49] proposed a survey that reviewed the privacy protection mechanisms, in literature, for Opportunistic Networks with a focus on location-privacy.

After giving a precise definition of OppNets, M. Alajeely *et al.* [50], gave an overview of routing protocols: Epidemic

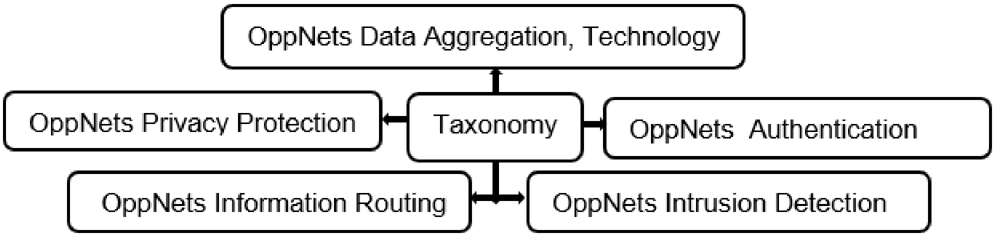

OppNets Data Aggregation, Technology
OppNets Privacy Protection
Taxonomy
OppNets Authentication
OppNets Information Routing
OppNets Intrusion Detection

FIGURE 11. Taxonomy of OppNets related proposals.

routing, PRoPHET, MaxProp, Spray and Wait, Direct Delivery and First Contact, and evaluated these different routing protocols as far as complexity, robustness and scalability are concerned.

Stressing on the advantage of the increasing number of mobile devices, A.M. Abali *et al.* [51], non-content with the traditional classification of geocast routing protocols into inter-cast and intra-cast, proposed a survey on geocast routing that encompasses the movement prediction methods' area of research such as: message endpoint identification, forwarding utility computations, forwarding algorithms, and message dissemination.

After elaborating on the concept of Opportunistic Networks; clarifying the significant differences between OppNets and other wireless networks, C.B. Avoussoukpo *et al.* [52] proposed a review of articles that tackled mutual authentication and privacy protection within OppNets.

Despite the interesting ideas discussed in the articles surveyed, as depicted in Table 1, there are still gaps to fill.

V. EVALUATION OF THE ROLE OF THE SEED OppNet IN OPPORTUNISTIC NETWORKS PROPOSED SCHEMES

The Seed OppNet (Seed Node, Root Node, Source Node) is of cardinal importance for Opportunistic Networks. The Seed OppNet sets up the OppNet, defines its mission, and plays a vital role in its transition from Seed OppNet to extended or expanded Seed OppNet. Due to Opportunistic Networks' characteristics, the Seed OppNet operates under specific constraints; it is not desirable for the Seed OppNet to play the role of a central authority, nor to become a single point of failure. Opportunistic Networks related proposals or schemes need special considerations when designing or proposing them. Although Opportunistic Networks is a relatively new research area, it is increasingly capturing researchers' attention such that more and more articles are addressing OppNets' issues. The aim of this section is twofold. First, it presents a concise and succinct comprehensive review of Opportunistic Networks related schemes. Second, it studies the relevance of Opportunistic Networks proposed articles under OppNets' constraints. More precisely, considering the domains of intrusion detection, authentication, routing, privacy protection, data aggregation, and the technology for OppNets, this section studies the role or the degree of involvement of the Seed OppNet in OppNets related articles. The study considers four degrees of involvement of the Seed OppNet namely:

- High degree: the Seed OppNet plays the role of a central authority
- Medium degree: the Seed OppNet does not play the role of a central authority but does more than registration.
- Small degree: the Seed OppNet does not perform any role other than registration and the release of Helpers.
- Not defined: The proposed scheme does not describe or emphasize the role of the Seed OppNet.

The study considers recent articles in literature based on a brief taxonomy illustrated in Fig. 11.

A. OppNets INTRUSION DETECTION SCHEMES

No system can prevent all types of attackers from breaking into a system. However, being able to notice the presence of an intruder is an exciting feature. So, intrusion detection mechanisms appear among others as an essential step in securing networked system in general and OppNets in particular. In the following, we provide a brief review of OppNets intrusion detection schemes and point out the role plays by the Seed OppNet in each of these schemes.

S. Gupta *et al.* [53] proposed a trust-based security protocol scheme that aims to prevent blackhole attacks within Opportunistic Networks. The proposed scheme is a function of a social group value (SGV) and a trust distribution technique. In the protocol, trust is a function of social group values that divides the network into groups. Here, "the OppNet designer" assigns the social group values, and therefore, the group a particular node belongs. The destination node calculates the trust value for each hop in the message vector. Then trust is distributed among other nodes that participated in the message routing process. By so doing, a malicious node will have a low and static trust value. A low and static trust value is a sign of the presence of an intruder. The authors described good ideas in their scheme. However, the notion of groups does not match OppNets' characteristics. Also, there is a clear source-destination path in their protocol. Meanwhile, there is no actual end-to-end path for Opportunistic Networks. The Seed OppNet identified in their scheme is "the OppNet designer" responsible for the attribution of the social trust value (SGV). The role of the Seed OppNet here is (High Degree).

M. Alajeely *et al.* [54] knew OppNets' characteristics and understood that packet dropping attacks challenge Opportunistic Networks. The authors proposed a scheme that detects packet dropping attacks while revealing the malicious nodes that may attempt to drop some packets. With a network packet divided into three parts: header, data, and trailer, the proposed scheme detects an attack thanks to an indicative field (also equipped with three subfields: the identification field, the flag field, and the offset field) in the header. The proposed scheme's advantage relies on the fact that the scheme detects both packets dropping attacks and malicious node. Also, any intermediary node can detect possible attacks. However, the scheme does not mention the temporary aspect of the network, and more importantly, no apparent role of the Seed OppNet was mentioned. Therefore, the role of the Seed OppNet for this scheme is (Not Defined).

Understanding the security challenges that exist within OppNets, M. Alajeely *et al.* [55] presented a novel attack and its countermeasure. Here, the attacker dropped a packet and replaced the dropped packet with a forged one. The power of their scheme resides in the simple idea of the creation time of each packet. Nonetheless, the role of the Seed OppNet is (Not Defined).

M. Alajeely *et al.* [56] proposed again a malicious node detection mechanism where a malicious node drops one or more packets and injects fake, forged packets. Based on Merkle tree hashing techniques, any node can first detect an attack and then identify the intruder. Still, placing this fantastic contribution in the context of OppNets and Seed OppNet is hard. Therefore, the role of the Seed OppNet is (Not Defined).

M. Alajeely *et al.* [57] proposed a malicious node detection mechanism to counter an attack that the authors previously called ‘‘packet faking attack;; where a malicious node drops one or more packets and injects fake, forged packets. Based on hash chain techniques, any node can first detect an attack, then identify the attacker. Still, placing this fantastic contribution in the context of OppNets and Seed OppNet is hard. The role that the Seed OppNet plays is (Not Defined).

M. Alajeely *et al.* [58] proposed a scheme to detect and counter a kind of packet dropping attack. Here, the authors called the attack and defence mechanisms; catabolism attack and anabolism defence, respectively. Both the attack and defence mechanisms rely on hash chain techniques. Although it is a useful feature that every node can detect and counter a catabolism attack, the authors have not clearly stated the Seed OppNet's role in their scheme. Thus, the role of the Seed OppNet is (Not Defined).

Reckoning the importance of intrusion detection in securing Opportunistic Networks, N. samaras *et al.* [59] suggested an energy-efficient, protocol-independent, multilayer intrusion detection mechanism for Opportunistic Networks. The proposed detection method uses cryptographic protocols and the available system information produced by the protocols in different layers. The Seed OppNet's role in the proposed scheme is (Not Defined).

Using the Merkle tree hashing technique and trust, M. Alajeely *et al.* [60] proposed a defence method against selective packet dropping attacks. The proposed algorithm is efficient in detecting both malicious paths and malicious nodes. Here, it is assumed that the sender (source node) and the destination (final receiver) are legitimate, and only intermediate nodes can be malicious. The proposed scheme highly depends on the Merkle root and the ultimate receiver. Upon receiving the message, the destination calculates his own Merkle root that he compares with the sender's. If both the sender and the destination's Merkle roots match, there was no dropping behaviour throughout the way. If both roots of the source node and the destination node do not match, a selective packet dropping attack has occurred, and the destination reports the path as malicious. The destination node uses the detection of the malicious path to building the trust value of each node, and finally detects malicious nodes. The proposed algorithm ends up discovering malicious path and malicious nodes. The proposed method is an excellent work because it presents a tangible advantage over cryptographic verification for with fewer calculations, malicious paths can be detected. However, neither the temporary aspect of the Opportunistic Networks nor the Seed OppNet's role is presented. Therefore, the role of the Seed OppNet for this algorithm is (Not Defined).

Using the Merkle tree hashing technique, trust, and reputation, M. Alajeely *et al.* [61] consecutive to their paper ‘‘Establishing trust relationships in OppNets using Merkle trees’’ proposed another defence method against selective packets dropping attacks. The proposed algorithm detects not only malicious paths but also malicious nodes. The authors developed a node by node packet dropping detection mechanism using two algorithms. Direct trust first; then, indirect trust and reputation. Each node maintains its trust table and stores it locally. The table records a node's direct and indirect experiences with other nodes in the network; both values are then used to calculate each node's reputation. The scheme proposed is a remarkable work, yet it does not fit OppNets' characteristics. It follows that the role of the Seed OppNet here is (Not Defined).

S. Rashidibajgan [62] proposed a trust structure to detect Sybil attacks within Opportunistic Networks. The proposed trust structure is based on neighbouring nodes' observation and Bayes' rules. Each node monitors neighbouring nodes and records their observation in a table. When two nodes come into contact, they exchange and update their observation tables, respectively. A node's definition is based on its updated observation table. The author developed a good idea. Nonetheless, the role of the Seed OppNet is (Not Defined).

S.K. Dhurandhe *et al.* [63] proposed a mechanism to detect Supernova and Hypernova's misbehaviour within Opportunistic Networks. To counter the Supernova and Hypernova's misbehaviour of some nodes, the authors proposed a method that calculates the number of messages generated by each node. The frequency of message generation by each node is monitored so that high messages generation

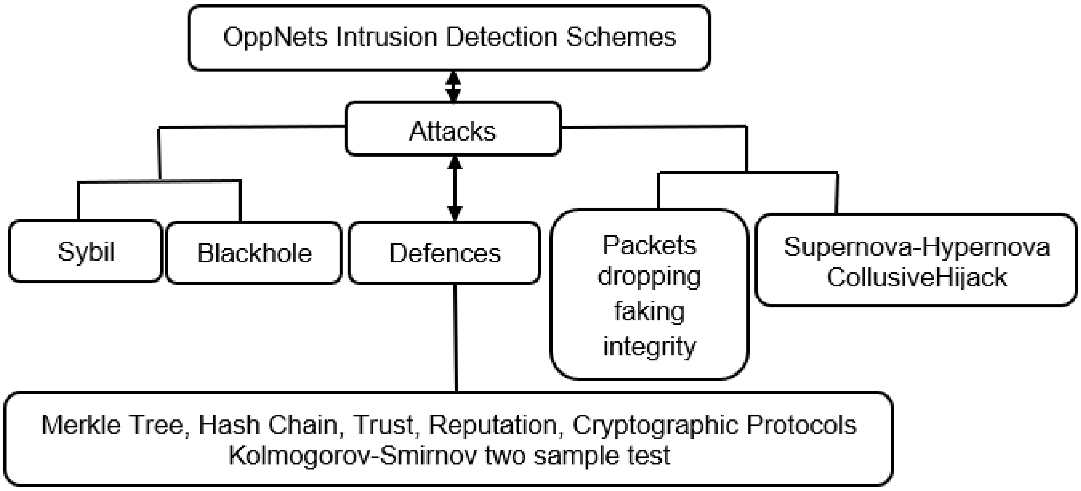

OppNets Intrusion Detection Schemes
Attacks
Sybil
Blackhole
Defences
Packets dropping faking integrity
Supernova-Hypernova CollusiveHijack
Merkle Tree, Hash Chain, Trust, Reputation, Cryptographic Protocols Kolmogorov-Smirnov two sample test

FIGURE 12. Taxonomy of OppNets intrusion detection schemes.

frequency nodes are labelled as Supernova and Hypernova nodes. Despite the excellent idea illustrated in the proposed mechanism, the role of the Seed OppNet is (Not Defined).

R. Doss *et al.* [64] proposed a method to secure OppNets against packets' integrity attacks. The proposed method relies on five different algorithms; finding and detecting modified packets and malicious paths, respectively, frequency and direct trust, indirect trust, meeting trust, and reputation. Merkle trees, trust, and reputation techniques ensure the packets' integrity protection. The authors' defence proposal is excellent because each node in the network can detect both malicious nodes and paths. However, the role of the Seed OppNet is still (Not Defined).

S.K. Dhurandher *et al.* [65], to detect malicious nodes within OppNets' environment, proposed a cryptography-based misbehaviour detection and trust control mechanism for OppNets. With established cryptographic protocols, the proposed scheme relies on infrastructure nodes. Infrastructure nodes monitor the network to detect suspicious misbehaving that may occur. Despite the monitoring role play by infrastructure nodes, it is not clear whether the infrastructure nodes represent the Seed OppNet. Therefore, the role of the Seed OppNet within the present proposed scheme is (Not Defined).

A. Altaweel *et al.* [66], first, proved that hybrid routing and prophet protocols within OppNets' environment are vulnerable to collusiveHijack attacks; attacks where an adversary can compromise a set of nodes, lying about their inner contact's time; then, opening rooms for attacks such as packet modification attack, traffic analysis attack, and an incentive seeking attack. Second, as a countermeasure, the authors proposed a collusiveHijack detection mechanism using the Kolmogorov-Smirnov two sample test; a statistical method that contrasts two distributions. The proposed scheme relies on two main techniques; the path detection technique and the hopping detection technique. Despite the satisfying results claimed, the detection algorithm does not acknowledge the Seed OppNet. So, the Seed OppNet's role is (Not defined).

To sum up, as illustrated in Fig. 12, intrusion detection schemes proposed for OppNets tackled the issues of sybil, blackhole, collusiveHijack, packet faking, packet integrity, packet dropping, and supernova-hypernova with Merkle tree, hash chain techniques, the Kolmogorov-Smirnov two-sample test, trust, reputation, and cryptographic protocols. What is more, as depicted in Fig. 13, most schemes proposed for OppNets to defend against intrusion do not fully understand Opportunistic Networks' requirements for the Seed OppNet that is supposed to determine the OppNets' mission is not considered in most schemes.

B. OppNets AUTHENTICATION SCHEMES

In an environment with little to no infrastructure's support, such as for Opportunistic Networks, making sure data is coming from the right source is sometimes cardinal. Therefore, authentication schemes proposed for OppNets are worthy of study.

J. Solis *et al.* [67] suggested using "best-effort" authentication, a method that accepts false positives but not false negatives, easier to break than the Merkle hash tree-based techniques, requiring fewer computations for benign nodes' fragment authentication by intermediaries in Opportunistic Networks. The study suggested that "best-effort" authentication is only for fragment authentication and should not replace traditional end-to-end message authentication. Although the study showed satisfactory delivery ratio, the Seed OppNet has no specific role. Therefore, the role of the Seed OppNet is (Not Defined).

C. Carver and X. Lin [68] proposed a scheme that helps a user discover proximity friends without compromising their privacy in an Opportunistic Network. The proposed scheme uses three steps: system initialisation, notification generation and opportunistic forwarding, and notification reception.

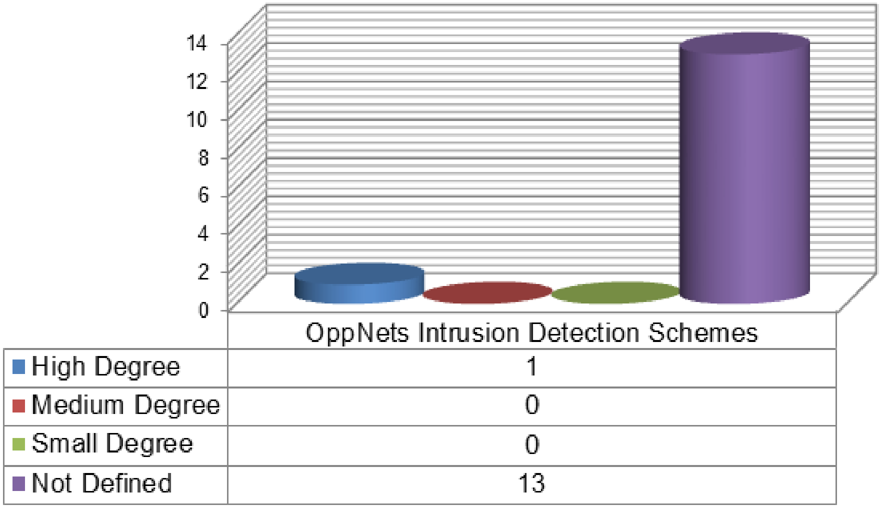


FIGURE 13. Evaluation of OppNets intrusion detection schemes.

A trusted party plays the role of a Seed OppNet and is responsible for the system initialisation. Also, any user wanting to discover proximity friends must resort to the trusted party for authentication. The proposed scheme relies on the Decisional Bilinear Diffie-Hellman problem. Moreover, the scheme's performance analysis shows satisfactory results. Since the trusted party is responsible for system initialisation and should be resorted to for authentication, the role of the Seed OppNet is (High Degree).

X. Cao, Y. Yin [69] proposed an identity authentication scheme that integrates trust into multidimensional scaling. The proposed scheme depends on a trust model called M-Trust that relies on an integrated trust value Q_{α}^{β} obtained by combining direct and indirect trust values. The article characterises OppNets with a Seed OppNet; here a root node. Also, Helpers have some flexibilities because they generate their private keys; the Seed OppNet participates slightly in that process. Also, each node sets the relationship intensity threshold δ. And when two nodes α and β come into contact, α queries the local repository and calculates the integrate trust value. Then, after considering the value-at-risk, the node β can get a certificate from α if $Q_{\alpha}^{\beta} \leq \delta$. The proposed scheme is, to some extent, relevant to OppNets. However, the phases; scheme initialisation, certificate issuance, certificate conflict reconciliation, and certificate repository update do not encompass the temporary and mission-oriented aspect of OppNets. The role of the seed OppNet in this scheme is (Small Degree).

M.H. Guo *et al.* [70] proposed an authentication scheme that protects users' privacy within Opportunistic Networks. The proposed scheme has two main phases: registration and authentication. Any node or user that wishes to communicate with another node should first register at the Seed OppNet. The registration process of any unauthenticated node A at the Seed OppNet Sn involves A's virtual identifier ID_a, public key PK_a, secret key SK_a; the Seed OppNet's public key PK_{Sn}, secret key SK_{Sn}. Also, the Seed OppNet uses a symmetric key, an arithmetic function $f()$, and a timestamp T_{sn}. If the registration is successful, node A can move within the network with its authentication credentials $M_j, f()$, and T_{sn}. Two nodes A and B that have already completed their registration at the Seed OppNet can engage in mutual authentication. The proposed scheme relies upon general cryptographic principles and achieves anonymity and privacy. It also mitigates tapping, forgery, replay, and man-in-the-middle attacks. The authors deeply understand OppNets' requirements and mission. Here, the Seed OppNet starts and ends the OppNet, and provides just registration for nodes. Therefore, the role of the Seed OppNet for the present scheme is (Small Degree).

Suggesting that mutual authentication is not critical within an OppNet's environment, C. Xi *et al.* [71], with the assumption that nodes have the social context's pieces of information of one another, proposed a non-cryptographic authentication mechanism based on reputation. The proposed scheme depends on two main elements; "identity trust relationship" and "behavior trust relationship" that depend on nodes' social attributes. However, despite the good results obtained after simulation, it is hard to locate the proposed scheme within OppNets' brackets. Therefore, the role of the Seed OppNet is (Not Defined).

U.P. Singh, N. Chauhan [72] proposed an authentication scheme, variant of M.H. Guo *et al.* [70]'s work. Here, the authors extended M.H. Guo *et al.* [70]'s work with the notion of dynamic registration where ordinary authenticated nodes become semi-super nodes. Seed nodes or static nodes appoint authenticated nodes as semi-super nodes by their trust and threshold values. The trust value depends on two parameters; encounter value and number of messages. However, the trust value does not serve much in the process of mutual authentication. The authors somehow understand OppNets'

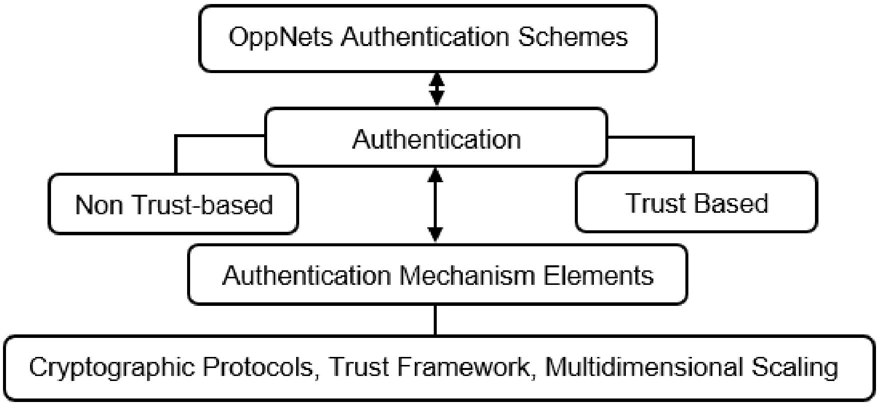

OppNets Authentication Schemes
Authentication
Non Trust-based
Trust Based
Authentication Mechanism Elements
Cryptographic Protocols, Trust Framework, Multidimensional Scaling

FIGURE 14. Taxonomy of OppNets authentication schemes.

requirements. Here, super nodes and semi-super nodes play the role of the Seed OppNet. The Seed OppNet is responsible for only registration and security confirmation if need be. Therefore, the role of the Seed OppNet is (Medium degree).

P. Kumar *et al.* [73] proposed a variant of M.H. Guo *et al.* [70]'s scheme that stresses the use of *RSA* and Diffie-Hellman key exchange for key generation and key exchange. The Seed OppNet is well defined and is in charge of generating all the public and private key pairs. The Seed OppNet is also in charge of the mutual authentication of nodes because for mutual authentication; nodes look through a list. Therefore, the role of the Seed OppNet is (High Degree).

P. Kumar *et al.* [74] suggested a secure framework that helps build trust and prevent all the same unauthorised users from tapping into sensitive data. The proposed scheme is incentive-based that relies on users' identities for authentication. The primary algorithm used alongside trust is the *RSA* algorithm. For the Seed OppNet is responsible for Nodes' registration, Nodes' keys generation and the Nodes' keys list keeping, the role of the Seed OppNet is (High Degree).

M. Gupta [75] proposed a data authentication mechanism where a key is appended to an original message to detect any possible alteration. A polynomial key and an authentication key the Seed OppNet generates and distributes to Helpers, help authorise messages. The Seed OppNet generates encoded data using the data packet and the polynomial key and generates an authentication key that is a function of a timestamp, a polynomial key, and a validity time. The proposed scheme appears tailored for Delay Tolerant Networks because the authors discussed the notion of source-destination, which does not exist in OppNets. The role of the Seed OppNet is (High Degree).

Considering the pre-established contacts' information, the Seed OppNet's identity, and cryptographic principles, C.B. Avoussoukpo *et al.* [76] proposed a user-centric, trust-based, and multi-levels authentication mechanism for Opportunistic Networks. Here, the Seed OppNet does the Nodes' registration and arbitration. So, the role of the Seed OppNet is (High Degree).

M. Abouaroek and K. Ahmad [77] leveraged the security features of *NRTU* algorithm, a ring-based cryptosystem, to propose an authentication scheme for opportunistic Networks. The Seed OppNet generates a unique *ID* and the key to encrypt and decrypt messages. For the Seed OppNet is responsible for *ID*'s allocation and verification, its role is (Medium Degree).

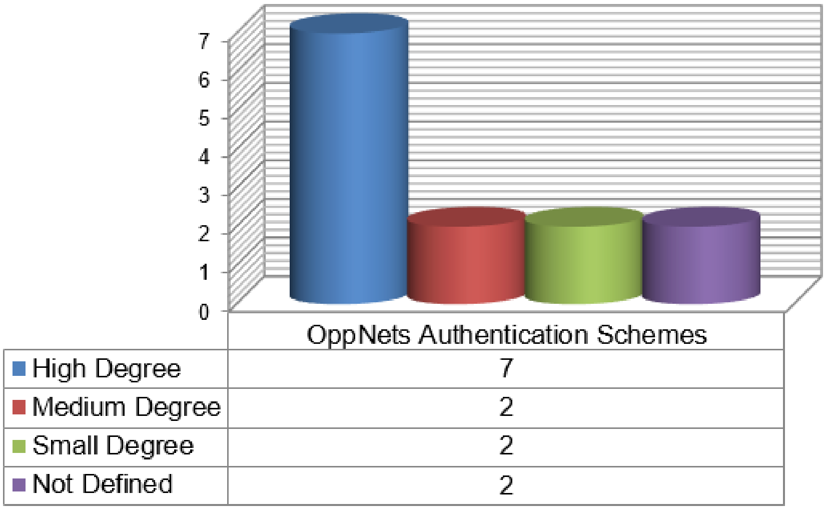
C.B. Avoussoukpo *et al.* [78] resorted to *BLS* signature and aggregate *BLS* signatures to propose an authentication scheme that allows a Seed OppNet to effectively and efficiently process pieces of information. The Seed OppNet is in charge of the system initialization, nodes' registration, and the authentication process. So, the role of the Seed OppNet is (High Degree).

K. Wang and K. Sakai [79] proposed a trust-based authentication mechanism for OppNets using Identity-Based Encryption (IBE). The Seed OppNet and the Helpers of high trust value can be Key Generation Centers (KGC) to avoid the trap of single point of failure of IBE. The Seed OppNet maintains *IDs*, derived Helpers' public keys from them, and is in charge of nodes' registration. So the role of the Seed OppNet is (High degree).

As depicted in Fig. 14, authentication schemes proposed for OppNets are trust-based and non-trust-based and used mostly existing cryptographic protocols' principles, trust framework, and multidimensional scaling as core parts of schemes. More importantly, as illustrated in Fig. 15, the authors showed a great mastery over OppNets' requirements. Most schemes involve the Seed OppNet into their design. However, for most schemes, the role of the Seed OppNet is High Degree or Medium.

C. OppNets PRIVACY PROTECTION SCHEMES

OppNets highly depend on users' altruism. So, whenever users are concerned with their privacy, OppNets might have additional challenges. Also, Opportunistic Networks may see their mission incomplete if potential Helpers do not have the assurance that their privacy is guaranteed. So, privacy protection schemes proposed for OppNets and their relevance



	OppNets Authentication Schemes
🟦 High Degree	7
🟥 Medium Degree	2
🟩 Small Degree	2
🟪 Not Defined	2

FIGURE 15. **Evaluation of OppNets authentication schemes.**

to OppNets deserve keen attention. We identified three types of privacy issues, namely, identity, location, and socal links.

B. Distl and T. Hossmann [80] acknowledged the usefulness of the contact graph for information routing in Opportunistic Networks. They also pointed out the security breach that the use of the contact graph poses. Thus, the authors proposed a scheme that changes the contact graph by adding and removing edges. The proposed algorithm considers an unweighted and undirected contact graph $G = \{V, E\}$ as input and outputs a modified contact graph $G' = \{V, E'\}$ such that $\mid E \mid=\mid E' \mid$. Doing so makes it hard for an attacker operating on a graph level to know any hidden information in $G = \{V, E\}$. The proposed scheme protects social links in Opportunistic Networks but there was no mention of a Seed OppNet in the proposal. Therefore, the role of the Seed OppNet is (Not Defined).

B. Distl and S. Neuhaus [81] proposed a mechanism based on the Bloom filter that uses social connections (pre-established social links) to improve performance without revealing users' private information. The algorithm detects social links, uses them for mutual authentication while protecting personal information. The proposed scheme achieves node's identity protection, security, and excellent performance. However, the Seed OppNet has no role in the algorithm. Thus, the role of the Seed OppNet is (Not Defined).

Assuming that users, in general, trust their social links, S. Zakhary and M. Radenkovic [82] resorted to social links and proposed a location protection scheme through request/reply location obfuscation-based techniques. Proximate friends are supposed to help users in need of location-based services. However, the relevance of the proposed scheme to OppNets is questionable. Therefore, the role of the Seed OppNet is (Not Defined).

The same as in S. Zakhary and M. Radenkovic [82], S. Zakhary and M. Radenkovic [83] leveraged the advantage of social links for location protection. The authors proposed a stochastic model for location prediction using a lightweight Markov model that detects users' contact and uses it to obfuscate requests and hide the original sender's location from the location-based service. Still, the role of the Seed OppNet is (Not Defined).

Using dynamic clustering, P. Kaur and J. Singh [84], proposed a scheme that protects users' identity within an OppNet. However, the notion of clusters does not match Opportunistic Networks' characteristics. The authors seem not to have a good understanding of OppNets' demands when proposing their scheme. Therefore, the role of the Seed OppNet is (Not Defined).

R. Huang *et al.* [85] proposed a mechanism to protect both the identity and the location of a user that requests the location-based services. The proposed scheme utilises users' social ties to achieve location privacy obfuscation. The location-based services' server is crucial to the proposed scheme. However, it not clear how all this meet OppNets' requirements. Therefore, the role of the Seed OppNet is (Not Defined).

The authentication schemes C. Carver and X. Lin [68], P. Kumar *et al.* [73], P. Kumar *et al.* [74], C.B. Avoussoukpo *et al.* [76], C.B. Avoussoukpo *et al.* [78], already discussed in the authentication section also protect users' identity with the role of the Seed OppNet being (High Degree).

The authentication scheme M.H. Guo *et al.* [70] discussed in the authentication section protects users' identity too. The role of the Seed OppNet is (Small Degree).

All in all, as illustrated in Fig. 16, the authors proposed various privacy protection methods to tackle identity, location, and social links' issues. Moreover, Fig. 17 exposed authors understanding of OppNets' characteristics and requirements. Most schemes do not include the Seed OppNet in their schemes.

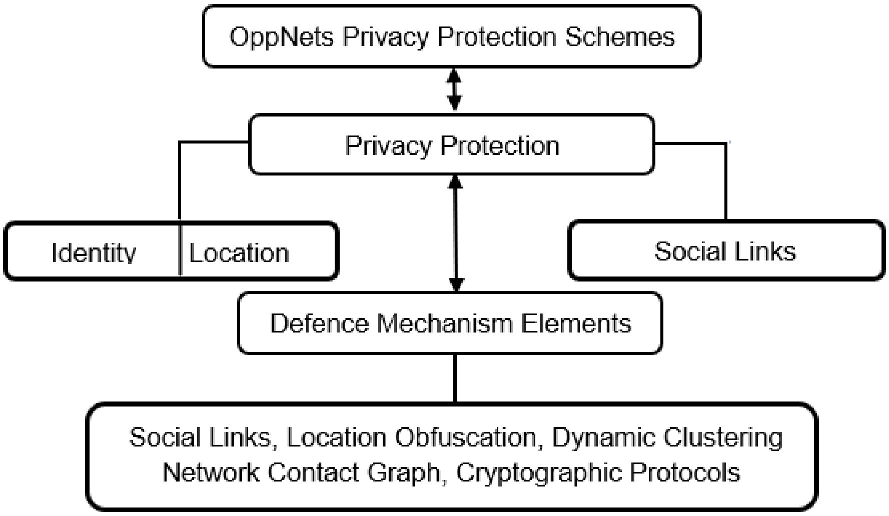
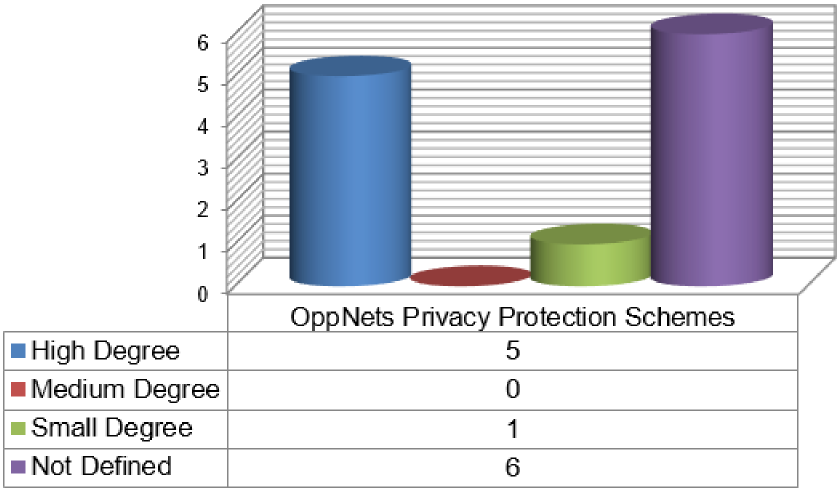

OppNets Privacy Protection Schemes
Privacy Protection
Identity
Location
Social Links
Defence Mechanism Elements
Social Links, Location Obfuscation, Dynamic Clustering
Network Contact Graph, Cryptographic Protocols

FIGURE 16. Taxonomy of OppNets Privacy Protection schemes.



	OppNets Privacy Protection Schemes
🟦 High Degree	5
🟥 Medium Degree	0
🟩 Small Degree	1
🟪 Not Defined	6

FIGURE 17. Evaluation of OppNets Privacy Protection schemes.

D. OppNets DATA AGGREGATION AND TECHNOLOGY

In an Opportunistic Network, to achieve a precise goal, the Seed OppNet has to deal with many other nodes called Helpers. So, data aggregation is paramount for the Seed OppNet to process efficiently data coming from Helpers. On the other hand, OppNets is still in its infancy and needs adequate technologies for its applications. In the following, we provide a brief but comprehensive review of OppNets' articles that tackled the questions of data aggregation and technology. Also, we point out the relevance of these articles under OppNets' constraints.

C.B. Avoussoukpo *et al.* [78] proposed a data aggregation mechanism for Opportunistic Networks that helps a Seed OppNet process at once pieces of information from Helpers. The proposed scheme harnesses the strength of digital signatures, *BLS* signature, and the aggregate *BLS* signatures; releasing the Seed OppNet of the burden of processing data coming from Helpers one at a time. The Seed OppNet is in charge of the system initialisation, nodes' registration, and the authentication process. So, the role of the Seed OppNet is (High Degree).

R.A. Difazio and P.R. Chitrapu [86] suggested a bandwidth management(BWM) policy to alleviate disconnectivity's issues in Opportunistic Networks. The bandwidth management policy has a bandwidth management controller equipped with a processor tailored to perform some task. The authors claim BWM could be useful in combining a lower speed, broad area network with continuous connectivity within OppNets with intermittent connectivity by generating a multi-connection service. The proposed policy is supposed to anticipate future events of an OppNet and use a learned route to infer how much data is cached from a

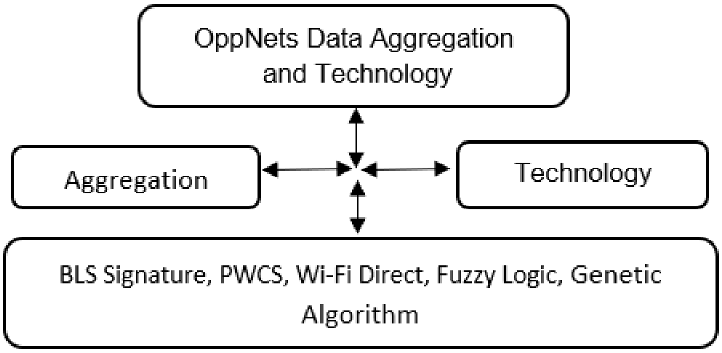

OppNets Data Aggregation and Technology
Aggregation
Technology
BLS Signature, PWCS, Wi-Fi Direct, Fuzzy Logic, Genetic Algorithm

FIGURE 18. **Taxonomy of OppNets Data Aggregation and Technology.**

wireless transmit-receive unit for a connection event. Despite the excellent achievement, placing their contribution within Opportunistic Networks' context is hard. The role of the Seed OppNet is (Not Defined).

For Opportunistic Networks need appropriate technology for their real-world applications, C.B. Avoussoukpo *et al.* [87] identified an existing technology that could help OppNets solve some of their challenges: the Polyvalent Wireless Communication System (PWCS). The authors clarified the concept of OppNets, described the PWCS technology, and showed the correlation between OppNets and the PWCS technology. They also discussed the limitations of PWCS technology. Despite the insightful contribution, the role of the Seed OppNet is (Not Defined).

Placing Opportunistic Networks within Delay Tolerant Networks and the Internet of Things while acknowledging the challenges that come with OppNets, M. Cuka *et al.* [88], to alleviate some of OppNets' challenges, proposed the design and implementation of an integrated intelligent system using fuzzy logic and genetic algorithm-based methods. For opportunistic Networks have particular characteristics, IoT device speed, IoT device density, IoT device remaining energy, IoT device selection decision, selection operator, crossover operator, and mutation operator, are the parameters required for the implementation of the integrated intelligent system. The role of the Seed OppNet is (Not Defined).

With the requisite that Opportunistic Networks rely upon little or no infrastructure, A. Ippisch and K. Graffi [89] created a mobile network application that connects android devices via Wi-Fi, aiming to answer some of OppNets' challenges. In effect, the proposed application forms or simulates an Opportunistic Network for smartphone-to-smartphone data transmission using the infrastructure mode of Wi-Fi for direct connections, providing an identification scheme to enable multi-hop routing. The application runs without users' interaction in the background and offers security thanks to symmetric and asymmetric encryptions. The role of the Seed OppNet is (Not Defined).

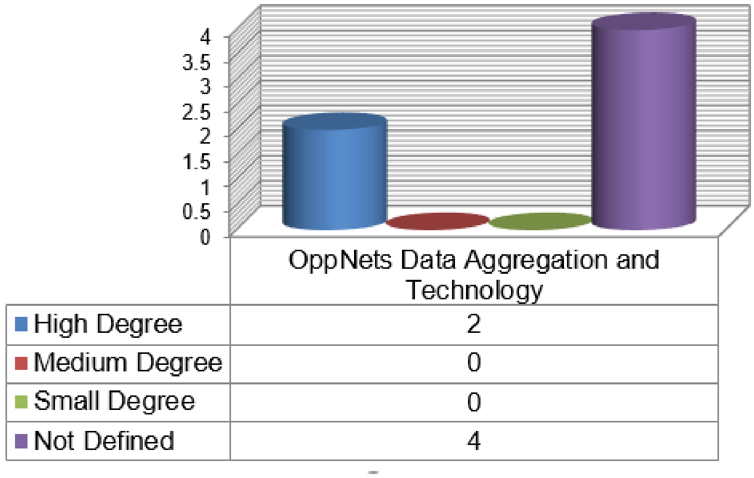
Opportunistic Networks are still more conceptual than practical. That is why M. Conti *et al.* [90] investigated the feasibility of creating Opportunistic Networks on top of Wi-Fi Direct. The experiment focuses on devices' discovery and group formation. In the devices' discovery phase, devices collect information about the neighbouring devices and find potential Helpers by scanning available supported wireless channels. The group phase, on the other, is under the supervision of the group owner, who plays the role of the Seed OppNet. This experiment describes OppNets correctly since it involved all the vital elements of OppNets. The group owner is in charge of the system initialisation, registration, and management; therefore, the role of the Seed OppNet is (High Degree).

As elaborated in Fig. 18, the authors were concerned with the applicability of Opportunistic Networks. They supported their ideas with existing notions such as *BLS* signature, PWCS, wi-fi direct, fuzzy logic system, and genetic algorithm. Moreover, as illustrated in Fig. 19, most schemes proposed for OppNets data aggregation and technology do not fully understand Opportunistic Networks' requirements for only two proposals included the Seed OppNet.

E. OppNets ROUTING

Besides authentication, privacy protection, data aggregation and technology, and intrusion detection, information or message routing in a temporary self-configured network such as Opportunistic Networks is a challenge for there is no predefined source-destination path. The completion of an OppNet's mission demands proper routing protocols that understand Opportunistic Networks' requirements. This section provides a brief but concise and comprehensive review of Opportunistic routing related schemes and points out the role plays by the Seed OppNet in each of these schemes.

M.A.T Prodhan *et al.* [91] proposed a quota-based routing scheme to solve the higher network contention and latency's problems created by the method that meant better chances of message delivery. In effect, flooding an Opportunistic Network with copies of the same message increases messages' chances of distribution. The proposed scheme aims to boost the message delivery ratio while reducing network contention and latency. The key features that make the proposed different



	OppNets Data Aggregation and Technology
🟦 High Degree	2
🟥 Medium Degree	0
🟩 Small Degree	0
🟪 Not Defined	4

FIGURE 19. **Evaluation of OppNets Data Aggregation and Technology.**

from other quota-based routing protocols are the probabilistic metric and the adaptive message priority principle. The authors have not integrated the Seed OppNet in their scheme; therefore, the role of the Seed OppNet is (Not Defined).

In a particular environment such as OppNets, integrating users' gregarious nature in a design can help boost the network functionality in many ways. R. Ciobanu *et al.* [92] used users' experience (social connection, interests, contacts history) to proposed an Opportunistic, social-aware and interest-based dissemination scheme that aims to reduce bandwidth consumption and congestion. In the proposed algorithm, not all nodes can transmit messages; only selected nodes are forwarders. The proposed scheme does not conform to OppNets' reality. Therefore, the role of the Seed OppNet is (Not Defined).

With the popular theory that no status or condition is permanent, S. Premalatha and V.M.A. Rajam [93] understood that a node could change any time from a friendly state to a selfish or malicious state. So, they proposed a routing algorithm that first considers the reputation of nodes before data forwarding. The authors do not understand the temporary nature of OppNets. Thus, the Seed OppNet role is (Not Defined).

Opportunistic Networks are of the self-organised's group; they have a mission and always invite potential Helpers to help achieve their goal. So, any pre-established link between Helpers could boost the transmission of information. That is why D. Huang *et al.* [94] proposed a link prediction pattern with kernel regression to improve information delivery rate within Opportunistic Networks. Despite the excellent idea proposed in the scheme, the scheme's conformity to Opportunistic Networks' requirements needs proof. Thus, the role of the Seed OppNet is (Not Defined).

Acknowledging that all nodes in an OppNet can act as a server, E. Papapetrou *et al.* [95] proposed a routing mechanism that uses SimBet protocol and Bloom filters for routing while preserving nodes' privacy. The proposed scheme does not use cryptographic protocols but relies on Bloom filters. Such a good scheme could have been an excellent proposal if the authors integrated the Seed OppNet in their scheme. Therefore, the role of the Seed OppNet is (Not Defined).

Classifying Opportunistic Networks routing schemes into two categories: single-copy and multi-copy schemes, L. Li *et al.* [96] proposed a routing mechanism to make a better tradeoff between the performance of single-copy and multi-copy methods. The authors suggested an algorithm based on the Nash Bargaining Solution (NBS) to improve the information delivery ratio and to use the network resources adequately. Their proposed scheme, called GameR, is designed to answer three main questions: the choices of the messages and nodes pairs for message delivery, the proper time to duplicate message copies, and the number of message copies that should be delivered. Despite the solutions proposed, the role of the Seed OppNet for this scheme is (Not Defined).

For users represent the heart of OppNets, self-configured networks such as Opportunistic Networks will function best if only users' experience is incorporated in OppNets related design. L. Yao *et al.* [97] included social trust in their routing decision and proposed a routing mechanism based on nodes' observation. Although nodes monitoring one another is a useful feature, the role assigned to the Seed OppNet is unknown. Therefore, the role of the Seed OppNet is (Not Defined).

Routing within an OppNet is always a challenge. Using nodes' collaboration and the dynamic Euclidean distance between every two sets of nodes as the basis of their design, S.K. Dhurandher *et al.* [98] proposed a routing scheme based on encounter and distance. Still, the role of the Seed OppNet is (Not Defined).

D.K. Sharma *et al.* [99] acknowledged that an OppNet could start with a single node. Moreover, they proposed a priority (first in, first out) routing mechanism for Opportunistic Networks. The main factors that characterise their scheme are urgency and security. However, the role of the Seed OppNet is (Not Defined).

Machine Learning has proved to be a useful tool when one has to deal with Things. That is why D.K. Sharma *et al.* [100], using a decision tree and neural networks, proposed a machine learning-based method to decide the probability of successful message delivery within OppNets. Nonetheless, the role of the Seed OppNet is (Not Defined).

Cooperation between modes is vital for any OppNet to reach its goal. A. Bamrah *et al.* [101] used the concept of centrality to better their previous scheme; History-Based Prediction Routing Protocol for OppNets. With a history table, home location table, and centrality table, the proposed scheme can boost message delivery. However, the role of the Seed OppNet is (Not Defined).

K. Khalid *et al.* [102] were concerned about energy consumption when routing messages within OppNets. They proposed an energy-aware version of their previously proposed scheme; History-Based Prediction Routing Protocol for OppNets. The energy constraints incorporated in the new scheme helps empty the buffer from already delivered messages. The role of the Seed OppNet is (Not Defined).

Without trust, Opportunistic Networks will undoubtedly amount to nothing. L. Li *et al.* [103] resorted to social trust and network coding to proposed a secure routing method for OppNets. The following parameters determine the trust value: the ratio of the number of contacts, duration of connections, number of forwarding packets, and the attributes matching. Still, the role of the Seed OppNet is (Not Defined).

J. Yoon *et al.* [104] were concerned with the limitations of the friendship-based routing methods for OppNets. They proposed a routing scheme to enhance the friendship-based routing mechanism. To apply regularity correctly, their proposed routing mechanism considers the inter-contact time and the contact duration. Nonetheless, the role of the Seed OppNet is (Not Defined).

With the privacy challenges inherent to routing within OppNets, X. Wang *et al.* [105] proposed a privacy protection routing mechanism that ensures effective communication. The proposed scheme has three main components; security-based mobility prediction, message handler, and report process. However, the Seed OppNet has no role in the proposed scheme. Therefore, the role of the Seed OppNet is (Not Defined).

In a hostile environment such as OppNets, some nodes can be selfish. Also, the selfishness of nodes can cause a delay that is energy-consuming. To solve nodes' possible selfish behaviour and reduce energy consumption, A. Chhabra *et al.* [106], based on the Stackelberg games, proposed a rewarding mechanism where selfish nodes get a negative reward while cooperative nodes get a positive appreciation. However, the role of the Seed is (Not Defined).

Nodes' mobility is advantageous to OppNets because mobility can help forward messages within an OppNet's environment. D.K. Sharma *et al.* [107] using existing established routing protocols and probabilistic routing techniques based on nodes' movements, proposed a routing mechanism that predicts the best path to take for a message to reach its destination. For the Seed OppNet got no role in the scheme, the role of the Seed OppNet is (Not Defined).

Energy is not always available for use in OppNets. S.J. Borah *et al.* [108] proposed three energy-effective algorithms for messages routing within OppNets' environment. The three proposed algorithms are an improvement of the protocols PROPHET, PRoWAIT, and EDR. However, the role of the Seed OppNet is (Not Defined).

In an OppNet, Helpers that are supposed to help complete the OppNet's mission may also display malicious behaviour making routing more challenging and even impossible. D.K. Sharma *et al.* [109] proposed a trust-like routing protocol that identifies the excellent node in a message forwarding process. The proposed scheme relies on a dataset that stores nodes' historical behaviours. The role of the Seed OppNet is (Not Defined).

Without nodes' mobility, there are no Opportunistic Networks. The coming in and leaving out the OppNets' features of nodes is an asset for OppNets. Using both OppNets' simulator (ONE) and pedestrian's simulator (pedSim), L. Chancay-Garcia *et al.* [110] evaluated ''the coming and leaving'' the OppNets' phenomenon. Here, the role of the Seed OppNet is (Not Defined).

M. Gupta *et al.* [111] decided to contribute to the open research problem of geocasting in OppNets. The authors proposed a novel geocasting for message dissemination to nodes within OppNets' environment. The novel suggested scheme depends on three steps; definition of the geographical region, unicasting, and data dissemination. The role of the Seed OppNet is (Not Defined).

V. Kuppusamy *et al.* [112] analysed Epidemic routing's performance in OppNets and discussed suggestions to optimise Epidemic routing within destination-less OppNets. However, the role of the Seed OppNet is (Not Defined).

Among other challenges haunting Opportunistic Networks are packets dropping attacks and their likes. D.K. Sharma *et al.* [113] proposed a routing mechanism based on Deep Learning to mitigate these problems. The memory of nodes' past experiences is considered before making decisions. After simulations, the proposed scheme outperforms some well-established routing protocols such as PRoPHET. The idea developed in this article is excellent; however, the proposed scheme could be better if the Seed OppNet was given an exact role. Therefore, the role of the Seed OppNet is (Not Defined).

For information to reach the desired destination, some routing mechanisms rely on the blind replication's method. However, the blind replication's method is energy-consuming. What is more, the blind replication's method may create selfish behaviour's tendency in nodes. That is why S. Sati *et al.* [114] proposed an energy-saving routing protocol that aims to use a minimum of nodes to deliver a

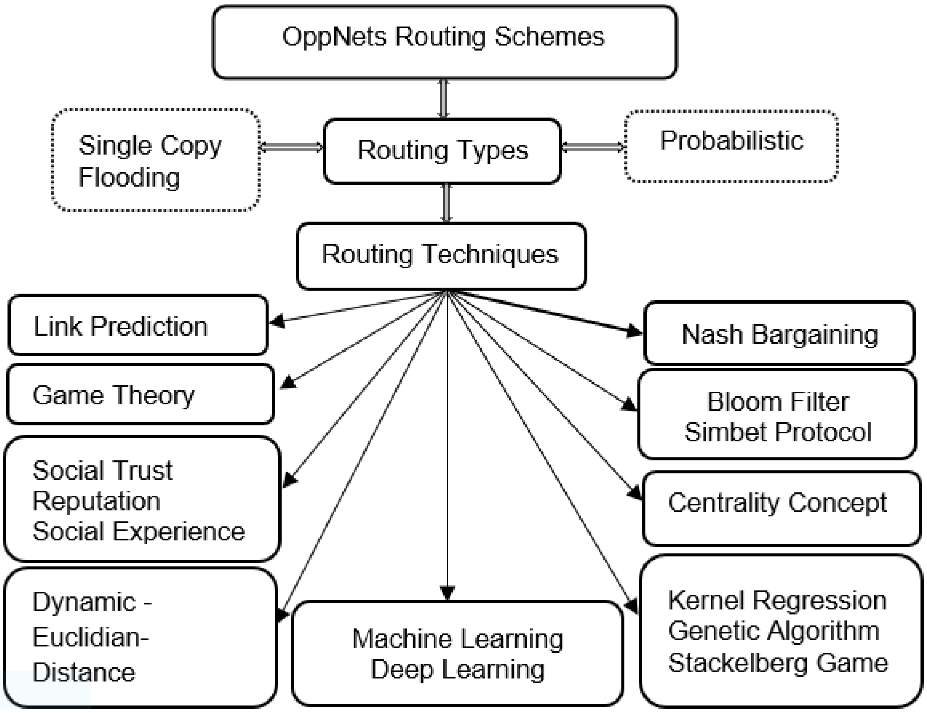

OppNets Routing Schemes
Single Copy Flooding
Routing Types
Probabilistic
Routing Techniques
Link Prediction
Game Theory
Social Trust Reputation Social Experience
Dynamic - Euclidian- Distance
Machine Learning Deep Learning
Nash Bargaining
Bloom Filter Simbet Protocol
Centrality Concept
Kernel Regression Genetic Algorithm Stackelberg Game

FIGURE 20. Taxonomy of OppNets Routing Schemes.

successful message. Still, the role of the Seed OppNet is (Not Defined).

OppNets rely on nodes' mobility. So, navigating in such an environment incurs communication delay and possible message delivery failure, among others. To mitigate transmission delay and message delivery failure within OppNets, S. Zhang *et al.* [115] proposed a prediction-based routing mechanism. The proposed method mainly depends on nodes' past experiences. However, the role of the Seed OppNet is (Not Defined).

Human beings do not move aimlessly; they move to meet their expectation for a purpose, justifying the Expectancy Theory of Value of Psychology. Moreover, moving for a purpose confines human beings naturally within geographical regions. S. Liu *et al.* [116] used the Psychology's Expectancy Theory of value and the concept of geographic functional cells to propose a routing method for Opportunistic Networks. The role of the Seed OppNet in the proposed scheme is (Not Defined).

Energy sustains life in all networks in general and Opportunistic Networks in particular. Any scheme or protocol that aims to avail power is worthy of study. Using the learning automata's approach, F. Zhang *et al.* [117], from *n*-Epidemic protocol, proposed an energy-efficient routing mechanism. The role of the Seed OppNet is (Not Defined).

All routing protocols aim to achieve higher messages delivery. Nevertheless, H. Ma *et al.* [118] believed that focusing only on higher message delivery results in an unfairness among nodes within OppNets when it comes to forward information. Identifying the main factors that may establish fairness among nodes, the authors proposed a fairness-aware routing method that optimises the information delivery ratio. However, the role of the Seed OppNet is (Not Defined).

Delay is not desirable, even in Delay Tolerant Networks. S. Chen *et al.* [119] were concerned with messages retransmission's delays within OppNets. So, they proposed a delay reduction routing scheme for Opportunistic Networks. However, the role of the Seed OppNets is (Not Defined).

Routing within Opportunistic Networks is a hot and daunting task. Also, the multiple copy techniques used for routing within OppNets have drawbacks, including the excessive usage of network resources. M. Erdogan *et al.* [120] proposed a partial flooding routing mechanism to reduce energy consumption within OppNets. However, the authors did mention nothing about the Seed OppNet. Therefore, the role of the Seed OppNet is (Not Defined).

An OppNet starts life with a Seed OppNet (root node, seed node) and uses opportunistically all possible resources available at its vicinity to reach a predefined goal. J.W. Baird [10] did have an excellent command over OppNets' demands and proposed a trust-based routing mechanism within Opportunistic networks. In the proposed scheme, the network, first and foremost, elects a Seed OppNet (root node) responsible for assigning prefix-label numbers to Helpers. However, a Seed OppNet does not designate the prefix-label numbers continually. So, the role of the Seed OppNet is close to one of the nodes in charge of registration. Therefore, the role of the Seed OppNet is (Small Degree).

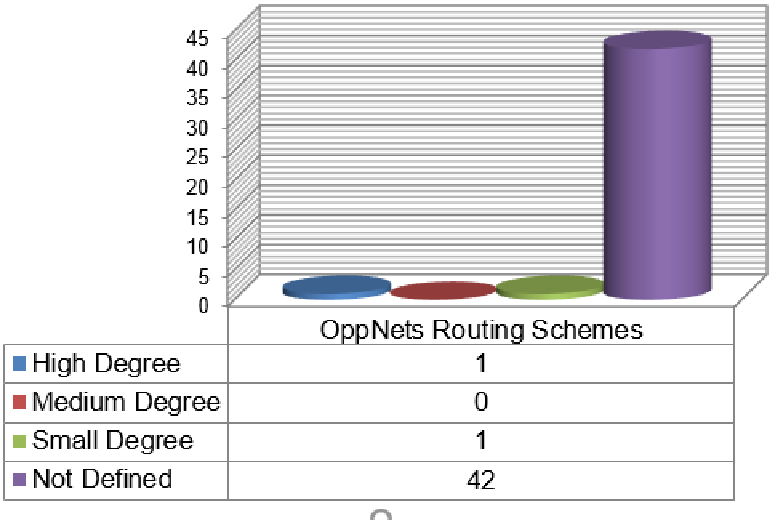


FIGURE 21. Evaluation of OppNets Routing schemes.

Physical proximity prediction is an essential factor in routing in challenging networks such as for Opportunistic Networks. L. Liu [121] proposed a physical proximity prediction routing protocol that outperforms Epidemic and PRoPHET routing protocols. For the proposed scheme, every mobile device maintains its physical locations and keeps its friends' physical locations' history. The role of the Seed OppNet is (Not Defined).

Opportunistic Networks highly depend on Helpers. Therefore, any social relation among Helpers could help boost OppNets' performance. X.H. Wu *et al.* [122] proposed a social-based routing mechanism that integrates; social relation's value and network topology's information before making a routing decision. The role of the Seed OppNet is (Not Defined).

The concept of Opportunistic Networks needs concrete examples of application for the researchers diving into OppNets to understand the Opportunistic Networks' characteristics better. Y. Xie *et al.* [123] applied OppNets to urban scenarios. The proposed scheme relies on nodes' grouping. The routing method considers three groups of nodes: super nodes, backbone nodes, and ordinary nodes. However, the role of the Seed OppNet is (Not Defined).

Opportunistic Networks have not only a dynamic topology but also nodes that have dynamic social interactivity. So any routing mechanism that relies on static social interactivity does have some limits. G. Xu *et al.* [124] evaluated the drawbacks of OppNets' routing methods based on dynamic social connections and proposed a novel opportunistic routing mechanism based on dynamic social relationships. However, the role of the Seed OppNet is (Not Defined).

W. Chen *et al.* [125] understood that although OppNets are infrastructure-less, they do rely, somehow, on a Seed OppNet that starts and ends the life process of an Opportunistic network. The authors proposed a routing method for the OppNets' environment with Ferry nodes as the Seed OppNet. The proposed scheme also includes users' experience. Here, the Seed OppNet plays the role of a central authority. Therefore, the role of the Seed OppNet is (High degree).

Routing within Opportunistic Networks has increasingly become a fascinating topic to the OppNets' research community. X. Wang *et al.* [126] were concerned with the time efficiency when routing within an OppNet. With the help of users' daily routine, and the new parameter (success ratio), the authors proposed a lightweight routing algorithm to build the forwarding table. The proposed scheme also aims to save the OppNets' resources. However, the role of the Seed OppNet is (Not Defined).

Routing methods that apply to Delay Tolerant Networks or Mobile ad hoc Networks do not apply to Opportunistic networks, for they have different characteristics. L.J. Chen *et al.* [127] proposed a routing mechanism that aims to leverage the robustness of the coding-base routing techniques and the performance's advantages of replication methods. Although the simulation results are satisfactory, the scheme's description does not include the core definition that OppNets rely on devices' discovery. Therefore, the role of the Seed OppNets is (Node Defined).

Traditional routing methods do not fit Opportunistic Networks' demands. For routing decision, M. Chen and H. Wang [128] suggested the use of all available information such as; nodes' attributes, contacts' attributes, messages' attributes. They proposed a routing mechanism that considers the factors mentioned above before forwarding a message. However, for a temporary network such as OppNets, the proposed method's relevance to Opportunistic Networks is questionable. The role of the Seed OppNet is (Not Defined).

Selfish nodes degrade Opportunistic Networks' performance and may also prevent the accomplishment of the Seed OppNet's goal. D. Soares *et al.* [129] proposed a routing

TABLE 2. Overview of Opportunistic Networks Proposals.

Article and Year	Category	Techniques	Role of the Seed OppNet	Relevant to OppNets
[53]-2013	Intrusion Detection	Trust	High Degree	Yes
[54]-2014	Intrusion Detection	Trust, Reputation	Not Defined	No
[55]-2014	Intrusion Detection	Trust, Reputation	Not Defined	No
[56]-2015	Intrusion Detection	Merkle Tree Hashing	Not Defined	No
[57]-2015	Intrusion Detection	Hash Chain	Not Defined	No
[58]-2015	Intrusion Detection	Hash Chain	Not Defined	No
[59]-2015	Intrusion Detection	Cryptographic Protocols	Not Defined	No
[60]-2016	Intrusion Detection	Merkle Root, Trust	Not Defined	No
[61]-2016	Intrusion Detection	Merle Tree, Trust, Reputation	Not Defined	No
[62]-2016	Intrusion Detection	Trust	Not Defined	No
[63]-2017	Intrusion Detection	Trust, Reputation	Not Defined	No
[64]-2017	Intrusion Detection	Merle Tree, Trust, Reputation	Not Defined	No
[65]-2017	Intrusion Detection	Cryptographic Protocols, Trust	Not Defined	No
[66]-2019	Intrusion Detection	Kolmogorov-Smirnov Two Sample Test	Not Defined	No
[67]-2011	Authentication	'Best-Effort' Authentication	Not Defined	No
[68]-2012	Authentication	Cryptographic Protocols	High Degree	Yes
[69]-2014	Authentication	Multidimensional Scaling, Trust	Small Degree	Yes
[70]-2015	Authentication	Cryptographic Protocols, Trust	Small Degree	Yes
[71]-2015	Authentication	Trust, Reputation	Not Defined	No
[72]-2017	Authentication	Cryptographic Protocols	Medium degree	Yes
[73]-2017	Authentication	Cryptographic Protocols	High Degree	Yes
[74]-2018	Authentication	Cryptographic Protocols, Trust	High Degree	Yes
[75]-2018	Authentication	Cryptographic Protocols	High Degree	Yes
[76]-2018	Authentication	Cryptographic Protocols, Trust	High Degree	Yes
[77]-2019	Authentication	NRTU algorithm	Medium Degree	Yes
[78]-2020	Authentication	BLS signature, aggregate BLS signatures	High Degree	Yes
[79]-2020	Authentication	Identity-based Encryption	High Degree	Yes
[80]-2014	Privacy Protection	Network Contact Graph	Not Defined	No
[81]-2015	Privacy Protection	Social Links, Bloom Filter	Not Defined	No
[82]-2012	Privacy Protection	Social Links, Location Obfuscation	Not Defined	No
[83]-2013	Privacy Protection	Social Links, Lightweight Markov Model	Not Defined	No
[84]-2015	Privacy Protection	Dynamic Clustering	Not Defined	No
[85]-2018	Privacy Protection	Social Links, Location Obfuscation	Not Defined	No
[68]-2012	Privacy Protection	Cryptographic Protocols	High Degree	Yes
[73]-2017	Privacy Protection	Cryptographic Protocols	High Degree	Yes
[74]-2018	Privacy Protection	Cryptographic Protocols, Trust	High Degree	Yes
[76]-2018	Privacy Protection	Cryptographic Protocols	High Degree	Yes
[78]-2020	Privacy Protection	BLS signature, aggregate BLS signatures	High Degree	Yes
[70]-2015	Privacy Protection	Cryptographic Protocols	Small Degree	Yes
[78]-2020	Data Aggregation and Technology	BLS signature, aggregate BLS signatures	High Degree	Yes
[86]-2016	Data Aggregation and Technology	Bandwidth Management	Not Defined	Yes
[87]-2020	Data Aggregation and Technology	PWCS	Not Defined	Yes
[88]-2017	Data Aggregation and Technology	Fuzzy Logic and Genetic Algorithm	Not Defined	Yes
[89]-2017	Data Aggregation and Technology	Wi-Fi Direct	Not Defined	Yes
[90]-2013	Data Aggregation and Technology	Wi-Fi Direct	High Degree	Yes
[91]-2011	Routing	Probabilistic Metric, Quota, Priority	Not Defined	No
[92]-2014	Routing	Trust, Reputation	Not Defined	No
[93]-2014	Routing	Trust, Reputation	Not Defined	No
[94]-2015	Routing	Kernel Regression	Not Defined	No
[95]-2015	Routing	SimBet Protocol, Bloom Filter	Not Defined	No
[96]-2015	Routing	SimBet Nash Bargaining	Not Defined	No
[97] -2015	Routing	Trust, Reputation	Not Defined	No
[98] -2016	Routing	Dynamic Euclidean	Not Defined	No
[99] -2016	Routing	Priority	Not Defined	No
[100]-2016	Routing	Machine Learning	Not Defined	No
[101]-2016	Routing	Concept of Centrality	Not Defined	No
[102]-2016	Routing	Experiment	Not Defined	No
[103]-2016	Routing	Social Trust, Network Coding	Not Defined	No
[104]-2016	Routing	Social Trust	Not Defined	No
[105]-2017	Routing	Prediction, Cryptographic Protocols	Not Defined	No
[106]-2017	Routing	Stackelberg Game	Not Defined	No
[107]-2017	Routing	Probabilistic Routing, Genetic Algorithm	Not Defined	No
[108]-2017	Routing	Energy Friendly	Not Defined	No
[109]-2017	Routing	Social Trust	Not Defined	No
[110]-2018	Routing	Analysis	Not Defined	No
[111]-2018	Routing	Geocasting	Not Defined	No

TABLE 3. Overview of Opportunistic Networks Proposals.

Article and Year	Category	Techniques	Role of the Seed OppNet	Relevant to OppNets
[112]-2018	Routing	Experiment	Not Defined	No
[113]-2018	Routing	Deep Learning	Not Defined	Yes
[114]-2018	Routing	Energy Friendly	Not Defined	No
[115]-2015	Routing	Reputation	Not Defined	No
[116]-2016	Routing	Expectancy Theory of Value	Not Defined	No
[117]-2017	Routing	Learning Automata	Not Defined	No
[118]-2018	Routing	Fairness-Aware	Not Defined	No
[119]-2018	Routing	Transmitters Selection	Not Defined	No
[120]-2010	Routing	Partial Flooding	Not Defined	No
[10] -2012	Routing	Social Trust	Small Degree	Yes
[121]-2013	Routing	Proximity Prediction	Not Defined	No
[122]-2015	Routing	Social Trust	Not Defined	No
[123]-2016	Routing	Node Grouping	Not Defined	No
[124]-2018	Routing	Social Trust	Not Defined	No
[125]-2016	Routing	User Experience	High Degree	Yes
[126]-2017	Routing	User Experience	Not Defined	No
[127]-2006	Routing	Experiment	Not Defined	No
[128]-2011	Routing	User Experience	Not Defined	No
[129]-2014	Routing	Reputation	Not Defined	No
[130]-2012	Routing	User Experience, Experiment	Not Defined	No
[131]-2017	Routing	User Experience, Experiment	Not Defined	No
[132]-2017	Routing	User Experience, Trust, Reputation	Not Defined	No
[133]-2020	Routing	Trust, Multi-Path Routing	Not Defined	No

mechanism based on nodes' reputation. The authors classified nodes into clusters depending on their degree of selfishness. However, there is no notion of clusters in Opportunistic Networks. The proposed routing mechanism fits mere Mobile ad hoc Networks. The role of the Seed OppNet is (Not Defined).

Opportunistic Networks are user-centric networks where collaborations among nodes are paramount. S. Chupisanyarote *et al.* [130] leveraged the community-like aspect of the nodes to examine the possibility that Things can collect and share data on behalf of other Things. The authors examined three possibilities, hop-limit, greedy relay request, and relay request on-demand. Although simulations suggested satisfactory results, locating the proposed ideas within OppNets' constraints is a daunting task. The role of the Seed OppNet is (Not Defined).

Opportunistic Networks can not function unless Helpers are willing to play their part in a task. W. Jia *et al.* [131] proposed a routing mechanism that harnesses Things' social characteristics. Their study came up with a threshold where nodes forward messages with the highest probability. However, The study did not include a Seed OppNet. Therefore, the role of the Seed OppNet is (Not Defined).

Without Helpers' participation, any OppNet's mission is doomed to fail. A. Kumar *et al.* [132] proposed a routing mechanism based on Helpers' altruism value. In their protocol, an altruism value is dynamic and determines the trustworthiness of a Helper. However, the authors' definition of Opportunistic Networks proves that they are not familiar with OppNets; their scheme is suitable for Delay Tolerant Networks. The role of the Seed OppNet is (Not Defined).

Trust and security are exciting features for Opportunistic Networks. S.K. Dhurandher *et al.* [133] suggested a routing protocol that includes secure multipath techniques and trust. However, neither the temporary nor the self-configured aspects of OppNets have been reflected in their proposal. The role of the Seed OppNet is (Not Defined).

In the light of the study of Opportunistic Networks routing schemes, as depicted in Fig. 20, the authors proposed single copy, flooding, and probabilistic routing types that included various manifold techniques. Moreover, despite the useful notions discussed in their proposals, as highlighted in Fig. 21, most routing schemes proposed for Opportunistic Networks did not include the Seed OppNet. So, the OppNets' routing schemes, somehow, lack substance.

VI. ANALYSIS

Opportunistic Networks, also called OppNets, are of the self-organised or self-configured's group. An OppNet does rely on opportunistic communication to function; however, OppNets should not be confused with mere opportunistic communication within Mobile ad hoc Networks or Delay-Tolerant Networks; an OppNet's life starts and ends with a Seed OppNet. A Seed OppNet with a predefined mission will also manage within the established Opportunistic Networks certified nodes called Helpers. The Seed OppNet with Helpers become an extended or expanded Seed OppNet. The degree of involvement of a Seed OppNet in an Opportunistic Networks' scheme determines how realistic or relevant this proposed scheme is to OppNets' characteristics and demands. As illustrated in Fig. 22 and depicted in Table 2 and Table 3, apart from the schemes proposed for OppNets authentication and OppNets privacy protection

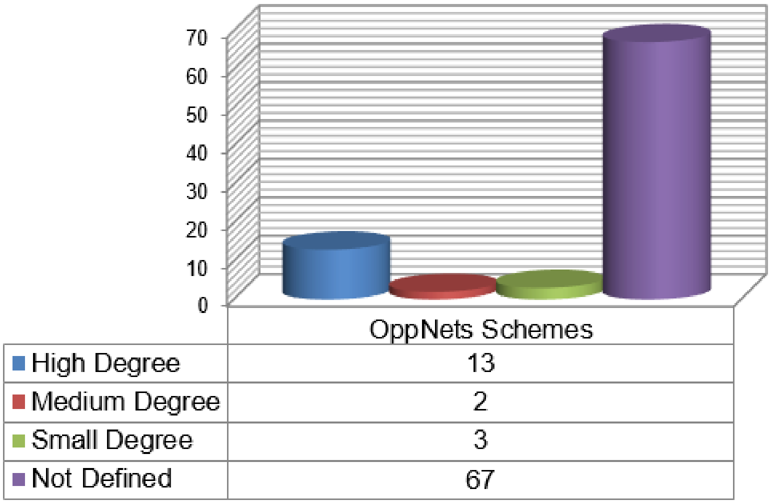


FIGURE 22. Evaluation of OppNets schemes.

that, to some extent, reflected, Opportunistic Networks' characteristics and demands; those proposed for OppNets intrusion detection, OppNets data aggregation and technology, and OppNets routing did not include OppNets' requirements. They failed to give the Seed OppNet a role. Therefore, these schemes are not relevant to Opportunistic Networks. They might be relevant to Mobile ad hoc Networks, Delay Tolerant Networks, or Opportunistic Communications as a whole. Any scheme designed for OppNets should include a Seed OppNet with a clearly defined role. We suggest that Opportunistic Networks are self-configured, temporary, and heterogeneous networks with unknown topology and an example of the Internet of Things, Internet of Vehicles, Industrial Internet of Things, and the Internet of Everything with Mobile ad hoc Networks' characteristics that need formalisations and breakthroughs. We introduce the novel idea of OppCNets (Opportunistic Communication Networks) that factors in the following notions: first, the Opportunistic Networks' definitions of B. Bhargava *et al.* [8], and L. Lilien *et al.* [9], second, the use of versatile wireless communication mechanisms or technologies, third, the use of a universal aggregator for data processing. OppCNets will be discussed in future works.

REFERENCES

[1] U. Cisco. *Cisco Annual Internet Report (2018–2023) White Paper*. Accessed: Dec. 17, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual -internet-report/white-paper-c11-741490.html

[2] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," CISCO, San Jose, CA, USA, White Paper 2011, Apr. 2011, vol. 1, pp. 1–11.

[3] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Social big-data-based content dissemination in Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.

[4] S. Sun, "Industrial Internet of Things (IIoT), 5G, and cognitive learning," in *Proc. IEEE Comsoc Asia–Pacific Region Newsletter*, no. 54, Dec. 2018, pp. 1–3.

[5] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, Jul. 2003.

[6] H. Hu, J. Zhang, X. Zheng, Y. Yang, and P. Wu, "Self-configuration and self-optimization for LTE networks," *IEEE Commun. Mag.*, vol. 48, no. 2, pp. 94–100, Feb. 2010.

[7] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT)," in *Proc. Internet Technol. Appl. (ITA)*, Wrexham, U.K., Sep. 2015, pp. 219–224.

[8] B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. S. Dillon, E. Chang, F. K. Hussain, W. Nejdl, D. Olmedilla, and V. Kashyap, "The pudding of trust [intelligent systems]," *IEEE Intell. Syst.*, vol. 19, no. 5, pp. 74–88, Sep./Oct. 2004.

[9] L. Lilien, Z. H. Kamal, V. Bhuse, and A. Gupta, "Opportunistic networks: The concept and research," in *Proc. Challenges Privacy Secur., NSF Int. Workshop Res. Challenges Secur. Privacy Mobile Wireless Netw. (WSPWN)*. Kalamazoo, MI, USA: Western Michigan Univ., 2006.

[10] J. W. Baird, "TAIRO: Trust-aware automatic incremental routing for opportunistic resource utilization networks," in *Proc. IEEE 31st Symp. Reliable Distrib. Syst.*, Irvine, CA, USA, Oct. 2012, pp. 481–482.

[11] C. S. Ding, *Fundamentals of Applied Multidimensional Scaling for Educational and Psychological Research*. New York, NY, USA: Springer, Apr. 2018.

[12] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, Jul. 1970.

[13] A. Broder and M. Mitzenmacher, "Network applications of Bloom filters: A survey," *Internet Math.*, vol. 1, no. 4, pp. 485–509, Jan. 2004.

[14] A. Papadogiannis, D. Gesbert, and E. Hardouin, "A dynamic clustering approach in wireless networks with multi-cell cooperative processing," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 4033–4037.

[15] S. H. Li, Q. W. Yin, Y. J. Hu, M. Guo, and X. J. Fu, "Overview of researches on ontology," *J. Comput. Res. Develop.*, vol. 7, no. 12, pp. 1041–1052, Jul. 2004.

[16] T. Hossmann, G. Nomikos, T. Spyropoulos, and F. Legendre, "Collection and analysis of multi-dimensional network data for opportunistic networking research," *Comput. Commun.*, vol. 35, no. 13, pp. 1613–1625, Jul. 2012.

[17] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.

[18] S. William, *Computer Security: Principles and Practice*. Upper Saddle River, NJ, USA: Pearson, 2012.

[19] J. H. Cheon, "Security analysis of the strong Diffie-Hellman problem," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, May 2006, pp. 1–11.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Nov. 1984, pp. 47–53.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003.

[22] T. Tassa, "Hierarchical threshold secret sharing," *J. Cryptol.*, vol. 20, no. 2, pp. 237–264, Apr. 2007.

[23] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 259–277, Feb. 2006.

[24] H. J. Choi and B. S. Jeong, "A timestamp-based optimistic concurrency control for handling mobile transactions," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin Springer, pp. 796–805, May 2006.

[25] A. L. Samuel, "Some studies in machine learning using the game of checkers," *IBM J. Res. Develop.*, vol. 44, no. 1.2, pp. 206–226, Jan. 2000.

[26] K. A. M. Evans and S. A. A. Elmustafa, "Internet of Things applications, challenges and related future technologies," *World Sci. Newsr.*, vol. 2, no. 67, pp. 126–148, 2017.

[27] E. Fleisch, M. Weinberger, and F. Wortmann, "Business models and the Internet of Things," in *Proc. Interoperability Open-Source Solutions Internet Things*. Cham, Switzerland: Springer, 2015, pp. 6–10.

[28] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horizons*, vol. 58, no. 4, pp. 1–11, Apr. 2011.

[29] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *J. Comput. Commun.*, vol. 3, no. 5, p. 164, 2015.

[30] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Social big-data-based content dissemination in Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.

[31] C. Arnold, D. Kiel, and K.-I. Voigt, "How the industrial Internet of Things changes business models in different manufacturing industries," *Int. J. Innov. Manage.*, vol. 20, no. 8, Dec. 2016, Art. no. 1640015.

[32] C. M. Huang, K. Lan, and C. Z. Tsai, "A survey of opportunistic networks," in *Proc. 22nd Int. Conf. Adv. Inf. Netw. Appl.-Workshops (Aina Workshops)*, Okinawa, Japan, Mar. 2008, pp. 1672–1677.

[33] H. A. Nguyen and S. Giordano, "Routing in opportunistic networks," *Int. J. Ambient Comput. Intell.*, vol. 1, no. 3, pp. 19–38, Jul. 2009.

[34] M. Conti and M. Kumar, "Opportunities in opportunistic computing," *Computer*, vol. 43, no. 1, pp. 42–50, Jan. 2010.

[35] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 126–139, Sep. 2010.

[36] D. Karamshuk, C. Boldrini, M. Conti, and A. Passarella, "Human mobility models for opportunistic networks," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 157–165, Dec. 2011.

[37] L. Liu and Y. Jing, "A survey on social-based routing and forwarding protocols in opportunistic networks," in *Proc. IEEE 12th Int. Conf. Comput. Inf. Technol.*, Chengdu, China, Oct. 2012, pp. 635–639.

[38] I. Woungang, S. K. Dhurandher, A. Anpalagan, and A. V. Vasilakos, *Routing in Opportunistic Networks*. New York, NY, USA: Springer, 2013, p. 83.

[39] B. Poonguzharselvi and V. Vetriselvi, "Survey on routing algorithms in opportunistic networks," in *Proc. Int. Conf. Comput. Commun. Informat.*, Coimbatore, India, Jan. 2013, pp. 1–5.

[40] B. Soelistijanto and M. P. Howarth, "Transfer reliability and congestion control strategies in opportunistic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 538–555, 1st Quart., 2014.

[41] C. Boldrini, K. Lee, M. Önen, J. Ott, and E. Pagani, "Opportunistic networks," *Comput. Commun.*, vol. 48, no. 14, pp. 1–4, Mar. 2014.

[42] V. F. S. Mota, F. D. Cunha, D. F. Macedo, J. M. S. Nogueira, and A. A. F. Loureiro, "Protocols, mobility models and tools in opportunistic networks: A survey," *Comput. Commun.*, vol. 48, pp. 5–19, Jul. 2014.

[43] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: A survey," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1812–1827, Jun. 2015.

[44] P. Yuan, L. Fan, P. Liu, and S. Tang, "Recent progress in routing protocols of mobile opportunistic networks: A clear taxonomy, analysis and evaluation," *J. Netw. Comput. Appl.*, vol. 62, pp. 163–170, Feb. 2016.

[45] M. Alajeely, R. Doss, and A. Ahmad, "Security and trust in opportunistic networks—A survey," *IETE Tech. Rev.*, vol. 33, no. 3, pp. 256–268, May 2016.

[46] S. R. Bharamagoudar and S. V. Saboji, "Routing in opportunistic networks: Taxonomy, survey," in *Proc. Int. Conf. Electr., Electron., Commun., Comput., Optim. Techn. (ICEECCOT)*, Mysuru, India, Dec. 2017, pp. 300–305.

[47] J. Dede, A. Forster, E. Hernandez-Orallo, J. Herrera-Tapia, K. Kuladinithi, V. Kuppusamy, P. Manzoni, A. bin Muslim, A. Udugama, and Z. Vatandas, "Simulating opportunistic networks: Survey and future directions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1547–1573, 2nd Quart., 2018.

[48] N. Mantas, M. Louta, E. Karapistoli, G. T. Karetsos, S. Kraounakis, and M. S. Obaidat, "Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: A survey," *IET Netw.*, vol. 6, no. 6, pp. 169–178, Nov. 2017.

[49] S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," *J. Netw. Comput. Appl.*, vol. 103, pp. 157–170, Feb. 2018.

[50] M. Alajeely, R. Doss, and A. Ahmad, "Routing protocols in opportunistic networks—A survey," *IETE Tech. Rev.*, vol. 35, no. 4, pp. 369–387, Jul. 2018.

[51] A. M. Abali, N. B. Ithnin, T. A. Ebibio, M. Dawood, and W. A. Gadzama, "A survey of geocast routing protocols in opportunistic networks," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.* Cham, Switzerland: Springer, Sep. 2019, pp. 683–694.

[52] C. B. Avoussoukpo, C. Xu, and M. Tchenagnon, "Ensuring users privacy and mutual authentication in opportunistic networks: A survey," *IJ Netw. Secur.*, vol. 22, no. 1, pp. 118–125, Jan. 2020.

[53] S. Gupta, S. K. Dhurandher, I. Woungang, A. Kumar, and M. S. Obaidat, "Trust-based security protocol against blackhole attacks in opportunistic networks," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Lyon, France, Oct. 2013, pp. 724–729.

[54] A. Ahmad, M. Alajeely, and R. Doss, "Defense against packet dropping attacks in opportunistic networks," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, New Delhi, India, Sep. 2014, pp. 1608–1613.

[55] M. Alajeely, A. Ahmad, R. Doss, and V. Mak-Hau, "Packet faking attack: A novel attack and detection mechanism in OppNets," in *Proc. 10th Int. Conf. Comput. Intell. Secur.*, Kunming, China, Nov. 2014, pp. 638–642.

[56] M. Alajeely, A. Ahmad, and R. Doss, "Malicious node traceback in opportunistic networks using Merkle trees," in *Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst.*, Sydney, NSW, Australia, Dec. 2015, pp. 147–152.

[57] M. Alajeely, A. Ahmad, and R. Doss, "Malicious node detection in OppNets using hash chain technique," in *Proc. 4th Int. Conf. Comput. Sci. Netw. Technol. (ICCSNT)*, Harbin, China, Dec. 2015, pp. 925–930.

[58] M. Alajeely, R. Doss, and V. Mak-Hau, "Catabolism attack and anabolism defense: A novel attack and traceback mechanism in opportunistic networks," *Comput. Commun.*, vol. 71, pp. 111–1185, Nov. 2015.

[59] N. S. Samaras, K. Kokkinos, C. Chaikalis, and V. Vlachos, "On intrusion detection in opportunistic networks," *Int. J. Innov. Regional Develop.*, vol. 6, no. 3, pp. 222–242, 2015.

[60] A. Ahmad, M. Alajeely, and R. Doss, "Establishing trust relationships in OppNets using Merkle trees," in *Proc. 8th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangalore, India, Jan. 2016, pp. 1–6.

[61] A. Ahmad, M. Alajeely, and R. Doss, "Reputation based malicious node detection in OppNets," in *Proc. 13th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Khon Kaen, Thailand, Jul. 2016, pp. 1–6.

[62] S. Rashidibajgan, "A trust structure for detection of sybil attacks in opportunistic networks," in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Barcelona, Spain, Dec. 2016, pp. 347–351.

[63] S. K. Dhurandher, A. Kumar, I. Woungang, and M. S. Obaidat, "Supernova and hypernova misbehavior detection scheme for opportunistic networks," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Taipei, China, Mar. 2017, pp. 387–391.

[64] A. Ahmad, R. Doss, M. Alajeely, and K. Ahmad, "Securing OppNets from packet integrity attacks using trust and reputation," in *Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Taipei, China, Mar. 2017, pp. 7–12.

[65] S. K. Dhurandher, A. Kumar, and M. S. Obaidat, "Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3191–3202, Dec. 2018.

[66] A. Altaweel, R. Stoleru, G. Gu, and A. K. Maity, "CollusiveHijack: A new route hijacking attack and countermeasures in opportunistic networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Washington, DC, USA, Jun. 2019, pp. 73–81.

[67] J. Solis, P. Ginzboorg, N. Asokan, and J. Ott, "Best-effort authentication for opportunistic networks," in *Proc. 30th IEEE Int. Perform. Comput. Commun. Conf.*, Orlando, FL, USA, Nov. 2011, pp. 1–6.

[68] C. Carver and X. Lin, "A privacy-preserving proximity friend notification scheme with opportunistic networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 5387–5392.

[69] X. Cao and Y. Yin, "An identity authentication scheme for opportunistic network based on multidimensional scaling," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Shanghai, China, Oct. 2014, pp. 87–93.

[70] M.-H. Guo, H.-T. Liaw, M.-Y. Chiu, and L.-P. Tsai, "Authenticating with privacy protection in opportunistic networks," in *Proc. 11th EAI Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness*, Taipei, Taiwan, Aug. 2015, pp. 375–380.

[71] C. Xi, S. Liang, M. Jianfeng, and M. Zhuo, "A trust management scheme based on behavior feedback for opportunistic networks," *China Commun.*, vol. 12, no. 4, pp. 117–129, Apr. 2015.

[72] U. P. Singh and N. Chauhan, "Authentication using trust framework in opportunistic networks," in *Proc. 8th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Delhi, India, Jul. 2017, pp. 1–7.

[73] P. Kumar, N. Chauhan, and N. Chand, "Authentication with privacy preservation in opportunistic networks," in *Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Coimbatore, India, Mar. 2017, pp. 183–188.

[74] P. Kumar, N. Chauhan, N. Chand, and L. K. Awasthi, "SF-APP: A secure framework for authentication and privacy preservation in opportunistic networks," *Int. J. Web Services Res.*, vol. 15, no. 2, pp. 47–66, Apr. 2018.

[75] M. Gupta, "Cyclic redundancy check based data authentication in opportunistic networks," in *Proc. Int. Conf. Wireless Intell. Distrib. Environ. Commun.* Cham, Switzerland: Springer, Aug. 2018, pp. 17–26.

[76] C. B. Avoussoukpo, C. Xu, and M. Tchenagnon, "Towards multi-factor mutual authentication with privacy protection in opportunistic networks," in *Proc. IEEE 18th Int. Conf. Commun. Technol. (ICCT)*, Chongqing, China, Oct. 2018, pp. 885–890.

[77] M. Abouaroek and K. Ahmad, "Node authentication using NTRU algorithm in opportunistic network," *Scalable Comput., Pract. Exper.*, vol. 20, no. 1, pp. 83–92, Mar. 2019.

[78] C. B. Avoussoukpo, C. Xu, M. Tchenagnon, and N. Eltayieb, "Towards an aggregate signature-based authentication for opportunistic networks," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (CyberSA)*, Dublin, Ireland, Jun. 2020, pp. 1–7.

[79] K. Wang and K. Sakai, "Randomized authentication using IBE for opportunistic networks," in *Proc. 49th Int. Conf. Parallel Process. ICPP Workshops*, Edmonton, AB, Canada, Aug. 2020, pp. 1–7.

[80] B. Distl and T. Hossmann, "Privacy in opportunistic network contact graphs," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Sydney, NSW, Australia, Jun. 2014, pp. 1–3.

[81] B. Distl and S. Neuhaus, "Social power for privacy protected opportunistic networks," in *Proc. 7th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangalore, India, Jan. 2015, pp. 1–8.

[82] S. Zakhary and M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 1059–1063.

[83] S. Zakhary, M. Radenkovic, and A. Benslimane, "The quest for location-privacy in opportunistic mobile social networks," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sardinia, Italy, Jul. 2013, pp. 667–673.

[84] P. Kaur and J. Singh, "Ensuring privacy in opportunistic networks using dynamic clustering," in *Proc. Int. Conf. Adv. Comput. Eng. Appl.*, Ghaziabad, India, Mar. 2015, pp. 866–869.

[85] R. Huang, B. Ying, and A. Nayak, "Protecting location privacy in opportunistic mobile social networks," in *Proc. (NOMS) IEEE/IFIP Netw. Oper. Manage. Symp.*, Taipei, Taiwan, Apr. 2018, pp. 1–8.

[86] R. A. Difazio and P. R. Chitrapu, "Bandwidth management (BWM) operation with opportunistic networks," U.S. Patent 9 313 766, Apr. 12, 2016.

[87] C. B. Avoussoukpo, C. Xu, and M. Tchenagnon, "Polyvalent wireless communication system (PWCS); a potentially useful technology for opportunistic networks," in *Proc. IEEE Int. Conf. Artif. Intell. Inf. Syst. (ICAIIS)*, Dalian, China, Mar. 2020, pp. 762–766.

[88] M. Cuka, D. Elmazi, R. Obukata, K. Ozera, T. Oda, and L. Barolli, "An integrated intelligent system for IoT device selection and placement in opportunistic networks using fuzzy logic and genetic algorithm," in *Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Taipei, China, Mar. 2017, pp. 201–207.

[89] A. Ippisch and K. Graffi, "Infrastructure mode based opportunistic networks on Android devices," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Ghaziabad, India, Mar. 2017, pp. 454–461.

[90] M. Conti, F. Delmastro, G. Minutiello, and R. Paris, "Experimenting opportunistic networks with WiFi direct," in *Proc. IFIP Wireless Days (WD)*, Valencia, Spain, Nov. 2013, pp. 1–3.

[91] M. A. T. Prodhan, R. Das, M. H. Kabir, and G. C. Shoja, "Probabilistic quota based adaptive routing in opportunistic networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process.*, Victoria, BC, Canada, Aug. 2011, pp. 149–154.

[92] R.-I. Ciobanu, R.-C. Marin, C. Dobre, V. Cristea, and C. X. Mavromoustakis, "ONSIDE: Socially-aware and interest-based dissemination in opportunistic networks," in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, Krakow, Poland, May 2014, pp. 1–6.

[93] S. Premalatha and V. M. A. Rajam, "Reputation management for data forwarding in opportunistic networks," in *Proc. Int. Conf. Comput. Commun. Informat.*, Coimbatore, India, Jan. 2014, pp. 1–7.

[94] D. Huang, S. Zhang, P. Hui, and Z. Chen, "Link pattern prediction in opportunistic networks with kernel regression," in *Proc. 7th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bangalore, India, Jan. 2015, pp. 1–8.

[95] E. Papapetrou, V. F. Bourgos, and A. G. Voyiatzis, "Privacy-preserving routing in delay tolerant networks based on Bloom filters," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Boston, MA, USA, Jun. 2015, pp. 1–9.

[96] L. Li, Y. Qin, and X. Zhong, "A novel routing scheme for resource-constraint opportunistic networks: A cooperative multiplayer bargaining game approach," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6547–6561, Aug. 2016.

[97] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594–605, Jan. 2016.

[98] S. K. Dhurandher, S. Borah, I. Woungang, D. K. Sharma, K. Arora, and D. Agarwal, "EDR: An encounter and distance based routing protocol for opportunistic networks," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Crans-Montana, Switzerland, Mar. 2016, pp. 1–9.

[99] D. K. Sharma, S. K. Dhurandher, M. S. Obaidat, S. Pruthi, and B. Sadoun, "A priority based message forwarding scheme for opportunistic networks," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Kunming, China, Jul. 2016, pp. 1–5.

[100] D. K. Sharma, S. K. Dhurandher, I. Woungang, R. K. Srivastava, A. Mohananey, and J. J. P. C. Rodrigues, "A machine learning-based protocol for efficient routing in opportunistic networks," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2207–2213, Sep. 2018.

[101] A. Bamrah, I. Woungang, L. Barolli, S. K. Dhurandher, G. H. S. Carvalho, and M. Takizawa, "A centrality-based history prediction routing protocol for opportunistic networks," in *Proc. 10th Int. Conf. Complex, Intell., Softw. Intensive Syst. (CISIS)*, Fukuoka, Japan, Jul. 2016, pp. 130–136.

[102] K. Khalid, I. Woungang, S. K. Dhurandher, L. Barolli, G. H. S. Carvalho, and M. Takizawa, "An energy-efficient routing protocol for infrastructure-less opportunistic networks," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Fukuoka, Japan, Jul. 2016, pp. 237–244.

[103] L. Li, X. Zhong, and Y. Qin, "A secure routing based on social trust in opportunistic networks," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Shenzhen, China, Dec. 2016, pp. 1–6.

[104] J. Yoon, S.-K. Kim, J.-Y. Lee, and K.-Y. Jang, "An enhanced friendship-based routing scheme exploiting regularity in an opportunistic network," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Chengdu, China, Dec. 2016, pp. 51–57.

[105] X. Wang, L. Wang, and Z. Ning, "A privacy-reserved approach for message forwarding in opportunistic networks," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Taipei, Taiwan, Mar. 2017, pp. 1070–1075.

[106] A. Chhabra, V. Vashishth, and D. K. Sharma, "SEIR: A stackelberg game based approach for energy-aware and incentivized routing in selfish opportunistic networks," in *Proc. 51st Annu. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, USA, Mar. 2017, pp. 1–6.

[107] D. K. Sharma, S. K. Dhurandher, M. S. Obaidat, A. Bansal, and A. Gupta, "Genetic algorithm and probability based routing protocol for opportunistic networks," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Dalian, China, Jul. 2017, pp. 58–62.

[108] S. J. Borah, S. K. Dhurandher, S. Tibarewala, I. Woungang, and M. S. Obaidat, "Energy-efficient Prophet-PRoWait-EDR protocols for opportunistic networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–6.

[109] D. K. Sharma, A. Sharma, and J. Kumar, "KNNR: K-nearest neighbour classification based routing protocol for opportunistic networks," in *Proc. 10th Int. Conf. Contemp. Comput. (IC)*, Noida, India, Aug. 2017, pp. 1–6.

[110] L. Chancay-Garcia, J. Herrera-Tapia, P. Manzoni, E. Hernandez-Orallo, C. T. Calafate, and J.-C. Cano, ''Evaluation of routing protocols for opportunistic networks in scenarios with high degree of people renewal,'' in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Krakow, Poland, May 2018, pp. 228–235.

[111] M. Gupta, S. K. Dhurandher, and P. Nicopolitidis, ''A novel and efficient geocasting in OppNets,'' in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Colmar, France, Jul. 2018, pp. 1–5.

[112] V. Kuppusamy, ''Performance analysis of epidemic routing in destinationless OppNets,'' in *Proc. IEEE 19th Int. Symp. World Wireless, Mobile Multimedia Networks (WoWMoM)*, Chania, Greece, Jun. 2018, pp. 1–3.

[113] D. K. Sharma, G. Sohi, H. Dhankhar, and M. Yadav, ''Direct perceptive routing protocol for opportunistic networks,'' in *Proc. 11th Int. Conf. Contemp. Comput. (IC)*, Noida, India, Aug. 2018, pp. 1–6.

[114] S. Sati, A. Sohoub, A. Eltahar, K. A. B. Ahmad, K. Ahmad, and A. Bakeer, ''Degree contact DC-epidemic routing protocol for opportunistic networks,'' in *Proc. Adv. Wireless Opt. Commun. (RTUWO)*, Riga, Latvia, Nov. 2018, pp. 198–203.

[115] S. Zhang, D. Huang, and Y. Li, ''Prediction-based routing methods in opportunistic networks,'' *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 10, pp. 3851–3866, 2016.

[116] S. Liu, X. Wang, L. Zhang, P. Li, Y. Lin, and Y. Yang, ''A social motivation-aware mobility model for mobile opportunistic networks,'' *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 8, pp. 4662–4677, 2016.

[117] F. Zhang, X. Wang, L. Zhang, P. Li, L. Wang, and W. Yu, ''Dynamic adjustment strategy of n-epidemic routing protocol for opportunistic networks: A learning automata approach,'' *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 4, pp. 2020–2037, 2017.

[118] H. Ma, H. Wu, G. Zheng, B. Ji, and J. Li, ''FARS: A fairness-aware routing strategy for mobile opportunistic networks,'' *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 5, pp. 368–370, May 2018.

[119] S. Chen, W. Zou, X. Liu, Y. Zhao, and Z. Zhou, ''Reduction of the retransmission delay for heterogeneous devices in dynamic opportunistic device-to-device network,'' *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 10, p. 13, Oct. 2018.

[120] M. Erdogan, K. Gunel, T. Koc, H. U. Sokun, and T. Dag, ''Routing with (p-percent) partial flooding for opportunistic networks,'' in *Proc. Future Netw. Mobile Summit*, Florence, Italy, Jun. 2010, pp. 1–6.

[121] L. Liu, ''P3: Physical proximity prediction routing protocol in socially-aware opportunistic networks,'' in *Proc. 2nd Int. Symp. Instrum. Meas., Sensor Netw. Autom. (IMSNA)*, Toronto, ON, Canada, Dec. 2013, pp. 368–370.

[122] X.-H. Wu, X.-F. Gu, and S. Poslad, ''Routing algorithm based on social relations in opportunistic networks,'' in *Proc. 12th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Chengdu, China, Dec. 2015, pp. 146–149.

[123] Y. Xie, J. Bao, Z. Song, and Y. Zhou, ''A hybrid opportunistic routing scheme based on nodes grouping strategy for VANETs in urban scenarios,'' in *Proc. 25th Wireless Opt. Commun. Conf. (WOCC)*, Chengdu, China, May 2016, pp. 1–5.

[124] G. Xu, Z. Xu, Y. He, J. Zhou, Y. Guo, and X. Guo, ''Opportunistic networks routing algorithm based on the uncertain social relationship,'' in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, Nanjing, China, May 2018, pp. 301–306.

[125] W. Chen, Z. Chen, W. Li, and F. Zeng, ''An enhanced community-based routing with ferry in opportunistic networks,'' in *Proc. Int. Conf. Identificat., Inf. Knowl. Internet Things (IIKI)*, Beijing, China, Oct. 2016, pp. 340–344.

[126] X. Wang, X. Sun, W. Pan, T. Xu, and X. Li, ''SRR: A lightweight routing protocol for opportunistic networks,'' in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Chengdu, China, Oct. 2017, pp. 588–592.

[127] L.-J. Chen, C.-H. Yu, T. Sun, Y.-C. Chen, and H.-H. Chu, ''A hybrid routing approach for opportunistic networks,'' in *Proc. SIGCOMM Workshop Challenged Netw. (CHANTS)*, Pisa, Italy, Sep. 2006, pp. 213–220.

[128] M. Chen and H. Wang, ''A multi-objective routing decision-making model for opportunistic network,'' in *Proc. IEEE Int. Conf. Cloud Comput. Intell. Syst.*, Beijing, China, Sep. 2011, pp. 316–320.

[129] D. Soares, E. Mota, C. Souza, P. Manzoni, J. C. Cano, and C. Calafate, ''A statistical learning reputation system for opportunistic networks,'' in *Proc. IFIP Wireless Days (WD)*, Rio de Janeiro, Brazil, Nov. 2014, pp. 1–6.

[130] S. Chupisanyarote, S. Kouyoumdjieva, O. Helgason, and G. Karlsson, ''Caching in opportunistic networks with churn,'' in *Proc. 9th Annu. Conf. Wireless Demand Netw. Syst. Services (WONS)*, Courmayeur, Italy, Jan. 2012, pp. 39–42.

[131] J. Wu, Z. Chen, and M. Zhao, ''Effective information transmission based on socialization nodes in opportunistic networks,'' *Comput. Netw.*, vol. 129, pp. 297–305, Dec. 2017.

[132] A. Kumar, S. K. Dhurandher, I. Woungang, M. S. Obaidat, S. Gupta, and J. J. P. C. Rodrigues, ''An altruism-based trust-dependent message forwarding protocol for opportunistic networks,'' *Int. J. Commun. Syst.*, vol. 30, no. 10, p. 3232, 2017.

[133] S. K. Dhurandher, J. Singh, I. Woungang, R. Kumar, and G. Gupta, ''Message trust-based secure multipath routing protocol for opportunistic networks,'' *Int. J. Commun. Syst.*, vol. 33, no. 8, p. 4364, 2020.

COSSI BLAISE AVOUSSOUKPO received the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), China, in 2019. He is currently working as an Assistant Professor with Yibin University. His research interests include cryptography and information security, opportunistic networks, machine learning, and quantum computing. He is a member of the International Association for Cryptologic Research (IACR).

TAIWO BLESSING OGUNSEYI (Member, IEEE) received the Ph.D. degree from the Communication University of China, Beijing. He is currently working as an Assistant Professor with Yibin University. His research interests include applied cryptography, privacy-enhancing a technologies, and machine learning. He is a member of IEEE.

MARIUS TCHENAGNON received the M.Sc. degree in computer science from the University of Electronic Science and Technology of China (UESTC). He is currently working as a Security Consultant with Top Mega Prestations. His research interests include wireless communication, opportunistic communication, cryptography, and information security.