Wireless Personal Communications (2024) 135:2039–2059
https://doi.org/10.1007/s11277-024-11064-9

Speculative Analysis of Wireless Network by Bibliometrics Tool

Renu Dalal[1] · **Manju Khari**[2] · **Sanjay Misra**[3,4]

Accepted: 4 April 2024 / Published online: 6 May 2024

Abstract
An emerging subclass of the wireless network is known as a Delay Tolerant Network (DTN), in this network whenever the contact opportunity occurs sender nodes select the relay node randomly and disseminate the message in the network. The basic properties of DTN include; no fixed source-to-destination route, longer delay between nodes, and frequent disconnection among nodes. DTN is also known as Opportunistic Networks (OppNets). Routing protocols for traditional ad-hoc networks can't work in DTN, because conventional networks require continuous end-to-end routes among sender and receiver nodes for the complete duration of message communication. So, OppNets used the principle of store-carry-forward to provide routing in the wireless network. This article provides a Bibliometrics evaluation of wireless networks for articles, sources, keywords, and others. The complete basics of the wireless network along with their classification, characteristics, routing protocols, strengths, weaknesses, and applications. This is analysed that only 14% of VANET-based protocols, 25% of MANET-based, 25% WSN-based, and 36% of OppNet-based protocols are already introduced in the wireless network.

Keywords Delay tolerant networks · Opportunistic networks · Routing protocols · Wireless networks

✉ Sanjay Misra
sanjay.misra@hiof.no

Renu Dalal
dalalrenu1987@gmail.com

Manju Khari
manjukhari@yahoo.co.in

[1] University School of Automation and Robotics, GGSIP University, East Delhi Campus, New Delhi, India

[2] School of Computer and Systems Science, Jawaharlal Nehru University, Delhi, India

[3] Department of Computer Science and Communication, Østfold University College, Halden, Norway

[4] Department of Applied Data Science, Institute for Energy Technology (IFE), Halden, Norway

1 Introduction

Due to the procreation of information technology, today's world is working in advanced networks, which include huge numbers of handheld gadgets with the ability to message broadcasting and data sharing in infrastructure-less mode. Tablets, mobiles, PDAs, smartphones, etc. are a few collections of handheld gadgets. Mobile Ad-hoc Networks (MANETs) are wireless networks, which include mobile nodes and work on a random topology [1–3]. The performance of MANET networks is directly proportional to the parameters like; linked among communicating nodes, message dropping, the routing protocol used during broadcasting the message, the traffic pattern of communication, etc. [4–5]. The few applications of MANETs are operations of military tactical, Androset, BOTNETs [6–7], search & rescue, disaster relief and for commercial use. After the advancement of the wireless network new network named the Opportunistic network was introduced by Kevin Fall in 2002 [8].

The OppNets works with the longer transmission delay among nodes with short-range communication areas according to the geographical proximity of mobile gadgets. For the dissemination of messages in OppNets, Bluetooth or Wi-Fi techniques are utilised. DTN/OppNet. network forwards the messages in a wireless network by using a Bundle Layer (BL). The sequence of adjacent data blocks is known as a bundle, it keeps the semantic information which permits the application to make progress in the network. These bundles are broadcast opportunistically in a store-carry-forward mechanism, whenever the opportunistic nodes come to their communicating range [9].

Many routing protocols were already introduced in OppNet. A description of a few protocols for an opportunistic network is Direct delivery: This protocol doesn't create many copies of messages. Only the sender node directly transmits the packet to the receiver node. If the receiver node doesn't receive the packet or if the sender node is not successful in sending the packet, either message will be discarded or destroyed, so in terms of delivery of the message this protocol is not reliable and efficient.

Epidemic Protocol: To save, the initial (original) message and the message for another node (work as a secondary buffer), two buffers are used by an epidemic routing protocol. For buffer management First-In-First-Out (FIFO) policy is applied. The first packet from the buffer is eliminated, whenever the buffer reaches its maximum capacity. By hop-count weightage and special 32-bit ID (identification number), messages in the buffer are categorized.

Spray and Wait Protocol: Transmission of replication of message packets is few as compared to epidemic protocol. Less delivery delay, negligible congestion and maximum scalability are provided by Spray and Wait for protocol. Cluster protocol: To update the online probability of contact is done by the EWMA (exponentially weighted movement average) scheme. Information transmission and routing in a network is done by gateways and clusters, which are selected by functions like join (), sync (), and leave () etc. Multiple very small size of clusters is formed, to avoid undefined errors. The objectives of this paper are as follows:

(a) To provide the background of wireless networks; the taxonomy of wireless networks is discussed.

(b) Bibliometrics assessment concerning wireless networks is encountered to give the information of highly contributed countries & authors, frequently used resources & keywords, and most cited authors.
(c) Characteristics, strengths, weaknesses, and applications of a different wireless network are included in the article, which provides immense knowledge about various wireless networks to beginners.

This article is structured as; Taxonomy with the classification of wireless networks is presented in Sect. 2. The Bibliometrics assessment for wireless networks and their important outcomes is addressed in Sect. 3. Section 4, presents the properties, strengths, weaknesses, and applications of diverse networks. Section 5 presents the analysis of routing protocols which are used in different wireless networks. Finally, the conclusion of the paper is shown in Sect. 6.

2 Taxonomy of Wireless Network

This section describes the diversity of wireless networks. Wireless networks are categorized into single-hop and multi-hop-based networks with sub-diversion in infrastructure-based and infrastructure-less based as presented in Fig. 1. In single-hop communication in a network, the transmitted node directly sends the message to the receiver node without using a relay node or intermediate node. However, due to the larger communication area in a network, the sender node uses multi-hop communication, here relay node is used by the sender node to transmit the packet to the receiver node. The way through which, the network uses resources like; internet connectivity, operation of communication, required service in the network, access points, base stations, etc. is known as an infrastructure-based network. When the nodes in the network work.

as a router and communicate without using any pre-defined infrastructure is known as an infrastructure-less network.

Wireless Local Area Networks (WLAN-802.11), Cellular Networks, and Wireless Metropolitan Area Networks (802.16) are examples of wireless network which exists in the category of a single-hop infrastructure-based wireless network. Bluetooth, Wi-Fi, WLAN-802.11, and Opportunistic networks lie in the class of single-hop infrastructure-less-based wireless networks. Contrasting classes of routing in OppNets are also shown in Fig. 1.

Wireless Sensor Network (WSN) is a multi-hop infrastructure-based wireless network. Here each sensor node, either keeps a radio trans-receiver with an in-built antenna or has a link to a microcontroller. WSN can work with both simple star topology and complicated multi-hop wireless mesh topology. Various categories of WSN routing techniques are shown in Fig. 1. Mobile Ad-hoc Networks (MANETs) and Vehicular Ad-hoc Networks (VANET) are examples of infrastructure-less based multi-hop wireless networks [10]. Existing routing protocols for MANET and VANET are also presented in Fig. 1.

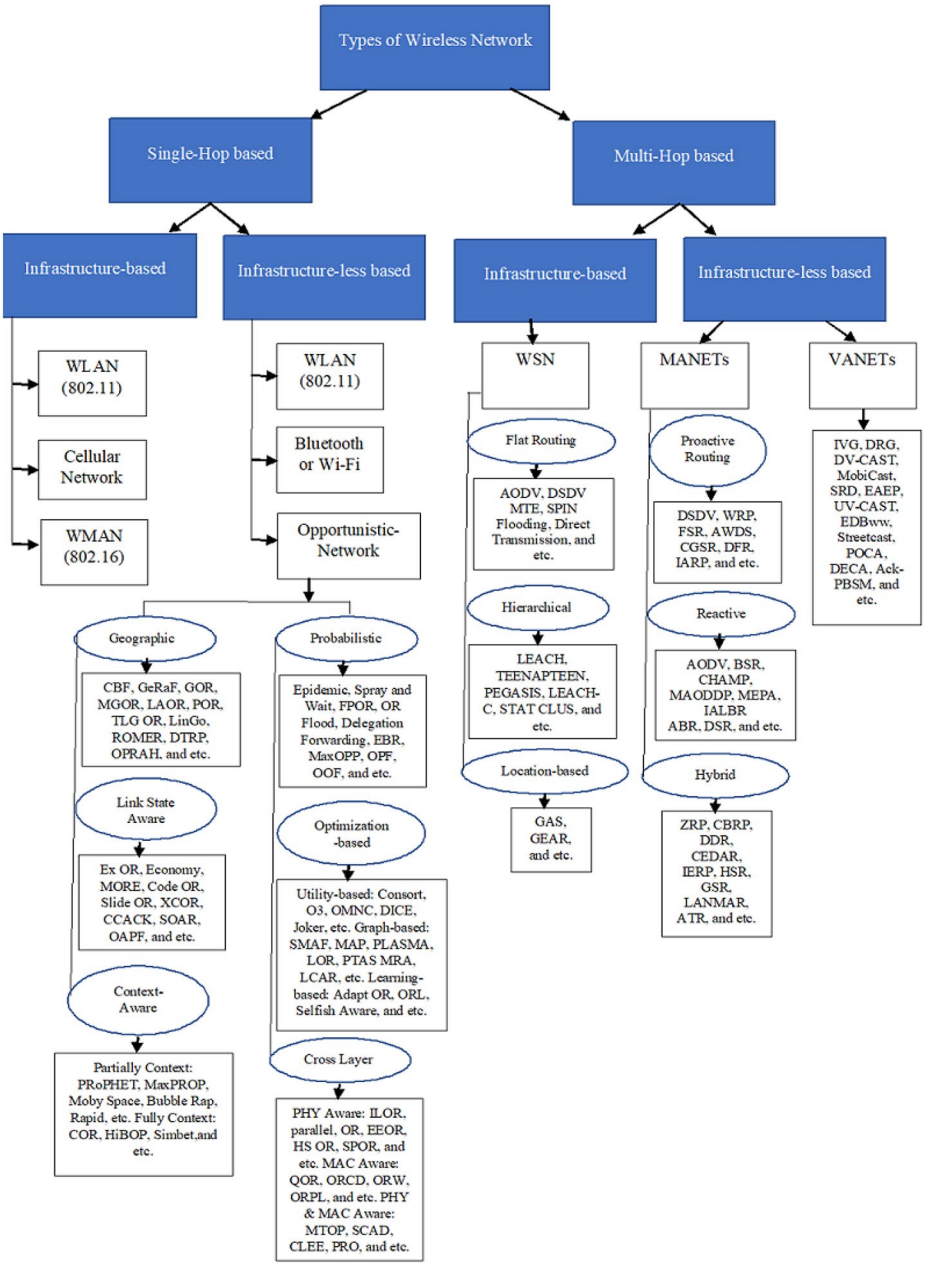

Fig. 1 Taxonomy of wireless network

3 Bibliometrics Analysis

Science mapping technique and performance analysis are integrated by the bibliometrics tool. Articles citation, network visualization, bibliographic coupling, co-occurrence of keywords, and co-occurrence of author citation network analysis are done by using the science mapping tool VOS viewer [11–12]. Diverse information like; sources from books & journals, no. of documents included, the average year of publication, average citation of the article, references, keywords, single-author papers, multi-author papers, and other information are included for wireless network bibliometrics analysis. The effective outcome of these 19 factors is presented in Table 1. This section is integrated with three subsections 3.1, 3.2, and 3.3.

3.1 Article and Countries Bibliometrics Analysis

In this subsection "Article publication concerning years" from 1996 to 2022 and "Country citation of papers & average country citation of papers" are discussed. The Bibliometrics tool [11] and VOS viewer mapping tool are used to find all relevant data. The number of articles published from 1996 to 2022 in the domain of wireless networks is depicted in Fig. 2. A total of 1030 research articles were published, but 147 is the maximum number of articles published in 2015. The least number of papers 11 exist in the year 2004. From 2009 to 2015 approximately 71% of articles were published more as compared to 1996 to 2005.

Table 1 Main information for bibliometrics

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	1996:2022
Sources (Journals, Books, etc.)	2
Documents	2000
Average years from publication	8.06
Average citations per document	20.85
Average citations per year per doc	2.092
References	61,727
DOCUMENT TYPES	
article	2000
DOCUMENT CONTENTS	
Keywords Plus (ID)	9530
Author's Keywords (DE)	4914
AUTHORS	
Authors	4403
Author Appearances	6427
Authors of single-authored documents	100
Authors of multi-authored documents	4303
AUTHORS COLLABORATION	
Single-authored documents	112
Documents per Author	0.454
Authors per Document	2.2
Co-Authors per Documents	3.21
Collaboration Index	2.28

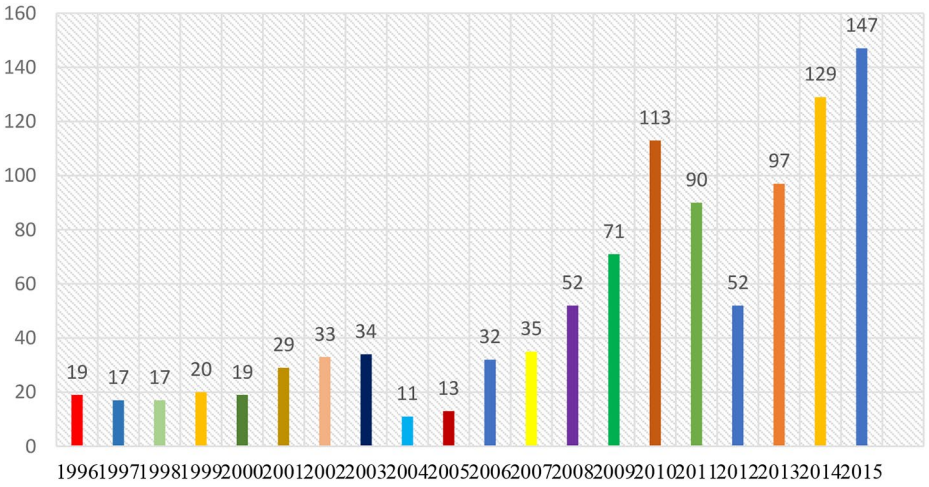

Fig. 2 Year-wise Number of Articles Published

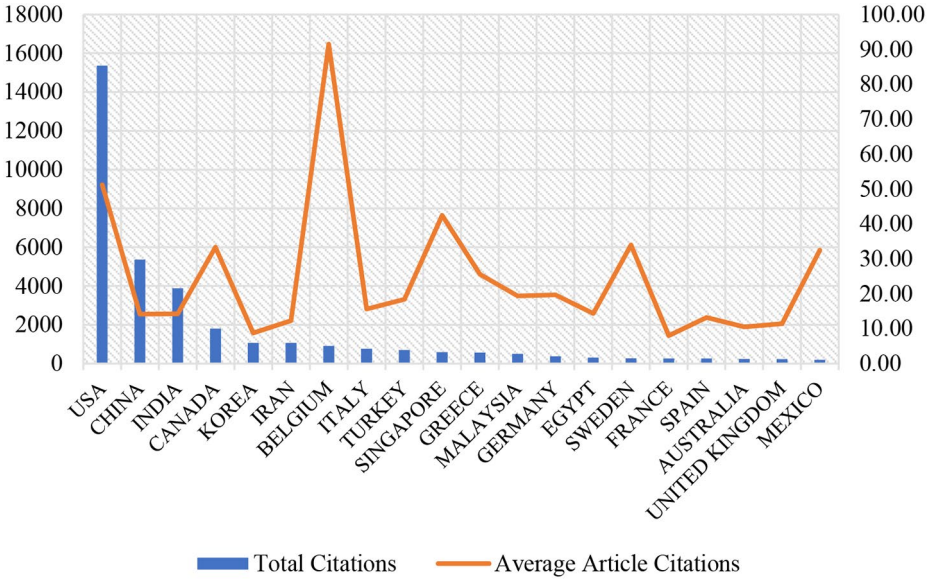

Fig. 3 Article citations & average article citation vs. country

Productions of articles by diverse countries like; the USA, CHINA, INDIA, and others are included by the tool. The citation of the research paper produced by the country and the average citation of the article concerning the country is presented in Fig. 3. The USA is found as the top country which receives the maximum number of article citations (15,362) and Mexico is considered as a bottom country in terms of article citations (195). China is second (5357) and India is third (3887) in the top most countries in terms of article citations. India received 76% and 80% more citations as compared to Belgium and Italy respectively.

65% and 74% more citations are received by the USA as compared to China and India respectively.

According to the average article citation concerning the country, Belgium is the top country (91.50) and France (8) is at the bottom. Belgium scored 89%, and 84% more average article citations as compared to Australia and India respectively. India received a 43% higher average article citation as compared to Korea. The USA received 76% and 64% more average article citations as compared to Iran and Turkey. The details of another country for the factor total citation and average total citation are presented in Fig. 3.

3.2 Citation Analysis of Author Keywords and Researchers

This sub-section discussed the author keyword citation and author citation network visualization. The graphical representation using the science mapping tool VOS viewer [11] is shown in Figs. 4 and 5.

During the bibliometrics analysis of wireless networks; approximately 9530 keywords were found but only, 4914 (40%) keywords were used by the researchers. Wireless Sensor Network, Routing, Quality of Services, Clustering, Load Balancing, and many other keywords are included by the tool; their co-occurrence of author keywords is shown in Fig. 4.

2000 research articles were encountered from 1996 to 2022. 4402 authors were included, out of which only 3% of authors are evaluated as single-author articles and 97% of articles are analysed as multi-authored. Figure 5 presents the visualization citation network for authors; colourful nodes are used to present different authors. According to the number of citations of a particular author; their node-size is varied. The large size of the author-node indicates, more citations of the author received and vice versa. The edges between colourful nodes show the collaborative work of the researchers; a greater number of edges shows a higher number of together articles.

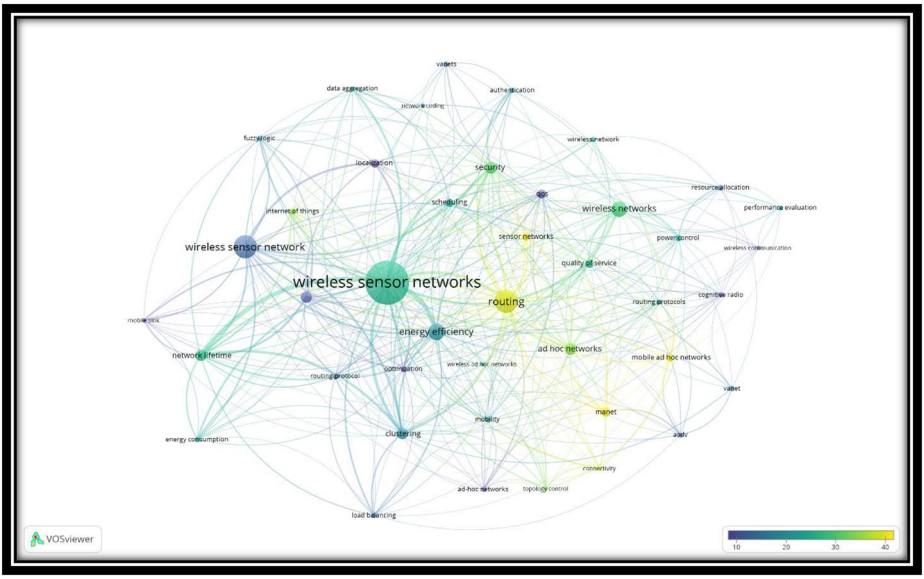

Fig. 4 Co-occurrence of author keyword citation

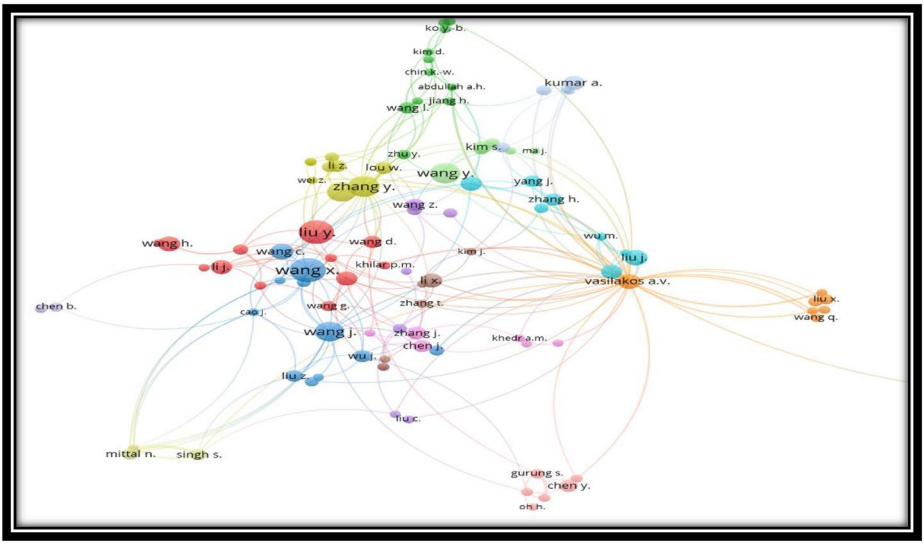

Fig. 5 Author's citation network visualization

3.3 Citation Analysis of Sources, Word Growth, and 3-D Plot

Article resources are the primary important input for bibliometrics analysis; the top 20 journals were encountered for wireless networks. Wireless networks, Transactions on Vehicular Networks, IEEE Communication Letters, IEEE Transactions on Networks, and other sources were found with their number of articles published as shown in Fig. 6. A total of 14,202 articles were published by these sources during 1992–2022.

Of the minimum number of articles (359), only 3% were produced by the "IEEE Communication Letters". Wireless networks journal is evaluated as the top source to provide the number of articles (1399). "Transactions on Vehicular Networks" is the second journal which published 91% of the articles; it generates 13% fewer articles as compared to the "Wireless Networks" journal. "IEEE Transactions on Networks", published 31.4%, and 67% more articles as compared to "Computer Networks", and "IEEE Communication Letters" journals respectively.

From the bibliometrics analysis; word growth from the various articles was evaluated (1996–2022) and graphically presented in Fig. 7. Different keywords like; ad-hoc networks, energy efficiency, algorithms, sensor nodes, routing protocols, and others were analysed by using various colour waves. "Algorithm" word was evaluated as highly cumulate occurrences from 1996 to 2017 as compared to other keywords. "Wireless networks", and "wireless sensor networks" found more word growth as compared to "algorithm" from 2018 to the present. "Energy efficiency", and "Energy utilization" were considered as the least cumulate occurrences from 1996 to 2022.

The three-field plot for the factor's authors, keywords, and effective sources from 1996 to 2022 is graphically represented in Fig. 8. Author, Keywords, and Source words are abbreviated as AU, DE, and SO respectively which are used in Fig. 8. Diverse authors (AU) like Kumar A, Wang D, Liu Y, Fang Y, and others are plotted first with different keywords (DE)

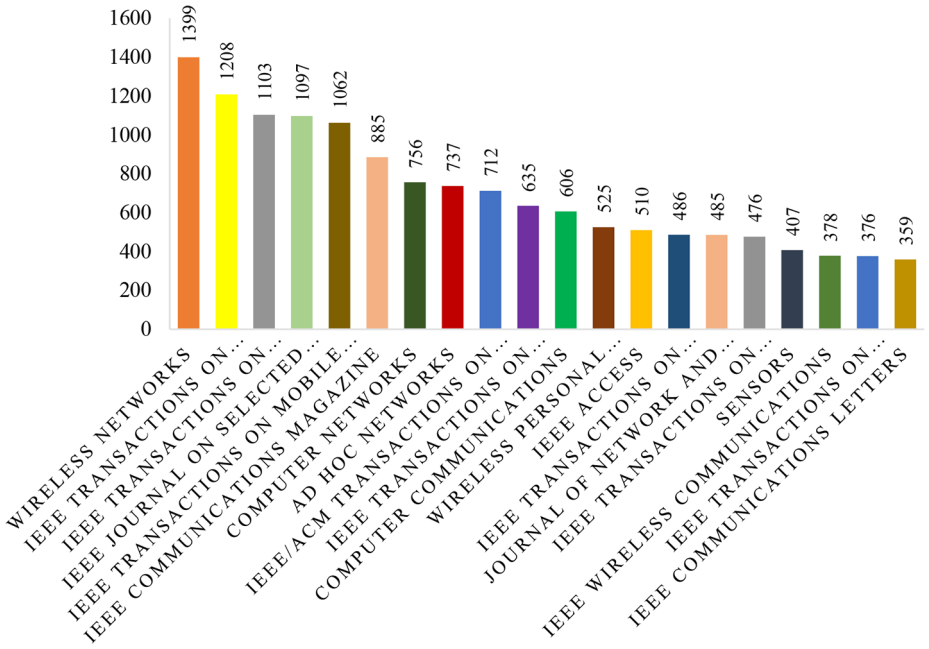

Fig. 6 Most cited sources

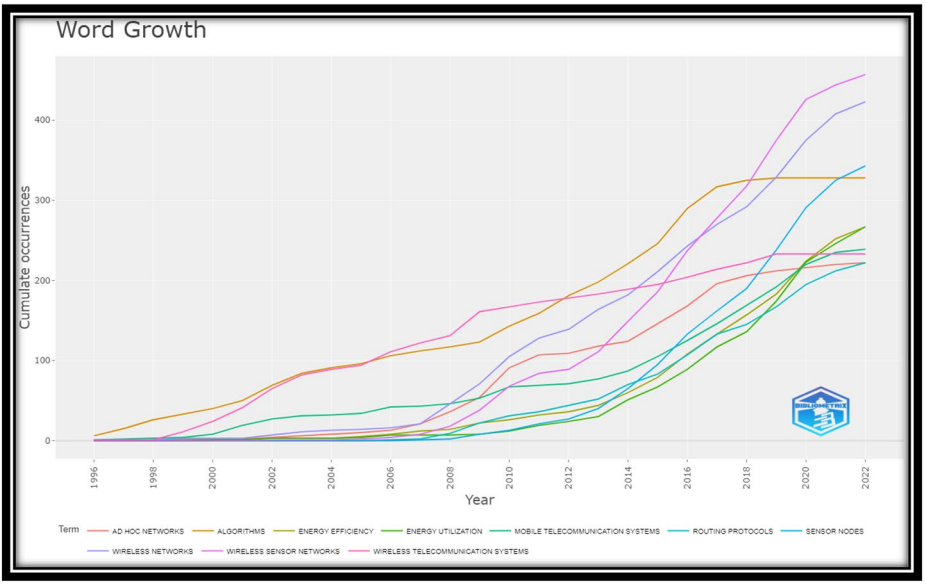

Fig. 7 Word growth used in wireless network

used by researchers. More number of edges between AU and DE indicates a greater frequency of keywords used by authors. Different DE which used in various sources (SO) like wireless networks, ad-hoc and wireless sensor networks, and others are shown by waves in Fig. 8.

4 Wireless Networks

In this section, diverse types of wireless networks like MANET, VANET, WSN, and OppNet are discussed with their important findings and outcomes. Significant features, strengths, weaknesses, and applications of these networks are summarized in Tables 2, 3, 4 and 5.

4.1 Mobile Ad-hoc Network (MANET)

Dynamic, self-organising, infrastructure-less, multi-hop based, and self-managing mobility nodes in the wireless network are known as MANET. In this, mobile gadgets can change their location from one place to another at any time. This network provides communication directly among nodes according to their transmission range. Mobile nodes in MANET are linked wirelessly [1–2, 5]. For the successful dissemination of messages in the network, relay nodes must cooperate [13–14].

4.2 Vehicular Ad-hoc Network (VANET)

The concept of setting up the topology of vehicles for the same type of application and situation of use is known as VANET [15–16]. This is a highly efficient and reliable network, which is used to interlink vehicles in the environment like urban cities or highways. Base stations are used in VANET, for dissemination of the information in the network, where vehicles are used as independent nodes [17].

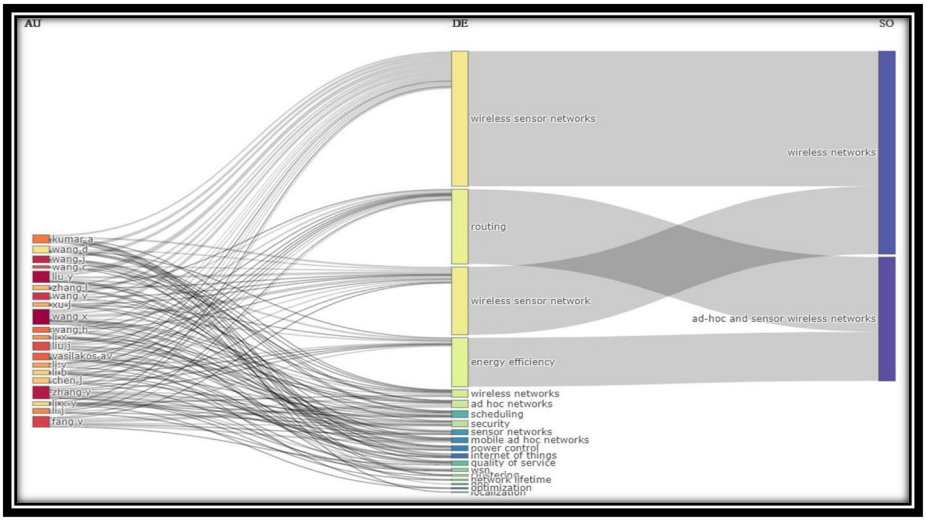

Fig. 8 Three field plot author, keywords and sources

Table 2 Details of MANET's

S. No	Features	Strength	Weakness	Applications
1	Bounded Security: Security services, routing procedures, and host configuration process are done in a distributed manner, due to not having a centralized firewall.	Each node is working as a router and doesn't follow any kind of centralized administration	Not able to provide high security and reliability during communication in the network. Data broadcast errors, hidden terminal problems, mobility-induced packet losses, etc., problems are introduced due to the broadcast feature of this network	At Local-level: By using mobile phones, laptops, palmtop computers, and- etc.; Instant ad-hoc networks can be formed by autonomous links and information can be shared and broadcast.
2	Negligible Human Interruption: This network permits minimum human intervention for network configuration because of the dynamic autonomous nature of MANET.	This network is robust and flexible. The router-free operation, high speed, fault tolerance, fast installation, and low cost.	Due to random changes in the topology of a network; the MANET network can't provide the high Quality of Service (QoS).	Military Battlefield: This network can work efficiently in ad-hoc networks with soldiers, headquarters of military information, and vehicles. The military tool can keep computer equipment so that ad-hoc networks can form.
3	Autonomous Nature of Node: Every node in MANET can work as a host or router in the ad-hoc network.	This network can form as a fly, i.e., because of the mobility of nodes, nodes can move at any time and any place.	Managing the power resources during communication in an ad-hoc network is also a complex task.	In Commercial Area: For relief in a disaster area like flood, earthquake, or fire, where rescue and emergency operations are a priority task. Where infrastructure-based communication is damaged, an ad-hoc network can work reliably.
4	Flexible Topology: The network topology may change frequently and at random periods because of the movability nature of mobile nodes with unidirectional or multidirectional connections.	It can provide communication in a wider area and with dense mobile nodes.	Communication between ad-hoc networks and fixed networks like IP-based is such difficult work.	In homes, classrooms, conferences, virtual meets, etc.; this network is applicable [1–3, 5].
5	Operation with limited energy: In MANET; Few or all mobile nodes are depending either on the batteries or other exhaustible sources for their energy.	Without considering the geographical location of nodes, MANET permits the authority to share information and services in the network.	This network is capable of transmitting a packet with multi-hops; therefore, routing becomes complex from a sender node to a receiver node [13–14].	-------

Table 3 Details of VANET's

S. No	Features	Strength	Weakness	Applications
1	Negligible Consumption of Energy: This network utilises very little energy when providing services in a network.	Vehicle nodes may change their location with high relative velocity so that communication among nodes in a very short period.	Identification of suspicious vehicle nodes in VANET is not a simple task.	Enhancement of Vision: This network can provide information to the drivers, about obstacles in the path and bad weather.
2	Security: It is the most secure network, due to nodes in this network are physically more secure than other wireless networks. It also minimizes the risk of infrastructure attacks.	Mixed vehicles nodes, specialized vehicles nodes, and fixed deployed vehicles nodes can work together in VANET.	A high level of vehicle movability gives frequent changes in network topology, therefore, maintaining reliable and good QoS is such complicated work.	Broadcasting of Warning Message: Prior warning messages can be forwarded to the vehicle's node about any danger ahead in the route. So, they can change their route.
3	Limitless Size Network: This network is highly scalable; therefore, it can connect one city to many cities or also link one country to more countries.	This network supports multi-hop communication in a wireless network like MANET.	Frequent changes in the velocity and density of vehicle nodes make communication difficult in VANET.	Message Transfer Operation: Slow-moving and stand-by vehicles can exchange or forward messages with the cooperation of nodes in a network.
4	Variable Topology: Because of the high movability of vehicle nodes in the environment, VANET's topology changes very frequently. Whenever the speed of vehicle nodes increases their communication time decreases.	VANET eliminates the constraint of processing power, low battery, and bounded storage capability of nodes, which are applicable in MANET.	In a Cluster network, choosing a cluster head (CH) is a challenging task.	Real-time Traffic: The Roadside Unit (RSU) is used as a data storage unit in VANET so that data can be used whenever required [15–16].
5	Defined Pattern of Mobility: The special feature of VANET is, the availability of pre-existing paths for vehicle nodes. Therefore, the movability pattern in the environment can easily be forecasted by the network designer.	This network works efficiently in both safety (including navigation, speed limit, collision alert, pedestrian crossing, lane changing, and work zone) and non-safety applications (road congestion, weather information, route navigation, dangers on the road, chatting, gas station, file sharing).	A minimum level of distribution of vehicle nodes in a particular location leads to a low level of communication among nodes in VANET [17].	-----

4.3 Wireless Sensor Network (WSN)

The collection of hundreds or thousands of sensor nodes is known as Wireless Sensor Network. Radio, power, processing, and sensing units are the primary parts of each

Table 4 Details of WSN's

S. No	Features	Strength	Weakness	Applications
1	It works on two kinds of structure layered network architecture and clustered structure. In the network, structures are the integration of five layers (application, transport, network, data link, and physical) and three cross-layers (power, mobility, and task management plane).	This network can work reliably without infrastructure.	At regular periods sensor nodes are required to charge because of their low battery life.	Traffic Monitoring: To detect a congested area in a city or town for the smooth functioning of vehicles on the road sensor nodes are utilised. Google Maps provides services to people to reach their destination within a minimum time and distance.
2	This network works with the topology named, star, mesh, and hybrid star.	Centralized monitoring may be used, if necessary, in a network.	Compared to the wired communication network, WSNs communicate at a low speed.	Weather Forecasting and Analysis: Diverse factors are sensed by the sensor node, in the environment such as the velocity of air, pressure, moisture in soil/air, forecasting of rainfall, and weather.
3	The sensor node can work with bounded exhaustible power resources like batteries.	WSN is easily applicable in non-reachable locations like mountains, deep forests, rural places, overseas, etc.	Security is a major concern during communication in a wireless network, but WSN is highly vulnerable to attack.	WSN in Healthcare: To monitor the internal changes in a human being; sensor nodes are used in healthcare. Due to its simple use, low cost, small size, and patient mobility; the heartbeat sensor node is applicable.
4	Nodes in WSN are highly movable and heterogeneous.	Any gadget such as a sensor node can join and leave the network at any place and at any time.	Produces resistance error, and long response time in commercial applications in the house.	WSN as IoT: Sensor nodes can be used as in-built in the things which can communicate through the internet.
5	WSN is highly scalable and able to handle node failure. Efficiently applicable to environmental constraints.	Low cost of installation due to no use of wiring.	Position sensors which are used in gaming applications are easily affected by the change in atmosphere, not very accurate in dark locations, and bounded working areas.	Detection and tracking of Suspicious nodes: In a military battlefield, sensor nodes are used to identify, track, and classify the suspicious or intrusion activity done by either vehicles or persons [18].

sensor node. This network works efficiently in a smaller area. Atmosphere pressure, temperature, humidity, etc. parameters are sensed by the sensor node. This information is disseminated to the destination node or sink node in WSN [18].

Table 5 Details of OppNet

S. No	Features	Strength	Weakness	Applications
1	Fixed and Dynamic Nodes: In this network, nodes are either mobile or fixed. Kind of opportunistic nodes are applicable in this network.	Delay Tolerance: This wireless network works on the principle of a store-carry-forward approach. So, the broadcast of a message directly depends on the node contact opportunity.	Congestion in the Network: Due to the non-existence of an end-to-end route in OppNet, it is difficult to identify and control the congestion by using a feedback loop.	Wildlife Preserving: For the preservation of animals and birds in the forest or wildlife; OppNet contacts can be utilised to count them. The animal/bird is assumed to be dead when that animal/bird is not in contact with other animals/birds for many days.
2	Recurrent Connectivity: Due to no end-to-end route existing from the source node to the destination node, there is an intermittent link in the routing of OppNet.	Low Cost & Infrastructures: The set-up and installation costs are not high. Due to the self-organised nature of this network, doesn't require any kind of infrastructure. OppNet can work with a single-hop wireless connection.	Delay of Message Transfer: This network works on high delay tolerance; this causes high transfer time from a source node to a receiver node.	Forecasting and Communication in Disaster areas: The areas that are badly affected by a man-made or natural disaster like an earthquake, flood, etc. OppNet can work efficiently and reliably.
3	Occasional node contact: There is no fixed interval of contact among nodes, therefore Opportunistic network is based on the principle of occasional contacts among nodes.	Data forwarding and data flooding are two types of message broadcast methods in OppNet. Data forwarding method, the source node first chooses the intermediate node to transfer the message by using some rules. However, in data flooding, the source node disseminates the packet directly and produces many duplicate copies of the message.	Ordering of Message Transfer: Nodes' contact time is unpredictable because of nodes' movability in the wireless network. Therefore, it is complex to manage the sequence of message packets during communication in a network.	Communication in Terrains like Mountain or Deserts: OppNet can be used to provide communication services to the area, where wired or wireless networks are not applicable. DTN can be easily established in terrain areas like the Himalayas, Thar desert in Rajasthan, etc.
4	Limited Energy Resources: All the opportunistic nodes in OppNet work with the constraint of bounded power resources. For predicting natural disasters like cyclones, an underwater oceanic network is used. This network helps to find the current and speed of water in the ocean.	Applicability: This network is applicable in various applications like; opportunistic computing, pervasive and urban sensing, mobile social networking, IoT, and many more areas [19].	Vulnerability of Attack: Because of the wireless characteristics of OppNet; this network is highly prone to malicious activity, and active or passive attacks during communication [20–9].	Security of Biosphere: Plants and trees in the forest can be protected by using an opportunistic network. Therefore, it helps to preserve the biosphere.

Table 5 (continued)

S. No	Features	Strength	Weakness	Applications
5	Store-Carry-Forward: This is the primary principle for OppNet, nodes in this network are associated with a bundle layer and due to intermittent connectivity among nodes, each node carries the message in their buffer and forwards this message to the appropriate next reliable node.	----	----	Traffic Monitoring: Opportunistic nodes are used on traffic lights to sense the traffic on the road during peak hours. According to this information, a driver can choose their route [8–9].

4.4 Opportunistic Network (OppNet)

The improvement in MANET wireless network with tolerance in the delay is known as OppNet. Whenever the node gets the opportunity to disseminate the message in the network, the procedure of message transmission has occurred. This opportunity is depending on the working range of nodes in the network. By using the intermediate node or relay node in a network, the source node forwards the packet to the destination node successfully by using the store-carry-forward procedure during routing [8–9].

5 Analysis of Wireless Protocols

This section provides the empirical evaluation of diverse types of concepts used in wireless networks. This section is divided into two sections; it includes a theoretical analysis of wireless protocols.

5.1 Wireless Protocols Analysis

Figure 9 depicts the number of existing routing protocols of the MANET wireless network concerning different types of concepts used during the designing of that protocol. Key-based protocol was proposed in [1], symmetric key, asymmetric key, and group key-based are the primary categories of MANET protocol. Approx. 14 protocol was in the key management-based class. DKPS, PKIE, and INF protocols are in the subclass of symmetric key-based. SRP, URSA,

SOKM, Z&H, ID-C, etc. exist in the sub-category of the asymmetric-key-based protocol. SEGK was based on the category of group-key management scheme [21–22]. Around 20 routing protocols were introduced in the class of trust-based protocols in MANET. ABED, GRE, lies in the sub-category of protocol-based trust schemes of MANET. WATCHDOG, PATHRATER, CONFIDENT, CORE, etc. were proposed protocols in system-level-based trust protocol [23–24]. 24 routing protocols were lies in reactive, proactive, and hybrid-based. The three categories topology-based, key-based, and trust-based routing protocols are highlighted with green, blue, and orange colours respectively.

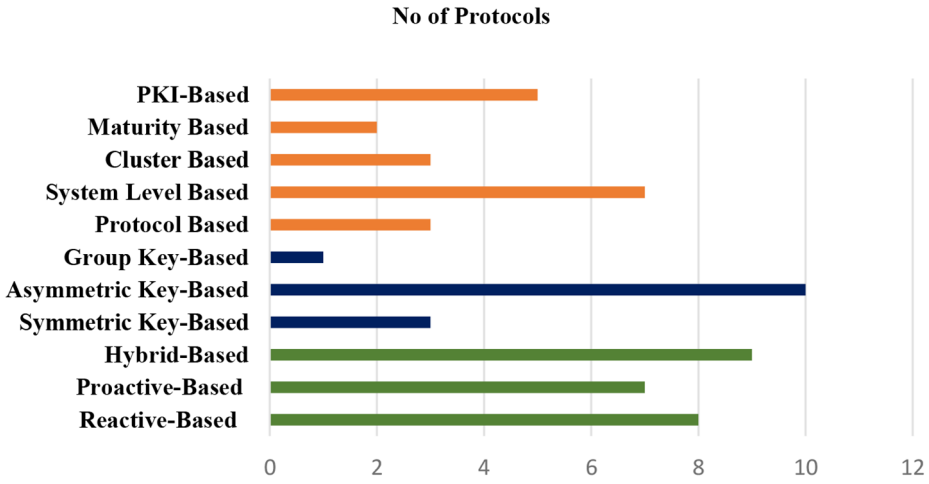

Fig. 9 Protocols of mobile Ad-hoc network

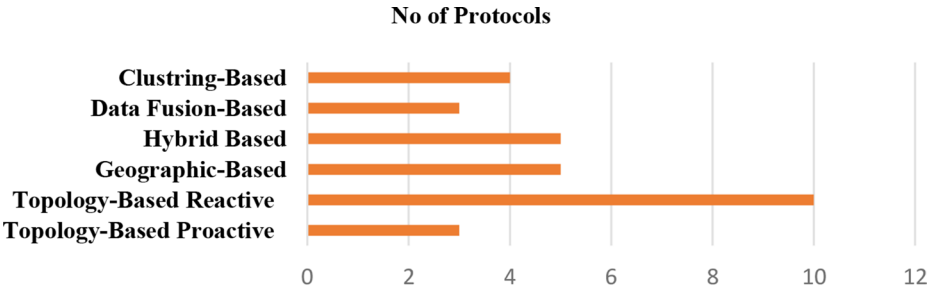

Fig. 10 Protocols of vehicular Ad-hoc network

Figs. 10 and 11 describe the number of protocols for VANET and WSN respectively. Approximately 40 routing protocols were proposed in the VANET. Diverse classes like topology-based reactive, proactive, hybrid, cluster, geographic, and data fusion-based concepts were introduced in this type of network. Sub-class proactive routing protocols in VANET include PBR, DSDV, and OLSR. AID, FLUTE, SADV, HFED, MDD, NDMR, PRAODV, etc., protocols exist in reactive routing protocols. A-STAR, GPCR, GYTAR, RIVER, and GeoSVR come in the category of geographic-based routing schemes in VANET. Integration of geographic and topology concepts produces hybrid routing protocols; a few examples are HLAR, LAGAD, ZRP, etc. The cluster-based category includes LORA_CBR, FTLocVSDP, C-VANET, LEAPER, etc. routing protocols. DDFP, FCMA, D-SEMA, etc., are examples of data fusion-based routing protocols in VANET [17].

Figure 11 presents various existing routing protocols in WSN. Security, flat, and location-based are different categories of protocols. SPINS, LKHW, LHA-SP, SERP, SMRP, BEARP, SR3, etc., are examples of security-based VANET protocols. Location-based WSNs include GAF, GEAR, TBFT, etc., and protocols lie in this category. QoS category includes SPEED, EAR, and SAR routing protocols. Approx. 60 routing protocols were included in WSN [25].

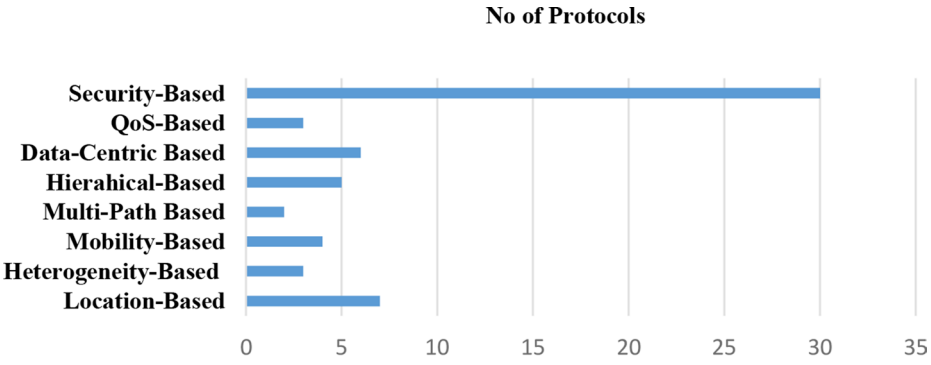

Fig. 11 Protocols of wireless sensor network

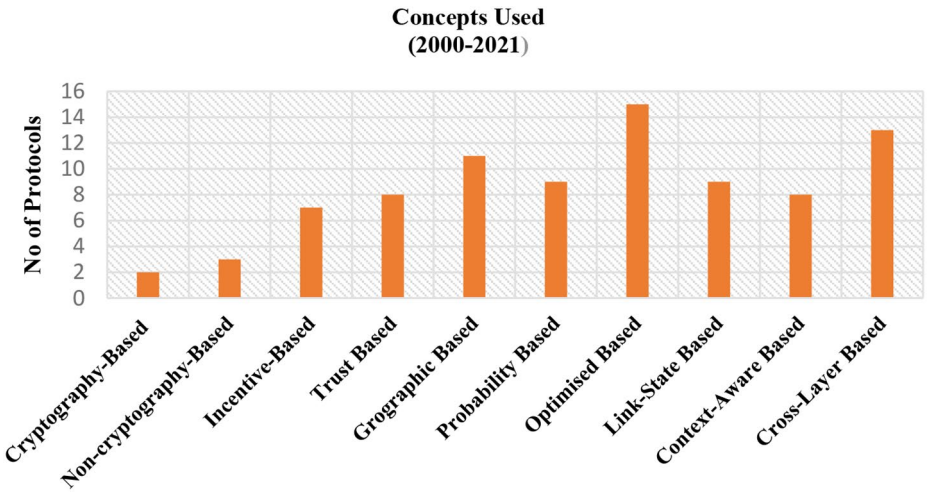

Fig. 12 Protocols of opportunistic network

Diverse types of opportunistic routing protocols are presented in Fig. 12. Sub-class cryptography included privacy in context-based and epidemic forwarding, and bootstrapping security associations in opportunistic networks [26–27]. Non-cryptography-based opportunistic routing class includes trust in the opportunistic network, social trust in the opportunistic network, and trust management scheme based on behaviour feedback for the opportunistic network [28–30]. Realization of Incentives to Combat Selfishness, Incentives and Reputation for Opportunistic Networks using Social Networks, Socially Selfish Aware Routing, Incentive-based pub/sub, Barter Trade, etc., come in the class of incentive-based secure routing protocol [31–33].

Various trust-based routing protocols were proposed in this category SUCCESS, RADON, and A trust-based framework for data forwarding [34], etc. Around 85 routing protocols in the opportunistic network were studied in this study. Routing for OppNet. exists in link-state aware classes are OR, ECONOMY, MORE, Code OR, Slide OR, etc. The geo-

graphical category includes CBF, GeRaF, GOR, MGOR, ROMER, etc. routing protocols. MaxPreps, FPOR, EBR, OPF, delegation forwarding, etc., are examples of probabilistic-based opportunistic routing protocols.

PHY-Aware ILOR, SPOR, EEPOR, TLGOR, Parallel OR, etc., are existing protocols in cross-layer routing protocols in the opportunistic network. The optimised-based category includes Graph-based SMAF, MABF, PLASMA, LOR, MAP, etc., routing protocols [9, 20, 35–39]. Figure 13 presents the analysis of existing routing protocols in the wireless network. A maximum ratio of existing protocols comes in the category of an Opportunistic network, and a minimum ratio is considered in the vehicular ad-hoc network.

6 Conclusion, Limitations and Future Work

Due to advancements in technology, wireless networks apply to multidivergent environments. In this study, diverse kinds of existing routing protocols are described. A concept used during the design of the protocol is discovered. Taxonomy was discussed to give background knowledge of the wireless network. Bibliometrics analysis of wireless networks by using the science mapping tool VOS viewer was shown in figure-2 to figure-8. Articles published on "Wireless Network" concerning years, citations of articles concerning countries, and highly cited keywords & sources used by authors, were empirically analysed to find the most suitable, source, keyword and other information which are useful for researchers.

Their benefits, weaknesses, properties, and applications were presented effectively (in tabular form) for MANET, VANET, WSN, and OppNet in this paper. Approximately 14% of routing protocols come under the category VANET. 25% of routing protocols exist in the MANET and WSN. A maximum of 36% of routing protocols come in the opportunistic network. This article also comes with limitations, the description of included protocols (ex. DDFP, FCMA, D-SEMA) for the different networks was not included. The simulation environment for the protocols is also not used in this paper. In future work, a systematic literature review with the implementation of novel protocols will be considered.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s11277-024-11064-9.

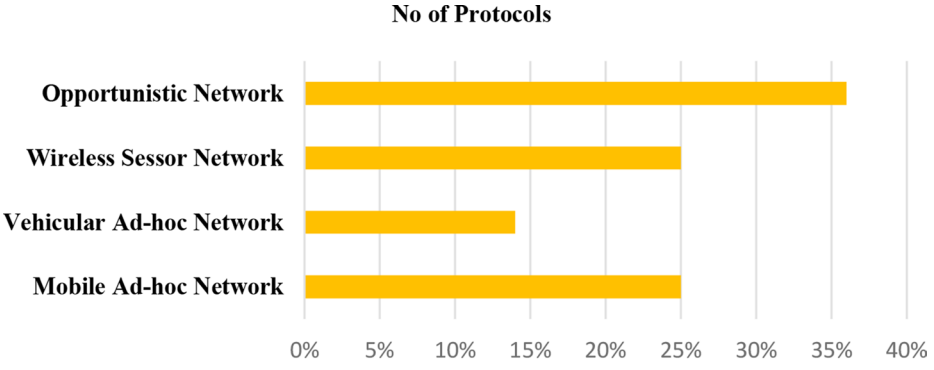

Fig. 13 Analysis of existing protocols in wireless network

Author Contributions Renu Dalal(RD), Manju Khari(MK), Sanjay Misra(SM). RD and MJ conceptualize the topic. RD, MJ, and SM are involved in Methodology, investigation, and validation. SM and MK supervised the whole work. All authors reviewed the manuscript.

Funding Open access funding provided by Institute for Energy Technology

Data Availability The data is collected from literature and the internet and all are duly cited.

Code Availability Not applicable.

Declarations

Conflict of Interest Authors do not have any financial or non-financial interests that are directly or indirectly related to the work submitted for publication.

References

1. Dalal, R., Singh, Y., & Khari, M. (2012). A review on key management schemes in MANET. *International Journal of Distributed and Parallel Systems*, *3*(4), 165.
2. Dalal, R., Khari, M., & Singh, Y. (2012). Different ways to achieve Trust in MANET. *International Journal on AdHoc Networking Systems (IJANS)*, *2*(2), 53–64.
3. Dalal, R., Khari, M., & Singh, Y. (2012). Survey of trust schemes on an ad-hoc network, In *International Conference on Computer Science and Information Technology*, Springer, Berlin, Heidelberg, pp. 170–180.
4. Dalal, R., Khari, M., & Singh, Y. (2012). Authenticity check to provide a trusted platform in MANET (ACTP), In *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*, pp. 647–655.
5. Dalal, R., & Khari, M. (2012). The New Approach to provide trusted platform in MANET. *International Journal of Security Privacy and Trust Management (IJSPTM)1*(6).
6. Khari, M., Dalal, R., Misra, U., & Kumar, A. (2020). AndroSet: An Automated Tool to Create Datasets for Android Malware Detection and Functioning with WoT. *In Smart Innovation of Web of Things*, pp. 187.
7. Khari, M., Dalal, R., & Rohilla, P. (2020). Extended Paradigms for Botnets with WoT Applications: A Review. *In Smart Innovation of Web of Things*, pp. 105.
8. Fall, K. (2003). A delay-tolerant network architecture for challenged internets, In *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ACM, Karlsruhe, Germany, pp. 27–34.
9. Dalal, R., & Khari, M. (2021). Empirical analysis of routing protocols in Opportunistic Network. *Research in Intelligent and Computing in Engineering* (pp. 695–703). Springer.
10. Ahmad, K., Udzir, N. I., & Deka, G. C. (2018). *Opportunistic networks: Mobility models, protocols, security, and privacy*. CRC.
11. He, X. R., Wu, Y. Y., Yu, D. J., & Merigó, J. M. (2017). Exploring the ordered weighted averaging operator knowledge domain: A bibliometric analysis. *International Journal of Intelligent Systems*, *32*(11), 1151–1166.
12. Van, E. N. J., & Waltman, L. (2009). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538.

13. Arebi, P. (2024). Improving AODV routing protocol using a multi-objective mechanism based on repairing broken links on the MANET networks. *International Journal of Mobile Network Design and Innovation*, *11*(1), 27–38.
14. Prasanna, K. S., Ramesh, B., & Review, A. (2024). An Efficient and Reliable Secure Routing Mechanism with the Prevention of Attacks in Mobile Ad-Hoc Network (MANET), *Wireless Personal Communications*, pp.1–40.
15. Chen, X., & Wang, X. (2024). Mobility handover in VANET. *Wireless Personal Communications*, pp.1–11.
16. Cai, S., & Wang, X. (2024). Domain-based address configuration for vehicular networks. *Wireless Personal Communications*, pp.1–19.
17. Jurado, F., Delgado, O., & Ortigosa, Á. (2020). Tracking news stories using blockchain to guarantee their traceability and Information Analysis. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 39–46.
18. Jadhav, P., & Satao, R. (2016). A survey on opportunistic routing protocols for wireless sensor networks. *Procedia Computer Science*, *79*, 603–609.
19. Dalal, R., & Khari, M. (2023). Efficacious implementation of deep Q-routing in opportunistic network. *Soft Computing*, pp.1–19.
20. Dalal, R., Khari, M., Anzola, J. P., & García-Díaz, V. (2021). V, Proliferation of opportunistic routing: A systematic review. *IEEE Access: Practical Innovations, Open Solutions*.
21. Bing, W., Jie, W., & Yuhong, D. (2008). An efficient group key management scheme for mobile ad hoc network. *International Journal and Networks*, Vol.
22. Aldar, C. (2004). *Distributed symmetric Key Management for Mobile ad hoc networks*. IEEE.
23. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating Routing Misbehavior in Mobile Ad-hoc Networks. *In ACM MobiCom conference*.
24. Buchegger, S., & Boudec, J. (2002). Performance analysis of the confident protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). *In MobiHoc'02, IEEE/ACM Symposium on Mobile Ad-hoc Networking and Computing*.
25. Shafiq, M., Humaira, A., Ata, U., & Shireen, T. (2020). Systematic Literature Review on Energy Efficient Routing Schemes in WSN–A Survey. *Mobile Networks and Applications*, pp. 1–14.
26. Shikfa, A., Onen, M., & Molva, R. (2010). Bootstrapping security associations in opportunistic networks, *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE Press, pp. 147–152.
27. Trifunovic, S., & Legendre, F. (2009). *Trust in opportunistic networks*. Computer Engineering and Networks Laboratory, pp.1–12.
28. Trifunovic, S., Legendre, F., & Anastasiades, C. (2010). Social trust in opportunistic networks, In *2010 INFOCOM IEEE Conference on Computer Communications Workshops*, IEEE, pp. 1–6.
29. Liang, X., JianFeng, S., & Zhuo, M. (2015). A trust management scheme based on behaviour feedback for opportunistic networks. *China Communications*, *12*(4), 117–129.
30. Mohammad, S. A., Rasheed, A., & Qayyum, A. (2011). VANET architectures and protocol stacks: a survey. In *International Workshop on Communication Technologies for Vehicles*, Springer, pp. 95–105.
31. Uddin, M., Godfrey, B., & Abdelzaher, T. (2010). RELICS: In-network realization of incentives to combat selfishness in DTNs, in *Proc. 18th IEEE Int. Conf. Netw. Protocols*, pp. 203–212.
32. Bigwood, G., Henderson, T., & IRONMAN. (2011).: Using social networks to add incentives and reputation to opportunistic networks, in *Proc. 3rd Int. Conf. Privacy Security Risk Trust*, pp. 65–72.
33. Li, Q., Gao, W., Zhu, S., & Cao, G. (2012). A routing protocol for socially selfish delay tolerant networks. *Ad Hoc Networks*, *10*(8), 1619–1632.
34. Li, N., & Das, S. K. (2010). RADON: Reputation-assisted data forwarding in opportunistic networks, in *Proc. 2nd Int. Workshop Mobile Opportunistic Netw*., pp. 8–14.
35. Zeng, K., Yang, Z., & Lou, W. (2009). Location-aided opportunistic forwarding in multi-rate and multihop wireless networks. *Ieee Transactions on Vehicular Technology*, *58*(6), 3032–3040.
36. Fussler, H., Widmer, J., Kasemann, M., Mauve, M., & Hartenstein, H. (2003). Contention-based forwarding for mobile ad-hoc networks. *Ad Hoc Networks*, *1*(4), 351–369.
37. Burgess, J., Gallagher, B., Jensen, D., & Levine, B. (2006). MaxProp: Routing for vehicle-based disruption-tolerant networks, *Proc. 25th IEEE Conf. INFOCOM*, vol. 6.
38. Bletsas, A., Dimitriou, A., & Sahalos, J. (2010). Interference-limited opportunistic relaying with reactive sensing, *IEEE Trans. Wireless Commun*,(9) 14–20.
39. Laufer, R., Dubois-Ferriere, H., & Kleinrock, L. (2009). Multirateanypath routing in wireless mesh networks, Proc. *IEEE Conf. INFOCOM*, pp. 37–45.

Renu Dalal received the bachelor's degree in computer science and engineering from the Indira Gandhi Institute of Technology, Delhi, India, affiliated with Guru Gobind Singh Indraprastha University, Delhi, and the master?s degree in information security from the Ambedkar Institute of Advanced Communication Technologies and Research, affiliated with Guru Gobind Singh Indraprastha University, where she is currently pursuing the Ph.D. degree in computer science and engineering. She has over eight years of experience in academics. She has published 15 papers in refereed national/international journals and conferences, such as IEEE, ACM, Springer, and Wiley. Her research interests include opportunistic networks, wireless ad hoc and sensor networks, data mining, and the IoT networks.

Manju Khari received the master's degree in information security from the Ambedkar Institute of Advanced Communication Technologies and Research, affiliated with Guru Gobind Singh Indraprastha University, Delhi, India, and a Ph.D. degree in computer science and engineering from the National Institute of Technology Patna. She is currently an Associate Professor with Jawaharlal Nehru University, New Delhi, prior to the university she worked with the Netaji Subhas University of Technology, East Campus, formerly the Ambedkar Institute of Advanced Communication Technologies and Research, Under the Government of NCT Delhi. She has published 80 papers in refereed national/international journals and conferences, such as IEEE, ACM, Springer, Inderscience, and Elsevier, ten book chapters in a Springer, CRC press, IGI Global, and Auerbach. She has coauthored of two books published by NCERT of XI and XII and co-editor in ten edited books. She has also organized five international conference sessions, three faculty development programme, one workshop, and one industrial meet in her experience. She delivered an expert talk, guest lecturers in international conference, and a member of reviewer/technical program committee in various international conferences. Besides this, she associated with many international research organizations as an Associate Editor/a Guest Editor of Springer, Wiley, and Elsevier books, and a reviewer of various international journals.

Sanjay Misra Dr. Sanjay Misra, a distinguished Senior Member of IEEE and ACM Distinguished Lecturer(21-24), currently serves as a Senior Scientist at the Institute for Energy Technology (IFE) in Halden, Norway. Previously, he held positions within the Computer Science and Communication department at Østfold University College, also in Halden. Dr. Misra holds a Ph.D. in Information and Knowledge Engineering (Software Engineering) from the University of Alcala, Spain, and an M.Tech. in Software Engineering from MLN National Institute of Technology, India. His expertise spans Applied Informatics, encompassing Software Engineering Applications, Cyber Security, Health Informatics, and Intelligent Systems utilizing AI and computational techniques. With an impressive publication record, including around 150 JCR/SCIE articles in prestigious journals such as Computers & Security and Engineering Applications of Artificial Intelligence, Dr. Misra consistently ranks among the top 2% of scientists globally, as recognized by Stanford University. He has received numerous awards for his outstanding contributions, including the 2014 IET Software Premium Award (UK). Dr Misra serves as Editor-in-chief and editor of multiple international journals, including the International Journal of Human Capital & Information Technology Professionals(EIC, IF. 1.9), Nature: Scientific Report((Impact Factor: 4.996), Elsevier: Alex. Engineering((Impact Factor: 6.8, Q1)), General chairs of several IEEE and Springer conferences and has edited numerous special issues and authored over 100 books and conference proceedings. A sought-after speaker, he has delivered over 100 keynotes and invited talks at prestigious conferences and institutes across more than 60 countries.