International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 2, April 2019, pp. 1145~1152
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i2.pp1145-1152

Opportunistic mobile social networks: architecture, privacy, security issues and future directions

Vimitha R. Vidhya Lakshmi, Gireesh Kumar T
TIFAC-CORE in Cyber Security, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India

Article Info

Article history:

Received Apr 1, 2018
Revised Oct 24, 2018
Accepted Nov 5, 2018

Keywords:

Data routing
Mobile social networks
Opportunistic networking
Privacy and security
Spam filtering

ABSTRACT

Mobile Social Networks and its related applications have made a very great impact in the society. Many new technologies related to mobile social networking are booming rapidly now-a-days and yet to boom. One such upcoming technology is Opportunistic Mobile Social Networking. This technology allows mobile users to communicate and exchange data with each other without the use of Internet. This paper is about Opportunistic Mobile Social Networks, its architecture, issues and some future research directions. The architecture and issues of Opportunistic Mobile Social Networks are compared with that of traditional Mobile Social Networks. The main contribution of this paper is regarding privacy and security issues in Opportunistic Mobile Social Networks. Finally, some future research directions in Opportunistic Mobile Social Networks have been elaborated regarding the data's privacy and security.

Corresponding Author:

Gireesh Kumar T,
TIFAC-CORE in Cyber Security,
Amrita School of Engineering, Amrita Vishwa Vidyapeetham,
Coimbatore, TamilNadu, India.
Email: t_gireeshkumar@cb.amrita.edu

1. INTRODUCTION

Social Networks are networking platform where users communicate with each other. Social Networks are classified based on type of device used for communication either as Web based Social Network or Mobile Social Network. Web based Social Networks are those types of social networks that use desktop as the device for communication. When the communicating nodes in social networks are mobile in nature then such kind of networking platform is said to be Mobile Social Networks (MSNs). Here mobility is due to using mobile devices such as smart phones, PDAs, tablets etc.

More details on MSNs, its architecture, types, usage, applications [1], privacy and security issues, existing solutions and some proposed solutions can be seen in [2]. MSN mainly falls into two categories: Traditional MSN and Opportunistic MSN (Future MSN or OMSN). The main differences between Traditional MSN and Opportunistic MSN are listed below in Table 1.

Table 1. Differences between Traditional MSN and Opportunistic MSN

Traditional MSN	Opportunistic MSN
Infrastructure Based	Infrastructure less
Includes Centralized or local Servers	No Centralized or local Server
Works with the help of Internet or intranet	Works without Internet but with the help of some short-range communication technologies (WiFi Direct, Bluetooth, NFC, etc.)

OMSN is a form of Mobile Ad-hoc Network (MANET) where data exchange/forwarding happens, on demand, among self organizing mobile nodes. These mobile nodes consider each other's social characters also for information exchange. Only difference between OMSN and MANET is found in the method of data routing. One of the major application and important form of opportunistic networking can be seen in Vehicular Social Networking. Vehicular Social Networks (VSN) are highly dynamic and connections get disconnected very fast. So, for such kind of networks this type of networking will be reliable and effective.

In opportunistic networking, the source node transfers data to destination node through one/many intermediate nodes that comes in the transmission range of transferring node. If there are no nodes in the transmission range of transferring node, the transferring node store the data and wait till it encounters with any node to transfer. The nodes work in store-carry-forward method. Therefore, opportunistic networks are said to be a special kind of Delay Tolerant Networks (DTNs).

Some of the advantages of OMSNs are: No infrastructure so cost effective, Power consumption is low, can be used in disaster relief, Best technology to be used in developing & rural regions and Avoids unnecessary communications. There are various applications for OMSNs including Message/File transferring, Audio/Video transferring, Disseminating/Forwarding Social Contents (news, traffic, alerts, social media, etc.), Finding Neighbor users which helps to meet people within range in conferences, malls, large companies, etc.

There are also many issues in OMSN in areas of Resource Management and User Behavior, Privacy and Security, Data mining, Mobile Crowd-Sourcing and Mobile IOT, of which privacy and security is considered as prior and discussed in detail in later sections. This paper is organized as: the architecture of OMSN and the architectural comparison of OMSN with MSN is discussed in Section 2. Section 3 gives brief overview of issues in OMSN. Privacy and security issues of OMSN are described in Section 4. Existing solutions and research directions regarding it are discussed in Section 5.

2. ARCHITECTURE OF OPPORTUNISTIC MOBILE SOCIAL NETWORK

The architecture of traditional MSN is compared with that of OMSN. There are two main architectural components present here: mobile node and server. Mobile nodes are the mobile users who use mobile devices such as smart phones, tablets, iPad or PDA's for communication. Servers can be centralized or local server which acts as content/service provider. All the information that is flowing in the network is stored and retrieved from these servers.

Figure 1 shows the architecture of traditional MSN. Here mobile nodes exchange information/data with other mobile nodes with the help of Internet using WiFi or base station as access points. The information is stored in content/service provider which acts as centralized server. In some cases, architecture of MSN will act in de-centralized manner also. Here instead of centralized servers, local servers take their role and mobile nodes communicate with each other through intranet.

Figure 2 shows the architecture of OMSN. Here mobile nodes communicate with each other directly without using Internet but with the help of some short-range communication technologies like direct WiFi, Bluetooth, NFC, etc. When one mobile node comes inside the transmission range of other mobile node, the data/information of both the nodes are exchanged with each other.

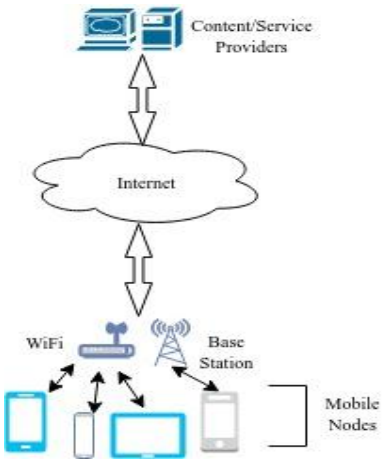

Figure 1. Architecture of traditional mobile social network

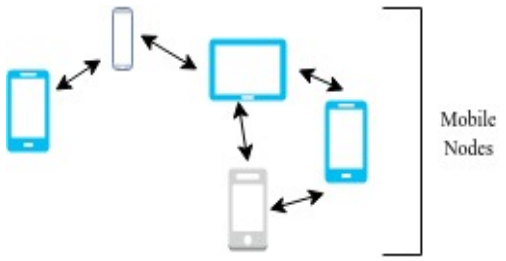

Figure 2. Architecture of opportunistic MSN

3. ISSUES IN OPPORTUNISTIC MOBILE SOCIAL NETWORKS

Issues in traditional MSNs and OMSNs are almost same and are seen per context suitability and importance. There are several issues and some of them are as follows:

3.1. Resource management and user behavior

Resources include bandwidth, battery energy, processing power, etc. More usage of these kinds of resources may lead to depreciation of resources. Therefore proper management in the usage of these resources is challenging. User behavior is a factor for participation of users in the data routing. Maximum participation is needed for proper data forwarding without delay and with high accuracy. But most of the users are selfish and ignore their participation due to their own limited battery power. Therefore analyzing user behavior and including proper user incentives are important for maximum participation of users. Resource management is an important factor which is to be solved in both the cases, traditional MSN as well as OMSN. But user behavior issue mainly affects OMSN because data routing/forwarding in OMSN purely depends on the mobile nodes that participate in message transferring.

3.2. Privacy and security

Privacy and security is an important research area that has no end and perfect solution. Even though there are many privacy and security solutions [3], [4], nothing is accurate and perfect until there are active hackers outside there. There are lots and lots of privacy and security issues in both traditional MSN and OMSN. And also there exist many solutions for privacy and security issues in traditional MSN. As OMSN is an upcoming technology only few privacy and security issues are solved. More concentration should be given in this area for secure and efficient OMSN.

3.3. Data mining

Mobile nodes usually involve in collecting the data from surroundings or storing their data into surroundings (cloud in case of traditional MSN or other mobile nodes in case of OMSN). In both the cases the computations should be done in such a way that the mobile node's battery consumption is low and the node's privacy is not compromised.

3.4. Mobile crowd-sourcing

There are several applications in traditional MSN that involves mobile crowd-sourcing. Existing solutions in traditional MSN does not handle service failures and does not ensure a high level of reliability. Therefore, sufficient works should be done in these areas. OMSNs mainly involve strangers or nodes that are completely unknown. These unknown nodes can be a trusted node or malicious node. It is difficult to find such kind of nodes in OMSN. Therefore, collective intelligent information is needed from a large group of people in-order to solve these kinds of complicated problems. This is known as crowd-sourcing and is also an important area of research in demand.

3.5. Mobile IOT

As days go web/Internet information gets increased and is getting overloaded. In addition to the above said overloading, information from IOT related technologies also contribute a major part. Studies say that the IOT related information together with web information is going to be larger than the current size of the web in the forthcoming years. In-order to avoid this information overloading, Mobile IOT can be in the form of opportunistic networking by using any short-range communication technology with high reliability and without Internet.

4. PRIVACY AND SECURITY ISSUES IN OPPORTUNISTIC MSN

The privacy and security issues in opportunistic networking are discussed in detail in [5]. Some of the sub-areas which need more attention in this area regarding privacy and security issues in OMSN include:

4.1. Misbehavior detection

There will not be any OMSN without any malicious node. Detection of these malicious nodes is quite difficult because the behavior of nodes in OMSNs cannot be per-determined. These kinds of nodes will be surely misbehaving gradually. Misbehavior of nodes can happen in two ways: 1) the node itself will be malicious as seen in case of intrusion detection or 2) the malicious node pretends to be non-malicious node as seen in case of Sybil attacks. Detection of these malicious nodes and avoiding them is an important issue in demand which is to be solved quickly and efficiently. Intrusion Detection: It is the detection of malicious nodes in OMSNs. These intruder nodes affect the OMSN badly, mainly during the time of data routing.

Real time intrusion detection is complicated and challenging due to the heterogeneous nature of opportunistic networking. Sybil Detection: Here, the malicious node/attacker forges the identity of the other non-malicious node in the OMSN. This is also a behavior-based attack in-order to gain the trust of the other nodes in the network.

4.2. User privacy

Privacy of users is important in all kinds of network especially in opportunistic networks. Only if the privacy of the user is guaranteed, the user will participate in this kind of network. Participation of user in OMSN is very important as the users are the main component in this network. They are the mobile nodes. User privacy includes the identity, location and other details involving user to be safe and must not be revealed to other nodes without the prior knowledge of the user.

4.3. Solution for dangerous attacks

There are many dangerous attacks in OMSN and finding proper solutions to these dangerous attacks is yet another issue. Some of the possible dangerous attacks have been formulated in [6], of these common and important attacks are ID Spoofing, Denial of Service attack, Man-in-the-middle attack and packet dropping. An efficient OMSN should be such a network that can withstand or sustain at-least the above said attacks.

4.4. Data privacy and security

Regarding data, the sub-areas are: Secure data routing/forwarding, Secure spam filter and Data privacy and security. Secure data routing means the data that is transferred from the source to the destination to be safe and confidential. Secure spam filter means the unwanted data or the data which the user feels unwanted should be filtered before this data reaches the destination mobile user. And also, the keywords used for filtering this, should be protected in terms of integrity and confidentiality. Data privacy and security involves the integrity and confidentiality of the data that is been circulated inside OMSN. The leakage of data outside OMSN should be prevented and also non-repudiation should be achieved efficiently.

5. FUTURE DIRECTIONS REGARDING DATA'S PRIVACY AND SECURITY ISSUES

5.1. Secure data routing

For secured and efficient routing mainly three things should be considered: a) Selection of legitimate relay nodes, b) Accurate delivery with high delivery rate, c) Low delivery latency and low network overhead. Of these three things, a) can be attained by correctly finding and avoiding the malicious nodes as relay nodes b) as well as c) can be achieved by increasing relay node participation and selecting relay nodes that have maximum delivery probability. Some relay nodes do not co-operative and participate because of its own battery power depreciation, fear and selfishness. So, this should be avoided by providing some user incentives. Some of the efficient routing protocols in OMSN, till date, are listed below in Table 2.

It is seen that most of the efficient routing protocols lack security and privacy. The routing methods are efficient in terms of high delivery rate, low delivery latency and low network overhead but are not secured. No efficient security schemes are incorporated in these routing methods to detect malicious nodes. Thus, data flowing inside the network will lack safety and privacy. Thus, proper security schemes also should be attached with these efficient routing protocols to achieve secure data routing. This area is one of the research directions in OMSN.

Table 2. Routing Protocols in OMSN

Sl.No.	Name of the technique & Year	Technique	Inferences
1	Epidemic, 2000 [7]	• Flooding based mechanism. • 2 buffers present: one for holding its own messages and the other for holding messages received from other nodes. • Every node maintains a Summary vector which holds the IDs of all messages.	• High delivery ratio • Low delivery latency • Insufficient buffer capacity • Very high network overhead (high bandwidth)
2	First Contact, 2004 [8]	• A node transfers message to another node whichever comes in first contact with it. • Routing path and relay nodes chosen randomly. • After message is transferred to relay nodes, the message is deleted. So only single copy of the message is maintained	• Low network overhead • High delivery latency (if no nodes comes in contact no transferring is done) • Low delivery ratio

Table 2. Routing Protocols in OMSN (*continue*)

Sl.No.	Name of the Technique & Year	Technique	Inferences
3	Direct Delivery, 2004 [9]	• Forwards message only when the destination node comes in contact with the source node.	• Low network overhead • High delivery latency, Low delivery ratio
4	PROPHET, 2004 [10]	• Probabilistic Routing Protocol using History of Encounters and Transitivity. • Maintains summary vector as well as delivery predictability metric.	• High delivery ratio • Low delivery latency • Low network overhead
5	Spray and Wait, 2005 [11]	• Controls the level of flooding. • Spray phase: Spread the message to the relay nodes. • Wait phase: If destination not found during spray phase then relay nodes having the copy of the message transfers the message directly to destination node when it comes in contact with any of the relay nodes.	• Low network overhead (less number of transmissions) • Low delivery latency • Low delivery ratio
6	MaxProp, 2006 [12]	• Proposed for VANETs (Vehicular Ad-hoc Networks). • Relay nodes will be the nodes that have maximum delivery probability. • Uses modified Dijkstras algorithm. And includes acknowledgement of messages delivered.	• Very high delivery ratio • Very low delivery latency • High network overhead
7	PROPICMAN, 2007 [13]	• Probabilistic Routing Protocol for Intermittently Connected Mobile Ad-hoc Network. • Maintains node profile and Routing path depends on the node profile of two-hop neighbor nodes which has the highest delivery probability.	• Low network overheads • Privacy of node profile is preserved
8	HiBOp, 2008 [14]	• History Based routing protocol for Opportunistic networks. • Depends on the context information, behavior of the user and user's social relationship.	• Better performance in resource utilization and user perceived QoS • Privacy, scalability and sensitiveness still remain unsolved
9	OPF, 2009 [15]	• Optimal Probabilistic Forwarding. • Includes OPF metric and depends on optimal stopping rule problem. • Works with other algorithms like ticket based forwarding.	• Delivery rate 5% less than epidemic and 20% more than delegation forwarding
10	CSPR, 2010 [16]	• Conditional Shortest Path Routing. • Link cost is based on conditional inter-meeting time.	• Higher delivery rate • lower end-end delay
11	Bubble Rap, 2011 [17]	• Relay nodes are selected depending on centrality and community social metrics.	• Low resource utilization • Better delivery performance
12	CiPRO, 2012 [18]	• Context Information Prediction for Routing in OppNets. Based on back propagation neural network model. • Both temporal and spatial activity dimension of the mobile node is considered.	• Outperforms other routing algorithms
13	HBPR, 2013 [19]	• History Based Prediction Routing. • Relay nodes selected depending on the node's behavioral information.	• Deliverey ratio and overhead ratio shows better performance than epidemic routing
14	GAR, 2014 [20]	• Group Aware cooperative Routing protocol. • Based on cooperative message transfer technique and a buffer management scheme.	• High delivery ratio • Improved latency and good-put
15	ML-SOR, 2015 [21]	• Multi-Layer- Social network based Opportunistic Routing. • Relay nodes selected based on metrics like tie strength, link prediction and node centrality.	• Better routing performance • Low overhead cost
16	Fibonary Spray and Wait, 2016 [22]	• Modified version of spray and wait protocol. • Better performance even in non-independent and identically distributed node structure.	• Better than spray and wait protocol
17	UBM, 2017 [23]	• Utility-based Buffer Management strategy. • Driven by caching policies, passive and proactive dropping policies and scheduling policies of senders.	• High delivery ratio • Low delivery delay • Low network cost

5.2. Secure spam filter

There are many types of information exchanged between the users of OMSN. Types of information are like rumors, advertisements, offers, newsletters, personal posts etc. Not all users in OMSN find all such information useful. Each user will have their own preferences and they consider all other information beyond their current needs as useless or unwanted information. Such useless or unwanted information for a user is called as spam.

Spams are of great issue to the OMSN users as spams drain the battery of mobile devices. There are different kinds of spam. Of these the three common kinds of spam are Email spam, Web spam and Mobile spam. Spammers first started with Email spam then it moved to Web spam and finally with the birth of smart phones Mobile spam emerged. The mobile spams are text message spams that are directed through Short message services (SMS) or any other communication services.

Text message spam includes both SMS spam and other spams received through any short-range communications in mobile devices. The type of spam seen in OMSN is mobile spam. These spams should be filtered properly and efficiently. This is known as spam filtering. Some of the spam filtering techniques in OMSN is listed below in Table 3. There are only few research articles in this area of spam filtering in de-centralized or distributed manner as it is a new upcoming technology.

Table 3. Spam Filters in OMSN

Sl.No.	Name of the technique & Year	Technique	Inference
1	PReFilter, 2012 [24]	• Privacy preserving Relay Filtering. • Filtering is done based on node's interest and this filtering policy is distributed among it's friends in the network. Privacy of filters and nodes are maintained.	• Filtering is done at early stages • Low delivery cost
2	Unwanted content control in PSN, 2013 [25]	• Based on distributed trust management. • Analyzes the behavior and traffic at each node.	• Effective and saves the model from malicious nodes
3	SAFE, 2013 [26]	• Social based updAtable FiltEring. • Privacy is preserved. • Based on properties of merkle hash tree. • Advancement of PReFilter model.	• Detects forged filters • High delivery ratio • Low delay and communication overhead
4	TBS, 2014 [27]	• Trust Based Spreading. • Solves the cold start problem. • Resilient to Sybil attacks.	• Limited hop and replication spreading • Blocks spam at early stages
5	PIF, 2015 [28]	• Personalized fIne grained Filtering. • Privacy is preserved. Includes social assisted filter distribution scheme, coarse and fine grained filtering schemes, merkle hash tree • Advanced model of PReFilter and SAFE.	• Detects forged filters • High delivery ratio, Low delay, Acceptable resource consumption • Blocks spams at early stages

The research direction here is to build a spam filter in OMSN which is safe, secure and privacy retained. OMSN use short range communication techniques for communication, so the spam filter should work in de-centralized manner. The filter should be light-weighted to reduce overheads of communication and computation. And the keywords used for filtering should be made secure and privacy preserved in-order to achieve filter integrity and confidentiality. In short, the model built should be secure, fast, light-weight, accurate and efficient.

5.3. Data privacy and security

The data flowing inside the OMSN should be made secure and privacy preserved. This means that the attacker should not be allowed to modify any data inside OMSN. And also, the attacker must be prevented from snooping any kind of information that is inside this network. Any form of leakage of data should be avoided. For this an efficient scheme, should be built quickly that works in OMSN.

It is also seen that in most of existing schemes non-repudiation is poorly supported. Non-repudiation means the assurance that someone can never deny something, that is, the mobile nodes after sending any data can never deny they did not send that data. The main points to be considered in non-repudiation are 1) whether it is a proper message content, 2) whether the message is from proper origin, 3) whether the proof of message by recipient is included and 4) whether acknowledgement of message by the recipient is included. There are only few articles related to this topic in OMSN like [29], [30]. Therefore, this is also a main research challenge which is to be considered by the researches in their future works.

6. CONCLUSION

This paper analyzes different aspects of OMSN and traditional MSN. It identifies features introduced in OMSN to improve performance of MSN. Architectural design of MSN and OMSN is compared including its internal components. OMSN is analyzed in various aspects including secure data routing, secure spam filtering and privacy issues. Guidance for future research direction which can be carried out in the area of secure data routing, secure spam filtering, dealing privacy and security issues of future MSN (OMSN) are expounded in this paper.

REFERENCES

[1] Pandian, Vijay Anand, and T. Gireesh Kumar. "A Novel Cloud Based NIDPS for Smartphones," In *International Conference on Security in Computer Networks and Distributed Systems*, 2014. Springer, Berlin, Heidelberg, pp. 473-484.

[2] Vimitha R Vidhya Lakshmi and Gireesh Kumar T. "Mobile Social Networks: Architecture, Privacy, Security Issues and Solutions," *Journal of Communications*, vol. 12, no. 9, 524-531, 2017.

[3] Lu, Jian-Zhu, Xiuwei Fan, Jipeng Zhou, and Hao Yang. "An Improvement on an Efficient Mobile Authentication Scheme for Wireless Networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)* 11, no. 10, pp. 6250-6257. 2013.

[4] Mantoro, Teddy, and Andri Zakariya. "Securing E-mail Communication Using Hybrid Cryptosystem on Android-Based Mobile Devices," *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 10, no. 4, pp. 807-814. 2012.

[5] Lilien, Leszek, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta. "Opportunistic Networks: the Concept and Research Challenges in Privacy and Security," *Proc. of the WSPWN*, pp.134-147, 2006.

[6] Haus, Michael, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. "Security and Privacy in Device-to-Device (D2D) Communication: A Review," *IEEE Communications Surveys & Tutorials* 19, no. 2, pp: 1054-1079, 2017.

[7] Vahdat, Amin, and David Becker. "Epidemic Routing for Partially Connected Ad Hoc Networks," *Technical Report CS-2000-06*, Dept. of Computer Science, Duke University, Durham, NC., 2000.

[8] Jain, S., Fall, K., & Patra, R. "Routing in a Delay Tolerant Network," In *Proceedings of ACM SIGCOMM,*. Vol. 34, No. 4, pp. 145-158, 2004.

[9] Spyropoulos, Thrasyvoulos, Konstantinos Psounis, and Cauligi S. Raghavendra. "Single-copy Routing in Intermittently Connected Mobile Networks," In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference* on, pp. 235-244, 2004.

[10] Lindgren, Anders, Avri Doria, and Olov Schelen. "Probabilistic Routing in Intermittently Connected Networks." In *Service Assurance with Partial and Intermittent Resources*, pp. 239-254. Springer, Berlin, Heidelberg, 2004.

[11] Spyropoulos, Thrasyvoulos, Konstantinos Psounis, and Cauligi S. Raghavendra. "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks," In *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, ACM, 2005. pp. 252-259.

[12] Burgess, John, Brian Gallagher, David Jensen, and Brian Neil Levine. "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," In INFOCOM 2006. *25th IEEE International Conference on Computer Communications. Proceedings*, IEEE, pp. 1-11, 2006.

[13] Nguyen, Hoang Anh, Silvia Giordano, and Alessandro Puiatti. "Probabilistic Routing Protocol for Intermittently Connected Mobile Ad Hoc Network (Propicman)." In *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium* on a, IEEE, pp. 1-6, 2007.

[14] Boldrini, Chiara, Marco Conti, and Andrea Passarella. "Exploiting Users' Social Relations to Forward Data in Opportunistic Networks: The Hibop Solution." *Pervasive and Mobile Computing* 4, no. 5, pp. 633-657. 2008.

[15] Liu, Cong, and Jie Wu. "An Optimal Probabilistic Forwarding Protocolin Delay Tolerant Networks." In *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, ACM, pp. 105-114, 2009.

[16] Bulut, Eyuphan, Sahin Cem Geyik, and Boleslaw K. Szymanski. "Conditional Shortest Path Routing in Delay Tolerant Networks," In *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE international symposium* on a, IEEE, pp. 1-6, 2010.

[17] Hui, Pan, Jon Crowcroft, and Eiko Yoneki. "Bubble Rap: Social-based Forwarding in Delay-Tolerant Networks," *IEEE Transactions on Mobile Computing* 10, no. 11, pp. 1576-1589. 2011.

[18] Nguyen, Hoang Anh, and Silvia Giordano. "Context Information Prediction for Social-Based Routing in Opportunistic Networks," *Ad Hoc Networks* 10, no. 8, pp. 1557-1569. 2012.
[19] Dhurandher, Sanjay K., Deepak Kumar Sharma, Isaac Woungang, and Shruti Bhati. "HBPR: History Based Prediction for Routing in Infrastructure-Less Opportunistic Networks," In *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference* on, IEEE, pp. 931-936, 2013.
[20] Chen, Honglong, and Wei Lou. "GAR: Group Aware Cooperative Routing Protocol for Resource-Constraint Opportunistic Networks," *Computer communications* 48, pp. 20-29. 2014.
[21] Socievole, Annalisa, et al. "Ml-sor: Message Routing Using Multi-Layer Social Networks in Opportunistic Communications," *Computer Networks* 81, pp.201-219. 2015.
[22] Das, Priyanka, et al. "Fibonary Spray and Wait Routing in Delay Tolerant Networks," *International Journal of Electrical and Computer Engineering (IJECE)* 6.6, pp. 3205. 2016.
[23] Yao, Jiansheng, Chunguang Ma, Haitao Yu, Yanling Liu, and Qi Yuan. "A Utility-Based Buffer Management Policy for Improving Data Dissemination in Opportunistic Networks," *China Communications* 14, no. 7, pp. 1-9. 2017.
[24] Lu, Rongxing, Xiaodong Lin, Tom Luan, Xiaohui Liang, Xu Li, Le Chen, and Xuemin Shen. "Prefilter: An Efficient Privacy-Preserving Relay Filtering Scheme for Delay Tolerant Networks," In *INFOCOM, 2012 Proceedings IEEE*, IEEE, 2012. pp. 1395-1403.
[25] Yan, Zheng, Raimo Kantola, Gaowa Shi, and Peng Zhang. "Unwanted Content Control via Trust Management in Pervasive Social Networking," In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference* on, IEEE, 2013. pp. 202-209.
[26] Zhang, Kuan, Xiaohui Liang, Rongxing Lu, and Xuemin Sherman Shen. "SAFE: A Social Based Updatable Filtering Protocol with Privacy-Preserving in Mobile Social Networks," In *Communications (ICC), 2013 IEEE International Conference* on, IEEE, 2013. pp. 6045-6049.
[27] Trifunovic, Sacha, Maciej Kurant, Karin Anna Hummel, and Franck Legendre. "Preventing Spam in Opportunistic Networks." *Computer Communications* 41, pp. 31-42. 2014.
[28] Zhang, Kuan, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. "PIF: A Personalized Fine-Grained Spam Filtering Scheme with Privacy Preservation in Mobile Social Networks*." IEEE Transactions on Computational Social Systems* 2, no. 3, pp. 41-52. 2015.
[29] Zhang, Aiqing, et al. "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks." *IEEE Transactions on Vehicular Technology* 65.4, pp: 2659-2672. 2016.
[30] Abd-Elrahman, Emad, et al. "Fast Group Discovery and Non-Repudiation in D2D Communications Using IBE." *Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015 International. IEEE, 2015.

BIOGRAPHIES OF AUTHORS

Vimitha R Vidhya Lakshmi was born in Kerala, India, in 1990. She received the B.Tech. degree in Information Technology and the M.Tech. degree in Computer and Information Science from the Cochin University of Science and Technology (CUSAT), India, in 2012 and 2015 respectively. She is currently pursuing the Ph.D. degree with TIFAC-CORE in cyber security, Amrita University, India. Her research interests include Mobile computing, Information security and Wireless communication.

Gireesh Kumar T was born in Kerala, India, in 1976. He received the M.Tech. degree from the Cochin University of Science and Technology (CUSAT), India, in 2003 and the Ph.D. degree from Anna University, India, in 2011, both in Computer Science and Engineering. He is currently working as associate professor with TIFAC-CORE in cyber security, Amrita University, India. His research interests include Wireless communication, Machine learning, Algorithm and artificial intelligence.