ISSN 2320 -2610
Volume 11, No.6, November - December 2022
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis011162022.pdf
https://doi.org/10.30534/ijmcis/2022/0111162022

A Survey of Privacy-Aware Mobile Social Network Protocols and Proposal of Lightweight Encryption Scheme for MSN with Multiple Security Features

Opeyemi Isaiah Enitan[1], Agboola Aderonke Morufat[2]
[1]Manchester Metropolitan University, United Kingdom, yenitan1@yahoo.com
[1]Covenant University, Ogun State, Nigeria, yenitan1@yahoo.com
[2]Manchester Metropolitan University, United Kingdom, agboolar@gmail.com

Received Date : November 02, 2022 Accepted Date : December 01, 2022 Published Date : December 07, 2022

ABSTRACT

Mobile Social Networks (MSNs) have gained significant popularity in recent years. MSNs users exchange valuable information during different types of communication. Therefore, security and privacy of MSNs is critical for users and groups. Unauthorized access to data, disclosure of sensitive information, violation of user's privacy, and disruption of shared data integrity are the major challenges associated with MSNs. A systematic review of existing privacy schemes for MSNs is conducted and identified that existing techniques were designed for preserving the privacy of specific services, such as preservation of proximity-based services privacy, protection of user's profile privacy, and preservation of location services privacy. All the reviewed privacy-aware schemes are not suitable for implementation at large scale, because they do not enforce all the required security features for secure and private communication. In this paper, we proposed a lightweight encryption scheme with the proof of decisional bilinear Diffie–Hellman condition to ensure the authentication, anonymity, privacy, and secure data sharing between MSN users at large scale.

Key words: Authentication, Anonymity, MSN, Lightweight Encryption, Security, Privacy.

1 INTRODUCTION

The influence of Mobile Social Networks (MSNs) has been significantly increased on user's lives by enabling them communicating with each other in any place at any time. To get registered with MSN, users are required to provide their personal information. After registering with MSN, users exchange sensitive information with each other. Dissemination of information and data shared over MSNs offers various opportunities to businesses, social, and economic researchers. For the sake of personal benefits, MSN providers may breach the privacy of information and data owners [1].

According to the ownership agreement, MSN providers have full rights to distribute and use the user's information and data in an appropriate way they guess [2]. For instance, in 2016 Facebook was accused by the Supreme Court of US for using the pictures of children for advertisement purpose without the consent of their parents [3].

MSN users may face unfavorable or adverse consequences on their lives due to disclosure of their private information. Therefore, every MSN user wishes secure and private communication. That's why encryption schemes are considered as effective and compelling approaches in this regard. However, still more improvement is required to done in this domain.

In many of the previous privacy-aware schemes, researchers focused on the privacy and security of service of MSNs. For instance, preservation of proximity-based services privacy, protection of user's profile privacy, and preservation of location services privacy. Therefore, most of the existing techniques are not suitable for implementation at large scale. Researchers in [4] fully categorized the security requirements in MSNs to reduce threats and protect user's privacy. These requirements include:

- Information security
- Anonymity
- Privacy
- Integrity
- User awareness
- Fine grained access control

Most of the previous techniques do not enforce all the above-listed security features for secure and private communication in MSNs. Therefore, herein, we proposed a lightweight encryption scheme with the proof of decisional bilinear Diffie–Hellman condition to ensure the authentication, anonymity, privacy, and secure data sharing between MSN users at large scale.

1.1 Research Scope

The scope of this research covers the theoretical design of the proposed encryption scheme regardless of its actual implementation and testing. Moreover, theoretical design of the proposed encryption scheme only covers the security aspects of communication. Other measures, such as performance and resource consumption parameters, are not focused on theoretical design of proposed encryption scheme. An assumption can be made in this regard that there is always a clear tradeoff between security and performance.

1.2 Paper Organization

The rest part of this paper is structured as:

The summary of previous privacy-aware schemes for MSNs is given in Section 2 in form of literature review. Theoretical design of proposed scheme is described in Section 3. Brief description of evaluation tools that can be used to analyze the effectiveness of proposed scheme is given in Section 4. Conclusions related to these papers are presented in Section 5, in the end.

2 LITERATURE REVIEW

Mobile Social Networks are vulnerable to sensitive information and privacy breaches without appropriate security controls in place. This issue worsens when profile matching in MSN extends to a multi-hop environment because a greater number of nodes can access the profile information, and more adversaries can be expected. Thus, it becomes the main challenge in MSNs to preserve users' privacy during the recovery process. Various privacy-aware routing schemes have been proposed to address this concern. The major classes of proposed privacy-aware routing protocols in literature are attribute-based encryption and privacy-preserving friending. However, some authors proposed secure MSN protocols using other i.e., hybrid approaches.

2.1 MSN Protocols Secured with ABE

Each user in MSN is identified by specific attributes set in an Attribute-Based Encryption Scheme. In this privacy-aware routing scheme, associated functions with attributes are used to determine the ability for decryption of each cipher text. Specific users having certain interests or sets of attributes can decrypt the data. A cryptographic software library proposed by [5] showed the record timing in computing the attribute-based encryption scheme with a security level of 128 bits.

A multi-authority privacy-aware routing scheme based on attribute-based encryption has been developed by researchers in [6] that offers no interaction among authorities.

Researchers in [7] proposed a privacy-ware routing scheme for MSNs. This routing scheme relies on multi-party computation and private set-intersection technique. The multi-party computation achieves a different level of privacy for secret profile matching with the help of polynomial secret sharing.

Another privacy-aware routing scheme for MSNs is proposed by [8] that cogitates the attribute value for each profile, followed by the measurement of the degree of similarity among finely grained profiles based on homomorphic encryption.

The authors in [9] proposed a secure routing scheme for MSNs that enforces an access control mechanism with efficient revocation and attributes identification capabilities using cipher text policy attribute-based encryption.

2.2 MSN Protocols Secured with Privacy-Preserving Friending

All the above-discussed privacy-aware routing schemes are based on asymmetric cryptography. Therefore, extensive computations are required in those schemes. Moreover, a complicated setup, such as a TTP server, is required. To overcome this problem, a friend discovery privacy-ware routing scheme is proposed by [10]. This routing scheme is based on profile matching in MSNs. Moreover, it combines attribute-based encryption and privacy-preserving friending based on a confusion matrix. Due to this novel approach, this routing scheme does not rely on TTP server and is more efficient than routing schemes based on attribute-based encryption.

The authors [11] proposed a privacy-preserving routing scheme for Mobile Healthcare Social Networks (MHSNs) named as Same Symptom-based Handshake Scheme (SSH). The referred scheme assists the network in matching the users with the same symptoms as the author while preserving the privacy of those users who don't have the same symptoms as the author. Like this approach, researchers proposed a privacy-aware routing protocol that measures similarity among users by counting their common interests [12].

Researchers in [13] proposed a privacy-aware routing scheme based on Deviation Query Exchange (DQE). This scheme obscures users' query points to avoid disclosing trajectories in MSNs. The best matching user is identified to exchange the queries when requested. This secure routing scheme prevents adversaries from rebuilding users' trajectories by collecting the information from the location-based services server. Thus, users can take advantage of location-based services in MSNs while preserving their privacy. Researchers performed an extensive performance and security analysis of their proposed routing scheme to test its efficiency and effectiveness. Evaluation results indicate that the DQW based privacy-aware routing scheme can protect the privacy of the user's trajectory effectively with less overhead on location-based services server.

2.3 MSN Protocols Secured with Other Approaches

A secure routing scheme called Achieving Secure, and Privacy-Preserving (ASPP) for MSNs is proposed by [14]. The ASPP privacy-aware routing scheme is based on a short signature technique, reactive routing protocol, and cooperative neighbor technique. The ASPP can preserve the privacy of messages against compound and elemental attacks in MSNs. Moreover, researchers claimed their proposed ASPP routing scheme is hardened against the warm hole, eavesdropping, packet tracing, packet analysis, and reply to

attacks. Under various testing scenarios, the ASPP routing scheme demonstrated a high rate of practicability and detection of various attacks.

The authors [15] proposed an Appointment Card Protocol (ACP) to preserve the privacy of the location and identity of the original requestor in MSNs. The main idea behind the ACP routing scheme is the utilization of social ties among users. The researchers introduce the concept of appointment cards to simplify the obfuscation operations of queries. By using the information available in the appointment card, the original requestor can send direct queries to the location-based services, ensuring that the location-based services server does not detect the private information of the requester. Moreover, in the ACP routing scheme, researchers reduced the query reply time by keeping a path for reply to messages after sending the query. Evaluation results indicated that the ACP routing scheme showed a greater query success ratio and effectively preserved user information privacy [15].

Researchers raised the concern that the private information of frequency and encounter time is vulnerable to exposure when nodes in MSNs communicate with each other using their real identities [16]. On the other side of the pillar, the anonymity of the node identity can protect the privacy of information. Still, it also restricts the nodes from gaining encounter information for real utility value calculation. To solve this problem, researchers proposed a privacy-aware routing scheme for utility-based routing in delay-tolerant MSNs [16]. In this routing scheme, MSN nodes can protect the privacy of their information and gain real utility value at the same time by:

- Generating and collecting the encounter record information using pseudo-identities after the occurrence of node encounters.
- Forward the information to trusted authorities for calculating the routing utility value.

The proposed routing scheme by [16] preserves the integrity and confidentiality of the messages through digital signatures and hashing techniques. Evaluation of this routing scheme in a simulation environment proved that it could protect the privacy of the node's information and forward the messages effectively with real utility value.

According to the authors [17], location-sharing service is critical in mobile social networks, especially Vehicular Social Networks (VSNs), for sharing information and tightening their social bonds. However, location sharing may leak nodes' information, including their relationship and location information. As a solution to this problem, researchers proposed a secure distance comparison routing scheme [17]. This secure routing scheme ensures the privacy of inter-user threshold distance. According to the authors, the privacy of inter-user threshold distance information is critical because it can effectively be utilized in identifying nodes, their location information, and their friend's information in [17]. In their proposed routing scheme, the authors induced privacy-preserving location sharing to shape sophisticated access control policies. Security analyses are performed by the authors to validate the safety of their proposed secure routing scheme. The experiments' results prove this routing scheme's efficiency [17].

According to the authors [18], the various existing efforts made to preserve the privacy of nodes in MSNs during location sharing rely on the deployment of trusted cellular towers, and some put extended time overhead. As a contribution to the preservation of node's identity privacy, location privacy, and social location privacy, researchers proposed a novel System Architecture for Mobile Online Social Networks (SAM) and a privacy-aware routing scheme based on that novel system architecture [18]. The authors of the routing scheme claimed that their proposed routing scheme covers the full features of privacy protection, including identity privacy, location privacy, and social location privacy [18]. This property distinguishes their proposed secure routing scheme from the existing privacy-aware routing schemes.

Due to the absence of end-to-end connections between nodes in MSNs, messages are transmitted from one node to another to track the intended destination. Thus, it is the main challenge in MSNs to select an appropriate methodology for effectively selecting intermediate nodes and offering privacy and security for all nodes. To this extent, the authors [19] proposed a secure routing scheme for MSNs where nodes can carry a message without having explicit knowledge of intermediate, source, and destination nodes. It is undeniable that all the nodes in any network are not trustworthy. Therefore, the authors adopted the trusted structure, a public key-sharing approach, and a cooperation method in their proposed privacy-aware routing scheme [19]. The evaluation results of this routing scheme demonstrated that it could effectively resist selective and selfish dropping attacks. Moreover, this routing scheme is also effective against Sybil attacks. The researchers also analyzed the performance of the routing scheme and proved that it performed well in terms of message drop, latency, and network overhead.

Table 1 gives the summary of the privacy-aware routing schemes for Mobile Social Networks proposed in various articles as reviewed in this section.

Table 1 gives the summary of the privacy-aware routing schemes for Mobile Social Networks proposed in various articles as reviewed in this section.

Table 1: Categories Of Privacy-Aware Schemes For MSNs Proposed In Existing Literature

Privacy Model	***Network Model***	***Aim***	***Pros***	***Cons***
Protection of user's profile privacy	Trusted key distribution	Limit the disclosure of user's profiles	Good average running time and less computation complexity	Not considered layer routing
Transparency, immutability, and accountability	Each node in the network possesses sociality strength	Detection and prevention of warm hole attacks	+ Less transmission delays + accurately detects the hole link	Implementation complexity

Privacy Model	***Network Model***	***Aim***	***Pros***	***Cons***
Location sharing privacy	Each node has a sociality with the target's demographics	Offering diverse privacy controls	+ Compared the ground truth traces and shared mobility	Not compared with other privacy-aware routing schemes
Preservation of user's privacy	During friendship discovery, each node possesses a personal profile	Ensure a high level of user profile privacy	+ Less communication overhead + Compared with other schemes	Privacy of identity and location is not considered.
Preservation of proximity-based services privacy	Alice and Bob Notation for testing	Prevent the privacy leak from proximity-based services in MSNs	+Gives concrete way for the implementation of secure proximity-based services	Limited scope
Preserving the integrity, confidentiality, and nonrepudiation of encounter records	Nodes are distributed sparsely and encountered opportunistically	Ensure the integrity, confidentiality, and nonrepudiation of encounter records	+ Secure + Efficient + Practical	Implementation complexity Not compared with other schemes

3 PROPOSED SCHEME

We have divided the system we suggested in five parts, the first three steps are critical. User key exchange, data encryption, and data decryption are the three procedures. The recommended technique will be discussed in further depth below.

To achieve end-to-end encryption, this technique uses two encryption phases. The transmitted data over the social networking site is concealed from the server using the first encryption phase that is using AES, and a standard access control is implemented using the second stage using CP-ABE, which employs ABE for the second stage. Additionally, in this configuration, the certificate authority is a different legal entity from the social network and is not subject to its control. Although the user's main key is not available to this certificate authority, it oversees creating and disseminating some cryptographic keys.

Architecture of our proposed privacy-aware scheme for MSNs is demonstrated in Figure 1.

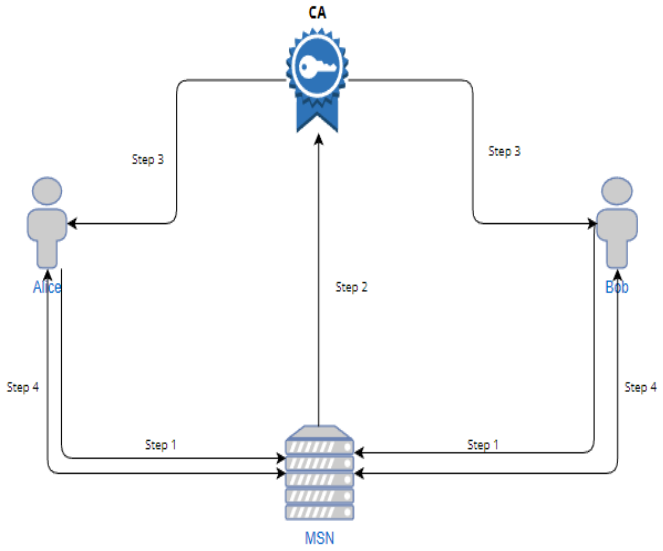

Figure 1: Proposed Privacy-Aware Scheme Architecture

Functional aspects of the proposed scheme are defined step by step in the following:

1. The entities in the communication that is entity A, Alice and Entity B, bob requests the MSN server for the exchange of key. Both entities in the communication are not required to be online at once. Users can ask for a specific re- transmission of their primary key to the MSN server. When requesting a key exchange, assume that there are two users online at once.
2. The server entity is MSN, and it requests that the CA server to give each of the entities both the encryption keys that are public RSA and private keys.
3. The keys generated in the process by the CA server that are both RSA public key and a private key are given to the entities. CA acquires these keys directly from users via social networks and distributes them once separately when all the entities are present on the socially connected network. To protect their private keys from their network provider, the entities A and B switch public keys. Entity B receives the private key that belongs to entity A and the public key of CA, whereas the RSA private key of entity A and the public key of entity B is acquired by CA. The entities in the communication are now prepared to provide their primary keys after reaching upon a mutual communication agreement by exchanging users' public keys.

4. The entity B's public RSA key is being used in the process and was acquired by the CA in step number 3 and has been given to the entity A. Entity A can now perform encryption on her own primary key, which is (EA_k). Key is used for performing the encryption type that is symmetric and shared to entity B through the MSN.
5. The encrypted key that is acquired by the CA and which is also provided by the entity A for the process of decryption is used by the entity B along with its own RSA key that is private. The process is done to reveal the main key of the entity A. On the device of entity B the man key of entity A is stored and it is further used for the process of decryption that is symmetric whenever the data exchange is performed.
6. The entity B performs the procedure of symmetric encryption on his primary key that is EB_k and for the purpose the RSA public key of the entity A has been utilized, that was provide to it in the step number 4 by the CA.
7. The key that is generated by the CA is RSA private and it belongs to entity A which she uses to perform decryption on the entity B's key. The process would result in the generation of the entity B's private key which is EB_k. Just like the entity B's device the device of entity A now has the primary key of the entity B which is further used for the communication whenever the data is set to be transmitted.
8. When the data transmission occurs, the entities participating in the communication have the keys for symmetric encryption and decryption after the completion of the earlier steps. Since the relevant keys are held on the devices of the entities, the method prevents MSN and the CA from obtaining the primary keys of those involved in communication. Because the server may see the contents of the main keys as they are transferred over the MSN, the procedure of encrypting the primary keys of the entities that are transmitted through MSN is essential.

The MSN server, on the other hand, cannot access the users' primary key since it is unaware of the RSA keys. This technique, which protects the user's private key, is the most critical aspect of their privacy.

Algorithm 1 shows the order in which the steps are performed for the key exchange by the entities.

Algorithm 1: Key Exchange Process

Step 1:
Begin
Step 2:
Alice to MSN
Send Req → Key_{ex}
Step 3:
Bob to MSN
Send Request → Key_{ex}
Step 4:
Check ID
MSN→ A_{id}
MSN→ B_{id}
If (A_{id} && B_{id} =exist)
{
A_{id} && B_{id} → CA
}
else
{ Req_{drop}
}
Goto step 10:
End if ()
Step 5:
CA → RSA_{key} → A&&B
Step 6:
Encryption
EA_k → $B_{pk(RSA)}$ → B
Step 7:
Encryption
EB_k → $A_{pk(RSA)}$ → A
Step 8:
Decryption:
B→ EA_k
Step 9:
A→ EB_k
Step 10
End

The encryption of data is performed in the steps as shown below in Algorithm 2:

Algorithm 2: Encryption Process

Step 1:
Begin
Step 2:
Encryption
A → $PT_{(AES)}$ → $EB\_k_{(MK)}$
PT→ T_{c1}
Step 3:
A to MSN
Send Request → $CP_{(ABE\_PK)}$
Step 4:
MSN→ A→ $CP_{(ABE\_PK)}$
Step 5:
A → Access policy (AP)
AP→ T_{c1}
Step 6:
Encryption
T_{c1} → $CP_{(ABE\_PK)}$
Step 7:
T_{c2} → T_{c1}
Step 8:
A → T_{c2}→ MSN
Step 9:
MSN→ T_{c1}
B→ EA_k
A→ EB_k
Step 10
End

The steps involved in the decryption of data are shown below in Algorithm 3: *Algorithm 3: Decryption Process*

Step 1:
Begin
Step 2:
B→ Send Request
T_{c1} →MSN
Step 3:
B to MSN
B→ Key($_{ATT\_B)}$
Step 4:
If (Key($_{ATT\_B)}$ = true)
{decrypt T_{c2} → Key($_{ATT\_B)}$
do (T_{c2}→ T_{c1})
}
Step 5:
MSN → T_{c1} → B
Step 6:
Decryption
T_{c1} → EB_k$_{(PK)}$
PT→ T_{c1}
Step 7:
B→ PT
Step 8:
End

With the recommended strategy, user data is safeguarded since it offers rigorous access control and privacy protection against server-related breaches. End-to-end encryption improves data integrity and transmission secrecy.

4 EVALUATION TOOLS

There are various network emulation and simulation tools available, and pertinent to the survey conducted above, to evaluate the proposed schemes by researchers. Following is the brief description of each.

4.1 The Network Simulator 2

Network Simulator 2 (NS2) is an event driven open-source network simulation tool. The primary use case of this simulation tool is in networking and computer communication research. NS2 offers significant support for simulation of multi-cast protocols, routing, TCP, Wireless Sensors Networks (WSNs), Mobile Social Networks (MSNs) and so on. According to the developers of NS2, it is still an ongoing project instead of finished and polished product [20]. Researchers are in contentious progress of enhancing the capabilities, reliability, and efficiency of NS2

4.2 OPNET Network Simulator

The OPNET network simulator can simulate the performance and behavior of any network type i.e. wired or wireless. This simulation tool is widely used for application troubleshooting, operation validation, network design and planning, hardware architecture validation, protocol modelling, telecommunication network's traffic modeling, and so on. This is also an open-source and freeware tool. However, network professionals can offer their pre-build devices and protocols models. They cannot make changes in existing ones. According to the developers of OPNET simulator, it is more versatile and powerful compared to other simulation tools. Event workflow of OPNET comprised of following phases:

- Create or import network topology
- Configuration of topology
- Creation of network traffic
- Make the choice of statistics
- Execution of simulation
- Display and publish results

4.3 OMNET++ Simulator

OMNET++ network simulator is specifically distributed under public academic license. This is a component-based modular and extensible network simulation framework built with C++ programming language. OMNET++ supports functionalities specific to various networking domains, such as photonic networks, IP networks, MSNs, Wireless Ad-hoc networks, and sensor networks. The main components of OMNET++ are:

- C++ kernel library for simulation
- Eclipse-based simulation integrated development environment
- QTENV, a runtime interactive graphical user interface.
- Command line interface
- Make file creation tool

5 CONCLUSION

Security is one of the crucial aspects of Mobile Social Networks due to the involvement of important and personal data exchange. When it comes to security, it doesn't mean protection of service. Instead, it is an umbrella term that should cover all important features required to protect the integrity, anonymity, confidentiality, and privacy of data in MSNs. Most of the privacy-aware routing schemes in existing literature are focusing on service of MSN (See Table 1). However, to fill the identified research gap, we proposed the theoretical design of lightweight privacy-aware scheme for MSNs that aims to protect the user's anonymity, their data privacy and integrity along with fine grained access control.

REFERENCES

[1] Suntaxi, Gabriela. **Preserving Secrecy in Online Social Networks: Data Outsourcing, Access Control, and Secrecy Schemes**. PhD diss., Dissertation, Karlsruhe, Karlsruher Institut für Technologie (KIT), 2020, 2020.

[2] Chang, Wei, Jie Wu, and Chiu C. Tan. **Friendship–based location privacy in mobile social networks.** International Journal of Security and Networks 6, no. 4 (2011): 226-236.

[3] Costello**, Caitlin R., Dale E. McNiel, and Renée L. Binder. Adolescents and social media: Privacy, brain development, and the law**. Journal of the American Academy of Psychiatry and the Law 44, no. 3 (2016): 313-321.

[4] Rathore, Shailendra, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, and Jong Hyuk Park. **Social network security: Issues, challenges, threats, and solutions**. Information sciences 421 (2017): 43-69.

[5] Zhang, Zhishuo, and Shijie Zhou**. A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of Mobile Things**. Computer Networks 201 (2021): 108553.

[6] Guo, Zhenzhen, Gaoli Wang, Yingxin Li, Jianqiang Ni, Runmeng Du, and Miao Wang. **Accountable Attribute-Based Data Sharing Scheme Based on Blockchain for Vehicular Ad Hoc Network**. IEEE Internet of Things Journal (2022).

[7] Zhou, Quan, Zhikang Zeng, Kemeng Wang, and Menglong Chen. **Privacy Protection Scheme for the Internet of Vehicles Based on Private Set Intersection**. Cryptography 6, no. 4 (2022): 64.

[8] Clarke, Rebekah. **An Intelligent Client-Centric Framework for Responsive, Privacy Conscious Personalisation.** PhD diss., Trinity College, 2021.

[9] Zhang, Shaobo, Guojun Wang, Qin Liu, and Jemal H. Abawajy. **A trajectory privacy-preserving scheme based on query exchange in mobile social networks**. Soft Computing 22, no. 18 (2018): 6121-6133.

[10] Zhou, Jun, Zhenfu Cao, Xiaolei Dong, and Thanos Vasilakos. **Gtsim-pop: Game theory based secure incentive mechanism and patient-optimized privacy-preserving packet forwarding scheme in m-healthcare social networks**. Future Generation Computer Systems 101 (2019): 70-82.

[11] Cai, Taotao, Jianxin Li, Ajmal Mian, Rong-Hua Li, Timos Sellis, and Jeffrey Xu Yu. **Target-aware holistic influence maximization in spatial social networks**. IEEE Transactions on Knowledge and Data Engineering 34, no. 4 (2020): 1993-2007.

[12] Nabil, Mahmoud, Muhammad Bima, Ahmad Alsharif, Willaim Johnson, Surya Gunukula, Mohamed Mahmoud, and Mohamed Abdallah. **Priority-based and privacy-preserving electric vehicle dynamic charging system with divisible e-payment**. In Smart cities cybersecurity and privacy, pp. 165-186. Elsevier, 2019.

[13] Luo, Entao, Qin Liu, Jemal H. Abawajy, and Guojun Wang. **Privacy-preserving multi-hop profile-matching protocol for proximity mobile social networks.** Future Generation Computer Systems 68 (2017): 222-233.

[14] Ferrag, Mohamed Amine. **Achieving Secure and Privacy-Preserving in Mobile Social Networks**. In Handbook of Research on Cloud Computing and Big Data Applications in IoT, pp. 94-126. IGI Global, 2019.

[15] Huang, Rui, Yichao Lin, Bidi Ying, and Amiya Nayak. **ACP: An efficient user location privacy preserving protocol for opportunistic mobile social networks**. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 1, pp. 610-619. IEEE, 2018.

[16] Jiang, Qingfeng, Kun Deng, Lei Zhang, and Chun Liu. **A privacy-preserving protocol for utility-based routing in DTNs**. Information 10, no. 4 (2019): 128.

[17] Xu, C., Xie, X., Zhu, L., Sharif, K., Zhang, C., Du, X. and Guizani, M., 2020. **PPLS: a privacy-preserving location-sharing scheme in mobile online social networks**. Science China Information Sciences, 63(3), pp.1-11.

[18] Chen, Juan, Shen Su, and Xianzhi Wang. **Towards privacy-preserving location sharing over mobile online social networks.** IEICE TRANSACTIONS on Information and Systems 102, no. 1 (2019): 133-146.

[19] Rashidibajgan, Samaneh, Thomas Hupperich, Robin Doss, and Anna Förster. **Secure and privacy-preserving structure in opportunistic networks**. Computers & Security 104 (2021): 102208.

[20] Hamidian, Ali, U. Korner, and A. Nilsson. **A study of internet connectivity for mobile ad hoc networks in ns 2.** Department of Communication Systems, Lund Institute of Technology, Lund University (2003).

[21] Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. **Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps.** IEEE Transactions on Industrial Informatics 14, no. 11 (2018): 4815-4828.