Ensuring Users Privacy and Mutual Authentication in Opportunistic Networks: A Survey

Cossi Blaise Avoussoukpo, Chunxiang Xu, and Marius Tchenagnon
(Corresponding author: Cossi Blaise Avoussoukpo)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
No.2006, Xiyuan Ave, West High-Tech Zone, Chengdu 611731, Sichuan, China
(Email: omramson@yahoo.fr)

(Received June 8, 2018; Revised and Accepted Oct. 20, 2018; First Online Feb. 16, 2019)

Abstract

The Opportunistic Communication main goal is to use short-term, simple, easy, convenient, and quick actions to communicate when limited or no traditional Communications infrastructure is available. For users' altruism represents the heart of any OppNets, using Communications Technologies such as Bluetooth, Wi-Max, or Wi-Fi to communicate poses not only routing challenges but also users privacy challenges. However, most researches on OppNets domain, focus more on routing security than users mutual authentication and privacy. This work provides a review of the state of the art proposals on users privacy and mutual authentication techniques with three main contributions. First, it clarifies the concept of OppNets. Second, it Points out the differences between OppNets and some communications models that emerged from Mobile Ad hoc Networks research. Third, it succinctly reviews the main existing techniques proposed for users mutual authentication and privacy protection in OppNets, organising them in a taxonomy. Finally, it discusses, the limits of the techniques studied.

Keywords: Mutual Authentication; OppNets; Opportunistic Communication; Privacy Protection

1 Introduction

Hitherto recently, mobile Ad Hoc network has captured the attention of researchers for years. It follows, the advent of Delay Tolerant Networks, Unstructured Networks, and Peer to Peer Communications. However, with the pervasiveness of mobile and fixed smart devices or systems equipped with various kinds of communication media such as Bluetooth, Wired Internet, Wi-Fi, Ham Radio, Satellite, a new type of network based on devices discovery called Opportunistic Networks surfaced. Moreover, the increasing number of mobile smart devices in use, together with the gregarious nature of human mobility, gives not only the idea of the creation of smart city [10, 20, 21] but also opens up the idea to use the mobility of devices for opportunistic communications when mobile devices come into contact. Here, mobility is an opportunity, not a challenge.

Opportunistic Networks [1] as a natural evolution of mobile Ad-Hoc network, are self–configured and made up of diverse systems, not formerly employed as components, which join dynamically to exploit the resources of separate networks according to the needs of a specific application task. Opportunistic Networks do not have an end-to-end path and rely solely on a Seed node (supernode, source node or root note) that invites other nodes called Helpers to form together, the opportunistic networks, whenever needs are. Here, both Seed node and Helpers that form the Opportunistic Network are not predefined, in other words, there are no fixed architectures like other networks to manage the Opportunistic Networks. For users represent the heart of Opportunistic Networks, OppNets can be useful across many domains such as crises management, info-mobility services and intelligent transportations, and pervasive healthcare. However, the wireless communication is not a safe environment [33]. Therefore, operating in OppNets poses not only routing challenges but also users privacy challenges. However, Opportunistic Networks related research tends to focus on routing.

There are various type of surveys on OppNets routing, among others the most useful and recent Nessrine Chacchouk's work [9]. There is less work dedicated to mutual authentication and users privacy for Opportunistic Networks. Meanwhile, users might be reluctant to join an Opportunistic Network if their identity, social links, or location can be compromised when operating in an Opportunistic Network environment. Moreover, due to the user-centric nature of such networks, users mutual authentication, when addresses rigorously can allow more users to join an Opportunistic network with confidence. That justifies the importance of this survey that reviews the state of the art techniques used for users privacy (location, social links, identity) and mutual authentication schemes providing three main contributions. First, it clarifies the concept of OppNets. Second, it Points out the differences between OppNets and some communications models that emerged from Mobile Ad hoc Networks research. Third, it succinctly reviews the main existing techniques proposed for users mutual authentication and privacy protection in OppNets, organising them in a taxonomy. Finally, it discusses, the limits of the techniques studied.

The remainder of this paper goes as follows. Section 2 provides useful definitions. Section 3 clarifies the concept of Opportunistic Networks, characterises OppNets, and Points out the differences between OppNets and some communications models that emerged from Mobile Ad hoc Networks research. Section 4 provides a taxonomy of the most significant existing proposals in the domain of Opportunistic Networks on Users Privacy and Mutual Authentication respectively; describing the most relevant approaches, and discussing their pros and cons. Section 5 provides an insightful summary of the works presented within each class. Finally, Section 6 concludes the paper and gives future research directions.

2 Background

2.1 Multidimensional Scaling

Multidimensional scaling (MDS) is one of several multivariate schemes that study the similarity or distance between two objects (data) which are presented in a low dimensional space.MDS visualises the results to reveal the hidden structure in the data [11]. MDS uses the distance between each pair of the objects as input and generate (2D or 3D)-points as output.

2.2 Bloom Filter

Burton H. Bloom conceived Bloom filter [3] in 1970. Bloom filters are kinds of hash tables, probabilistic space-efficient data structures that verify whether an element is a member of a set [14]. The raison d'être of Bloom filters is that; they are more space-efficient than hash tables, super fast insert and super fast lookups. Bloom filters concede false positive but no false negative. For Broder and Mitzenmacher [6], on any occasion, a list or set is used, and space is case-sensitive, one can resort to Bloom filter if the false positive can be solved.

2.3 Dynamic Clustering

A cluster is a subset of data with common characteristics. Clustering, also called unsupervised learning is the process of making the difference between similar and dissimilar dataset dividing the dataset into groups. As opposed to static clustering, in dynamic clustering, the clusters are formed, and cluster heads are selected [5].

2.4 Opportunistic Network Contact Graph

A contact graph reveals keen pieces of information about social links. Two elements characterise the contact graph G; G={V,E}. V is a set of nodes and E a set of edges [16]. Figure 1 gives an idea of how an opportunistic contact graph can look like.

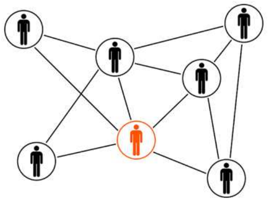

Figure 1: Network contact graph

2.5 K-Anonymity

K-Anonymity is a model for protecting data privacy. It relies on the principle that if at least K people share the same quasi-identifiers in the same table, then no individual can be individually tracked [25].

2.6 Markov Models

Markov models depend on Markov processes that are memoryless chains of events for which the next event depends on the current event but not the past event [17]. Markov models are composed of a set of states, state transition probability, and an initial state distribution. Figure 2 is an example of a Markov model with the states A, B, and C .

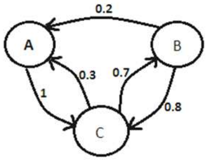

Figure 2: A markov model

2.7 Decisional Bilinear Diffie-Hellman Problem

Let $\mathbb{G}$, $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p, g a generator of $\mathbb{G}$ and e, a bilinear map; $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let x,y,z,$c \in \mathbb{Z}_p$ be randomly chosen. The Decisional Bilinear Diffie-Hellman (DBDH) assumption [26] holds in $\mathbb{G}$ if no probabilistic polynomial-time algorithm can distinguish the tuples (g , g^x,g^y,g^z , $e(g,g)^{(xyz)}$) from the tuple (g , g^x,g^y,g^z , g^c) with non-negligible advantage [30].

2.8 Identity-Based Cryptography

Shamir [27] was the first person to propose the idea of Identity-Based Cryptography (IBC) in 1984. IBC main goal was to simplify the certification management of conventional PKI supported security schemes. However, it was until 2001 that Boneh and Franklin introduced the first practical solution of IBC based on the Diffie-Hellman Problem from Weil pairing. An IBC scheme is made up of four randomised algorithms [4].

Setup : Generate the master secret key S and the system parameters.

Extract : Given a user's identity, generate the corresponding private key by using the master secret key.

Encrypt : To encrypt a message m for a user, take the user's identity and m as input, and generate the corresponding ciphertext.

Decrypt : To decrypt a ciphertext c, take the user's private key and c as input, and recover the corresponding message.

2.9 Threshold Secret Sharing

Threshold secret sharing allows a secret to be shared among multiple parties or users in such a way that only a sufficient number of users together can reconstruct the secret.

2.10 Mutual Authentication

Generally, authentication is the process of establishing an identity; the process of proving that a user or a process is, who or what it claims to be. Mutual authentication, also called two-way authentication refers to two parties authenticating each other at the same time [23, 32]. In a Network, TLS and mTLS are examples of mutual authentication protocols.

3 Opportunistic Networks

3.1 What are Opportunistic Networks (OppNets)?

Leszek Lilien *et al.* were the first to clearly and formally define the concept of Opportunistic Networks (OppNets) [1]. Opportunistic Networks, characterised as the most challenging evolution of mobile Ad hoc Networks rely on limited or no infrastructure. Opportunistic Networks are self–configured and made up of diverse systems, not employed initially as components, which join dynamically to exploit the resources of separate networks according to the needs of a specific application task. Opportunistic Networks do not have an end-to-end path and rely solely on a Seed node(s) (Supernode(s) or Source node(s)). The Seed node(s) or Seed OppNet is an essential part of OppNets for everything starts with the Seed OppNet that expands by inviting other nodes called Helpers [31].

3.2 Significant Differences between OppNets and other Networks

The first and most important fact to understand is that most people mistake Opportunistic Communications For OppNets. Although nodes within an OppNets also communicate opportunistically, the "Opportunistic" referred to by other Networks is limited because for opportunistic communication to happen, devices wait till they are in each other range. In contrast, OppNets should realise opportunistic growth and opportunistic use of resources acquired by this opportunistic growth. Second, Delay Tolerant Networks routing algorithms, always look for an existing end to end route first. If there is no end to end route, Delay Tolerant Networks routing algorithms resort to opportunistic communications. On the other hand, for OppNets, messages are always sent opportunistically, and an existing end to end path is never considered.

3.3 Important Applications for OppNets

OppNets can be useful in all emergency situations, healthcare, and military. For example, OppNets can effectively and efficiently; help inform people before a disaster, organise rescue operation during and after a disaster [24, 29]. Also, With an ageing society, and people living in remote areas with no access to proper medical facilities, people with chronic medical conditions [2] can enjoy remote healthcare assistance. Moreover, OppNets can be useful in the military for security operations.

3.4 Users Privacy Challenges in OppNets

Users are at the heart of OppNets for users are the ones who carry devices. So, users privacy and devices privacy are related. The most critical users privacy challenges for OppNets are Helpers privacy and OppNet privacy on the one hand, and authentication and mutual authentication of nodes within an OppNet on the other hand.

4 Taxonomy of Users Privacy and Mutual Authentication in OppNets

Since the advent of OppNets that is a natural evolution of Mobile Ad Hoc Networks, Researchers have achieved great things to advance the new domain of research, OppNets. However, research works tend to focus more on routing; there are even many surveys on routing in OppNets. Moreover, mutual authentication within an OppNet on the one hand, users privacy, on the other hand, get less attention. Meanwhile, within such a hostile environment like OppNets, these questions are worth to consider. The following sections provided a succinct review of the existing literature based on the proposed taxonomy which is schematically illustrated in Figure 3 and sorted in Table 1.

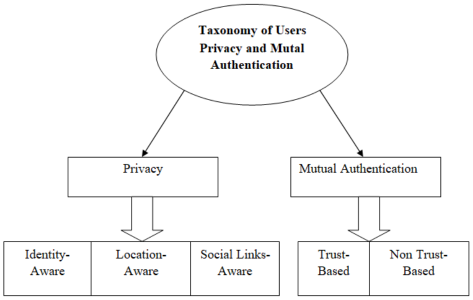

Figure 3: Taxonomy of users privacy and mutual authentication proposals for OppNets

Table 1: Users privacy and mutual authentication schemes taxonomy

schemes	schemes
Users Privacy	Mutual Authentication
Social Links Aware	Trust-Based
Distl [13]	Cao [7]
Distl [12]	Singh [28]
Location Aware	Non-Trust-Based
Zakhary [34]	Ma [22]
Zakhary [35]	Carver [8]]
Identity Aware	Guo [15]]
Kaur [18]	Kumar [19]]

4.1 Mutual Authentication in OppNets

Before two nodes enter an OppNet environment, they register at the Seed OppNet. They resort to mutual authentication before engaging in communication. Two classes of mutual authentication techniques are considered in this study: Non Trust-Based and Trust-Based. The literature on this topic is limited for it is a relatively new domain of research.

4.1.1 Trust-Based Mutual Authentication

Xiamei and Ying [7] proposed an authentication scheme based on trust and rooted on Multidimensional scaling. Their scheme depends on a trust model called M-Trust that relies on an integrate trust value $\mathbb{Q}_\alpha^\beta$ obtained by combining direct and indirect trust values. First of all, each node generates its private key; a root node participates slightly in that process. Also, each node sets the relationship intensity threshold δ. When two nodes α and β come into contact, α queries the local repository, calculate the integrate trust value. Then, after considering the value-at-risk, the node β can get a certificate from α if $\mathbb{Q}_\alpha^\beta \leq \delta$. The proposed scheme is an excellent job for it meets most of the requirements of the opportunistic networks. However, the root node(seed OppNet) does play a third party role which is not desirable for OppNets. Umesh Pal Singh and Naveem Chauhan [28] proposed an authentication scheme for opportunistic communication within a trust framework. The proposed scheme is a variant of Ming Huang Guo's work. Here, the authors added to Guo's work, the notion of dynamic registration where ordinary authenticated nodes become semi-super nodes. Seed node or static nodes appoint authenticated nodes as demi-super nodes by their trust and threshold values. The trust value depends on two parameters; encounter value and number of messages. Nevertheless, the trust value does not serve much in the process of mutual authentication.

4.1.2 Non-Trust-Based Mutual Authentication

Ma and Jamalipour [22] combined both (t, n) Threshold Secret Sharing and Identity-Based Cryptography and proposed a scheme that aims to mitigate malicious attacks through opportunistic nodes authentication. The proposed scheme considered the use of (t, n) secret sharing to solve not only the key escrow problem of Identity-Based Cryptography but also the single point of failure of PKG. Any node that is waiting for authentication must reveal its unique and unchangeable identity that could be its IP address, MAC address or a combination of them. Afterwards, the authenticating node, from direct encounters of t unique PKGs can reconstruct its private key. In the process of getting its private key, the authenticating node should forward both its identity and a self- generated public key to an encountered PKG. Also, Authors evaluated the delay performance of their scheme, studying, on the one hand, the trade-off between security and reliability, and on the other hand the trade-off between security and convenience. Although the proposed scheme can solve major issues such as key escrow problem and single point of failure, how to choose n PKGs, remain a crucial problem for resorting to a third party may raise other concerns.

Christ and Xiaodong [8] proposed a scheme that, with Opportunistic Networking, a mobile phone user finds friends nearby, using both Bluetooth and 3G technologies. Here, friends' identity privacy is protected. The proposed scheme uses three phases to notify friends nearby: system initialisation, notification generation and opportunistic forwarding, notification receiving. A trusted party does the system initialisation. Any user that wants to discover proximity friends must contact the trusted party for authentication. Afterwards, the user sends a packet notification with a time to live to friends. Upon reception and verification of the packet notification, friends choose at will to join the packet sender. For Christ and Xiaodong 'scheme is based on the Decisional Bilinear Diffie-Hellman problem, the proposed scheme is semantically secure under chosen plaintext attack. The scheme performance

Table 2: Users privacy and mutual authentication proposals overview

schemes	Year	Type	Techniques	Pros	Cons
Ma [22]	2010	Authentication	Threshold Secret Sharing+Identity-Based Cryptography	Solve the Key Escrow problem and the Single Point of Failure.	Third Party issue.
Guo [15]	2015	Authentication	Cryptography Principles	Uses Simple Cryptography Principles. Achieves Privacy	Registration at Seed node
Kumar [19]	2017	Authentication	RSA+ Diffie-Hellman Key exchange Protocol	Designed after Guo [15]	Third-party issue
Cao [7]	2014	Authentication	Trust+Multidimensional scaling	Users are considered	Third-party issue
Singh [28]	2017	Authentication	Trust Framework+Guo [15]	Use of Trust Framework	Third-party issue
Carver [8]	2012	Authentication	Decisional Bilinear Diffie-Hellman problem	Achieves Privacy	Third-party issue
Distl [13]	2014	Social Links protection	Contact Graph	Satisfactory result after simulation	Does not scale to more massive graphs
Distl [12]	2015	Social Links protection	Bloom Filter	Satisfactory result after simulation	Designed for free routing
Zakhary [34]	2012	Location protection	Social Links+ K Anonymity technique	Satisfactory result after simulation	The Social Links Problem
Zakhary [35]	2013	Location protection	K-Anonymity technique, lightweight Markov-based location prediction model	Satisfactory result after simulation	The Social Links Problem
Kaur [18]	2015	Identity protection	Dynamic Clustering	Dynamic Concept	Clustering Concept

analysis also shows satisfactory results. However; the role of the trusted party in the scheme is too critical for opportunistic networking aims to promote the direct contact between users.

Ming Huang Guo *et al.* [15] proposed an authentication scheme that also protects users' privacy for Opportunistic Networks. The proposed scheme has two main phases: registration and authentication. Any node or user that wish to communicate with another node should first register at the supernode. The registration process of any unauthenticated node A at the supernode S involves A's virtual identifier ID_a, public key PK_a, secret key SK_a; the supernode's public key $PKsn$, secret key $SKsn$.The supernode uses a symmetric key, an arithmetic function $f()$, and a timestamp Tsn . If the registration is successful, node A can move within the network with its authentication credentials M_j, $f()$, Tsn.

Two nodes A and B that have already completed their registration at the super node can then engage in mutual authentication. The proposed scheme achieves anonymity and privacy due to the techniques used for registration and authentication processes. It also mitigates tapping, forgery, resend, and Man-in-the-middle attacks. Despite an excellent job, the supernode job appears as a major single point of failure. Prashant Kumar *et al.* [19] proposed a scheme for authentication and privacy protection for opportunistic communications. This scheme is a variant of the scheme proposed by Ming Huang Guo *et al.* The proposed scheme stresses the use of RSA and Diffie-Hellman for key generations and key exchange which is useless. Also, the role of the seed node is too much for it generates all the Public and private keys pair for the nodes. The seed node also does the mutual authentication for the nodes because for mutual authentication, nodes look through a list.

4.2 Users Privacy Proposals for OppNets

4.2.1 Social Aware Proposals

An opportunistic contact graph is of great importance for it encoded social information that is used to solve challenging opportunistic networking problems. Considering the trade-off between privacy and utility in the contact graph, Distl and Hossmann [13] proposed a scheme that changes the contact graph by adding and removing edges.

The algorithm works as follows. First, consider an unweighted and undirected contact graph $G = \{V, E\}$ as input. Second, output a modified contact graph G'={V,E'} such that $|E| = |E'|$. Here, it is hard for an attacker operating on a graph level to know any hidden information in $G = \{V, E\}$. Although the proposed algorithm shows satisfactory results, it does not scale to larger contacts graphs. Considering the importance of users for opportunistic networking, and balancing the trade-off between social links and users privacy, Bernhard Distl and Stephan Neuhaus [12] proposed a scheme that uses the social connections to improve performance without revealing users private information.

The key component of the proposed algorithm is Bloom filters that help achieve privacy for users. Here, Authors are interested in pre-established social links. The algorithm detects social links, uses social links for mutual authentication revealing no personal information. The proposed work is an excellent achievement for it found a way to overturn the concern over social connection into an asset that can be available for other applications. However, more attacker models are yet to be studied.

4.2.2 Location Aware Proposals

Zakhary and Radenkovic [34] were principally interested in how location privacy can influence communications in opportunistic networks. To solve the location matter, they resort to social links. Assuming that users trust their social links, the proposed scheme offers location privacy through request/reply location obfuscation techniques. A user (U_a) that wants a location-based service looks for proximate friends and forwards a copy of their request to an available friend (U_b). With a social forwarding protocol, (U_b) will contribute to help (U_a) achieve his goal without revealing its location. However, the social links privacy was not addressed adequately.

The quest for location –privacy in opportunistic mobile social networks [35] is a variant of a previous scheme that Zakhary and Radenkovic designed. The goal is almost the same. Only the techniques differ. Here, Zakhary *et al.* proposed a stochastic model for location prediction using a lightweight Markov model to drive the privacy protection scheme. The scheme depends on the fact that users trust their contact (friends and relatives) in their social network. The scheme detects users' contact and uses it to obfuscate requests and hide the original sender's location from the location-based service. The proposed work is a collaborative and distributed protocol that offers location K anonymity for each node participates in the anonymisation process. Authors' scheme achieves better than many other protocols. Still, social links privacy should also be considered carefully.

4.2.3 Identity Aware Proposals

Motivated by the fact that opportunistic networks could be of great help if privacy is maintained, Kaur and Singh [18]proposed a scheme that protects users' identity. The proposed scheme relies on dynamic clustering. The algorithm follows the following steps. First, it characterises the network with a finite number of nodes, divides the network into clusters, and generates of cluster heads of each cluster. Second, cluster heads store the information of all its neighbouring nodes, and nodes communicate with each other through the cluster heads. Third, each transmission will be formed along with the new cluster heads. Although the use of dynamic clustering enhances the privacy of the network, the notion of the cluster, on the one hand, an the key role of the base station, on the other hand, do not match opportunistic networks characteristics.

5 Summary

This Section, through table 2 provides a concise and insightful summary of the works studied within Mutual Authentication and Users Privacy classes respectively.

5.1 On Mutual Authentication

5.1.1 Basis on Comparing Mutual Authentication Schemes

OppNets are self-configured and depend on little or no infrastructure with the Seed OppNet as a vital component. On the mutual authentication schemes proposed, this paper, not only described the achievement of those proposals but most importantly compared those proposals concerning the role of the Seed OppNet. For OppNets schemes, it is not desirable for the Seed OppNet to play the role of a Central authority or third party. The (Cons) column in Table 2 gives an idea of the degree of involvement of the Seed OppNet for each scheme.

5.1.2 Summary on Mutual Authentication Schemes

From the works studied within Mutual Authentication class, Xiamei and Ying [7], Ma and Jamalipour [22], and Ming Huang Guo *et al.* [15] impacted the domain Significantly. Other proposals are variant of the works in [15]. Ming Huang Guo et. al used general cryptographic principles to demonstrate the mutual authentication. Xiamei and Ying used trust and multidimensional scaling. Ma and Jamalipour on the other hand, used threshold secret sharing and identity-based cryptography.

5.2 On Users Privacy

5.2.1 Basis on Comparison

As challenging as OppNets are, achieving privacy is tantamount to compromising something. Thus, this paper identified what it took for each proposed scheme to achieve their goal. The (Cons) column in Table 2 gives an idea of the compromise made in each users privacy scheme.

5.2.2 Summary on Privacy Schemes

On Identity protection, Kaur and Singh [18] did a remarkable work using dynamic clustering. Zakhary and Radenkovic [34], [35] did the most work on Location protection using social links. On Social links protection, Distl and Hossmann [13] and Distl and Neuhaus [28] did the most work using contact graph and bloom filter respectively.

6 Conclusion and Future Research Directions

This work clarifies the OppNets concept and Points out the differences between OppNets and some communications models that emerged from Mobile Ad hoc Networks research. What's more, this paper provides a comprehensive survey on users Mutual Authentication in OppNets on the one hand; and Location, Identity, and Social links protection within OppNets on the other hand. The different proposals were organised in a taxonomy.OppNets are the most challenging evolution of Mobile Ad hoc Networks research due to their infrastructure-less nature and their ability to expand from a Seed OppNet.For users represent the heart of OppNets, much effort should be put on Mutual Authentication and privacy protection within OppNets. As future works, an existing multipurpose communication system that can be beneficial to OppNets will be studied and presented. Also, a trust-based mutual authentication mechanism will be proposed.

Acknowledgments

This study was supported by the National Key&D Program under the Grant 2017YFB0802000, and the National Natural Science Foundation of China under the Grant 61370203. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. A. Alduailij and L. T. Lilien, "A Collaborative healthcare application based on Opportunistic resource utilization networks with OVM primitives," in *International Conference on Collaboration Technologies and Systems (CTS'15)*, pp. 426–433, 2015.

[2] A. S. Bleda, R. Maestre, A. Jara, "Ambient assisted living tools for a sustainable aging society in modeling and optimization in science and technologies," *New York : Springer*, pp. 193–220, 2014.

[3] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, pp. 422–426, 1970.

[4] D. Boneh and M.Franklin, "Identity-based encryption from the weil pairing," *Advances in Cryptology (Crypto'01)*, LNCS 2139, pp. 213 – 229, 2001.

[5] A. Bouchachia, "Dynamic clustering," *Evolving Systems*, vol. 3, no. 3, pp. 133–134, 2012.

[6] A. Z. Broder and M. Mitzenmacher, "Network applications of bloom filters: A survey," *Internet Mathematics*, vol. 1, no. 4, pp. 485–509, 2003.

[7] X. Cao and Y. Yin, "An identity authentication scheme for opportunistic network based on multidimensional scaling," in *International Conference on Cyber-Enabled*, pp. 87-93, 2014.

[8] C. Carver and X. Lin, "A privacy-preserving proximity friend notification scheme with opportunistic networking," in *IEEE International Conference on Communications*, pp. 5387–5392, 2012.

[9] N. Chakchouk, "Communication Networks," vol. 17, no. 4, pp. 2214–2241, 2015.

[10] M. Conti, F. Delmastro, V. Arnaboldi, "People-centric computing and communications in smart cities," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 122–128, 2016.

[11] T. Cox and M. Cox, "Multidimensional Scaling, 1994. (https://ncss-wpengine.netdna-ssl.com/wp-content/themes/ncss/pdf/Procedures/NCSS/Multidimensional_Scaling.pdf)

[12] B. Dist and S. Neuhaus, "Social power for privacy-protected opportunistic networks," in *7th International Conference on Communication Systems and Networks (COMSNETS'15)*, pp. 1–8, 2015.

[13] B. Distl and T. Hossmann, "opportunistic network contact graphs," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 1–3, 2014.

[14] R. Ganesan, D. Thiyagarajan, "Cryptographically imposed model for efficient multiple keyword-based search over encrypted data in cloud by secure index using bloom filter and false random bit generator," *International Journal of Network Security*, vol. 19, No.3, pp. 413–420, 2017.

[15] M. H. Guo, H. T. Liaw, and M. Y. Chiu, "Authenticating with privacy protection in opportunistic networks Ming-Huang," *EAI International Conference on Heterogeneous, Networking for Quality, Reliability, Security and Robustness (QSHINE'15)*, pp. 375–380, 2015.

[16] T. Hossmann, G. Nomikos, Spyropoulos, and F.Legendre, "Collection and Analysis of Multi-dimensional Network data for Opportunistic Networking research," *Elsevier Computer Communication*, 2012. (http://www.

eurecom.fr/en/publication/3751/detail/collection-and-analysis-of-multi-dimensional-network-data-for-opportunistic-networking-research-1)

[17] C. Hu, F. Al-Ayed and H. Liu, "An efficient practice of privacy implementation: Kerberos and markov chain to secure file transfer sessions," *International Journal of Network Security*, vol. 20, no. 4, pp. 655–663, 2018.

[18] P. Kaur and J. Singh, "Ensuring privacy in opportunistic networks using dynamic clustering," in *International Conference on Advances in Computer Engineering and Applications,*, pp. 866–869, 2015.

[19] P. Kumar, N. Chauhan, and N. Chand, "Authentication with privacy preservation in opportunistic networks," in *Proceedings of the International Conference on Inventive Communication and Computational Technologies (ICICCT'17)*, pp. 183–188, 2017.

[20] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[21] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile Ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2534–2540, June 2008.

[22] Y. Ma, A. Jamalipour, "Opportunistic node authentication in intermittently connected mobile ad hoc networks," in *16th Asia-Pacific Conference on Communications (APCC'10*, pp. 453–457, 2010.

[23] Y. Ma, "NFC communications-based mutual athentication scheme for the internet of things," *International Journal of Network Security*, vol. 19, No.4, pp. 631–638.

[24] R. Martí, A. Martín-Campillo, J. Crowcroft, E. Yoneki, "Evaluating opportunistic networks in disaster scenarios," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 870–880, 2013.

[25] Q. Qian, S. Ni, M. Xie, "Clustering based K-anonymity algorithm for privacy preservation," *International Journal of Network Security*, vol. 19, No. 6, pp. 1062–1071, 2017.

[26] A. Saha and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* pp. 457-473, 2005.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Crptohraphy*, LNCS 196, pp. 47–53, 1985.

[28] U. P. Singh and N. Chauhan, "Authentication using trust framework in opportunistic networks," in *8th International Conference on Computing, Communications and Networking Technologies (ICCCNT'17)*, 2017. (https://ieeexplore.ieee.org/document/8203956)

[29] M. Turoff, "The paradox of emergency management," *Conference–Kristiansand (ISCRAM'15)*, 2015. (https://pdfs.semanticscholar.org/d49c/f309f520312fc55d90d11195cbc84b76c738.pdf)

[30] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[31] Y. Wang, G. Xu, M. Zhang, H. H. Jin, "Research on the topological evolution of uncertain social relations in opportunistic networks," in *IEEE 1st International Conference on Edge Computing*, 2017. (https://ieeexplore.ieee.org/document/8029276)

[32] C. H. Wei, M. S. Hwang, A. Y. H. Chin, "A mutual authentication protocol for RFID", *IEEE IT Professional*, vol. 13, no. 2, pp. 20–24, Mar. 2011.

[33] C. Y. Yang, J. S. Chen, M. S. Hwang, "The capacity Analysis in the Secure cooperative communication System," *International Journal of Network Security*, vol. 19, no. 6, pp. 863–869, 2017.

[34] S. Zakhary, M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in *IEEE International Conference on Communications (ICC'12)*, pp. 1059–1063, 2012.

[35] S. Zakhary, M. Radenkovic and A. Benslimane, "The quest for location-privacy in opportunistic mobile social networks," in *9th International Wireless Communications and Mobile Computing Conference (IWCMC'13)*, vol. 667-673, 2013.

Biography

Cossi Blaise Avoussoukpo is currently a PhD candidate at the University of Electronic Science and Technology of China (UESTC). His research area includes Wireless communications, Opportunistic communications, Cryptography, and Information security.

Chunxiang Xu received her PhD degree from Xidian University in 2004, in P.R.China.She is currently a Professor at the University of Electronic Science and Technology of China (UESTC). Her research area includes cloud computing security, cryptography and information security. She is a member of the IEEE organisation.

Marius Tchenagnon received his MSc degree in computer science from the University of Electronic Science and Technology of China (UESTC). His research area includes Wireless Communications. Opportunistic Communication, cryptography and information security.