Key Management for Secure Network Coding-enabled Mobile Small Cells

Marcus de Ree[1,2], Georgios Mantas[1,3], Ayman Radwan[1], Jonathan Rodriguez[1,2], and Ifiok Otung[2]

[1] Instituto de Telecomunicações, Aveiro, Portugal
[2] University of South Wales, Pontypridd, UK
[3] Faculty of Engineering and Science, University of Greenwich, UK
{mderee, gimantas, aradwan, jonathan}@av.it.pt
ifiok.otung@southwales.ac.uk

Abstract. The continuous growth in wireless devices connected to the Internet and the increasing demand for higher data rates put ever increasing pressure on the 4G cellular network. The EU funded H2020-MSCA project "SECRET" investigates a scenario architecture to cover the urban landscape for the upcoming 5G cellular network. The studied scenario architecture combines multi-hop device-to-device (D2D) communication with network coding-enabled mobile small cells. In this scenario architecture, mobile nodes benefit from high transmission speeds, low latency and increased energy efficiency, while the cellular network benefits from a reduced workload of its base stations. However, this scenario architecture faces various security and privacy challenges. These challenges can be addressed using cryptographic techniques and protocols, assuming that a key management scheme is able to provide mobile nodes with secret keys in a secure manner. Unfortunately, existing key management schemes are unable to cover all security and privacy challenges of the studied scenario architecture. Certificateless key management schemes seem promising, although many proposed schemes of this category of key management schemes require a secure channel or lack key update and key revocation procedures. We therefore suggest further research in key management schemes which include secret key sharing among mobile nodes, key revocation, key update and mobile node authentication to fit with our scenario architecture.

Keywords: 5G, Security, Privacy, Key Management, Mobile Small Cells, Network Coding, D2D Communications.

1 Introduction

It has been almost a decade since the 4G mobile network was first introduced. Since that time, many more users and devices joined the network. Not only are our smartphones using the 4G network, but also the rapidly increasing number of devices within the Internet of Things (IoT) concept [1, 2]. Furthermore, since the introduction

of the 4G mobile network, the mobile data volume has risen immensely. It is expected that by 2021 the number of wireless devices connected to the network is 100 to 10,000 [3] times higher, and the volume of mobile data is 1,000 times higher [3, 4]. This surge puts a lot of pressure on the current 4G network, which has to share its resources among the growing number of devices. This also causes a reduction in data rates and increases latency.

To address these challenges, new technologies are emerging to create the next generation 5G network [5, 6, 7, 8, 9]. These new technologies will deliver higher network capacity, allow the support of more users, lower the cost per bit, enhance energy efficiency, and provide the adaptability to introduce future services and devices. It is envisioned that this new 5G network will be deployed by 2020 and beyond [3, 5, 6, 10], with data rates reaching speeds going up to 10 Gb/s, and reduces the latency to delays as low as 1 millisecond end-to-end [10].

One approach of increasing throughput inside the 5G network is by utilizing network coding. Network coding is an emerging network technology, which no longer treats data, moving through the network from sender to receiver, as commodities. Traditional routers inside a network can duplicate and forward incoming data packets, but network coding allows multiple packets at a router to be encoded together, before being forwarded. The concept of network coding was first introduced in [11]. It is an emerging communication paradigm that has the potential to provide significant benefits to networks in terms of bandwidth, energy consumption, delay and robustness to packet losses [12, 13, 14].

Another emerging technology for the 5G network is small cells. The small cell technology is the most effective solution to deliver ubiquitous 5G services in a cost-effective and energy efficient manner to its users. In particular, mobile small cells are proposed to cover the urban landscape and can be set up on-the-fly, based on demand, using mobile devices (i.e., user equipment) or Remote Radio Units (RRUs) [15]. Moreover, mobile small cells are networks consisting of mobile devices which are within relative close proximity to one another and thus, it allows device-to-device (D2D) communications that enable high data rate services such as video sharing, gaming and proximity-aware social networking. Consequently, end-users are provided with this plethora of 5G broadband services while the D2D communications improves throughput, energy efficiency, latency and fairness [16, 17].

This paper investigates, in terms of security and privacy challenges, a scenario architecture of the EU funded H2020-MSCA project “SECRET” [18] focused on secure network coding-enabled mobile small cells, and explores how existing key management schemes can provide security and privacy in a similar architecture. This will form the basis for designing novel key management schemes that can support efficiently and effectively existing and new integrity schemes against pollution attacks in network coding-enabled mobile small cells. The proposed schemes are expected to provide robust and low complexity key management including secret key sharing among mobile nodes, key revocation, key update, and mobile node authentication.

2 Scenario Architecture

We present a scenario architecture of the EU funded H2020-MSCA project "SECRET" [18] focused on secure network coding-enabled mobile small cells. In this scenario architecture, the technologies of mobile small cells, network coding and D2D communications are combined, as illustrated in Fig. 1. The cellular network, consisting of macro cells, is broken down into mobile small cells. Each mobile small cell is controlled by a hotspot (or cluster-head). This is a mobile node (device) within the cluster of mobile nodes that is selected to become the local radio manager to control and maintain the cluster. In addition, the hotspots of the different clusters are controlled by a centralized software-defined controller. Through cooperation these hotspots form a wireless network of mobile small cells that have several gateways/entry points to the mobile network using intelligent high-speed connections [19, 20]. Data traffic between mobile nodes is established through D2D communications, and optimized by utilizing network coding.

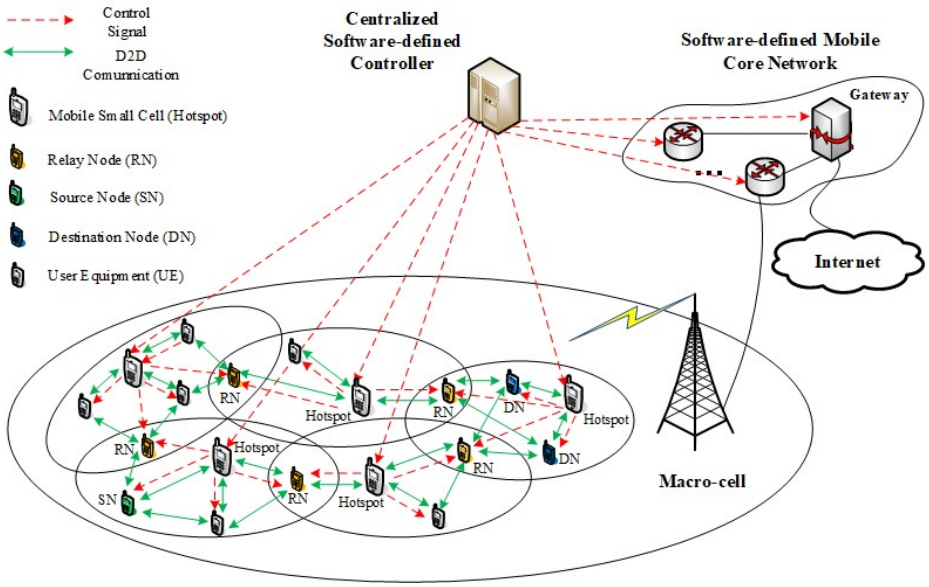

Fig. 1. Scenario Architecture

Suppose that a mobile node wishes to share a multimedia file with two other mobile nodes. The mobile node in possession of the multimedia file, the source node (SN), sends this file to the mobile nodes requesting the file, the destination nodes (DNs). Note that these mobile nodes are not required to be in the same mobile small cell, as illustrated in Fig. 1. Through D2D communications, the multimedia file – using multiple hops – is being routed by mobile nodes, through the network of mobile small cells from the SN to the DNs.

This architecture has multiple advantages, compared to the currently employed architecture. By allowing multi-hop D2D communications through a network of mobile small cells, data traffic within this scenario is no longer required to be routed through the base station (BS). This means that the data is no longer required to travel the long distances to and from the BS, but has a more direct route. This significantly reduces latency. Since the transmissions travel shorter distances, the transmissions require less power to reach its destination. This means that this architecture also allows data transmission to be more energy efficient. This architecture also reduces the workload of the BS, which relieves stress on the cellular network.

3 Security and Privacy Challenges

The proposed architecture brings a set of new technologies together, and with that it also comes with a number of security and privacy challenges. This section will explore this kind of challenges that every individual technology poses in our proposed architecture.

3.1 Multi-hop wireless network

Allowing data packets in transmission to traverse multiple hops to reach the intended receiver, brings a spectrum of privacy threats. These privacy threats can be split into two categories, data privacy and identity privacy. Data privacy threats cover all attacks in which the attacker tries to uncover information about the data transmitted to the intended receiver. The attacker uses techniques such as eavesdropping and identity impersonation. These attacks are well studied and various cryptographic techniques have been developed to prevent these attacks from being effective. These cryptographic techniques are able to provide data confidentiality using data encryption schemes, entity authentication using identification schemes, and data authentication using signature schemes. These techniques counter all the aforementioned challenges. However, many of these countermeasures require both the sender and the intended receiver to be in possession of a shared cryptographic key. Thus, it is obvious that key management plays a critical role to achieve data privacy [21, 22].

Identity privacy is the other category of privacy threats in a multi-hop wireless network. The challenge of providing identity privacy lies in the establishment of secure communication between two mobile nodes. To establish secure communication between two mobile nodes, both nodes are required to prove their identity to each other. This requirement prevents any attacker from using an impersonation attack. However, both mobile nodes wish to remain anonymous to the intermediate nodes routing the identifying information. This challenge can be solved with anonymous mutual authentication. With anonymous mutual authentication, both mobile nodes participate in an interactive zero-knowledge proof of identity protocol. This protocol involves exchanging challenges to prove their identity to each other, without actually sending any private identifying information. However, all zero-knowledge proof of identity protocols either require both mobile nodes to have a pre-established secret, or

depends on a Trusted Third Party (TTP). This TTP is a central control point that every node in the network trusts, but does not fit in our proposed architecture due to the lack of infrastructure. Both mobile nodes are therefore required to have a pre-established secret (such as a shared cryptographic key) in order to communicate [22, 23].

3.2 Network coding-enabled network

A network coding-enabled network allows the encoding of data packets at routers inside the network, and decoding at the receiver's end. This provides significant benefits to networks in terms of bandwidth, energy consumption, delay and robustness to packet losses. Despite these tremendous advantages, networks utilizing network coding technology are vulnerable to the so-called pollution attack. In this attack, a malicious adversary controls a router such that it can mutate data packets by introducing pollution in the original data packet. Network coding causes this pollution to spread downstream by encoding proper data packets with polluted data packets. This leads to the inability to properly decode and retrieve the information at the intended receivers. A successful pollution attack wastes a lot of costly network resources. The challenge posed by this attack is similar to the vulnerability of data modification in any wireless network. Data integrity is required to prevent any polluted data packets from being transmitted further through the network. The research community proposed various integrity schemes [24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34] to solve this problem. However, the efficiency and effectiveness of the integrity schemes are closely related to the key management schemes which are responsible for the generation, distribution, use and update of the cryptographic keys used by the integrity schemes. In the literature, there are various proposed schemes for key distribution which are used in network coding-enabled networks, but they suffer from drawbacks that limit their effectiveness and reliability [28, 29]. Therefore, it is of utmost importance the design of novel key management schemes that can overcome the limitations and drawbacks of the existing key management schemes in order to support efficiently and effectively existing and new integrity schemes against pollution attacks in network coding-enabled mobile small cells.

3.3 Device-to-Device communications

Device-to-Device (D2D) communications bring into the studied scenario architecture a number of security and privacy challenges. The sole introduction of D2D communications poses challenges when it comes to location privacy. Location privacy is a challenge, since data transmissions between mobile nodes requires close proximity. This allows colluding users to perform a boundary attack to locate nearby mobile nodes. One promising work [35] applied homomorphic encryption to privately identify whether friends are within a nearby distance without revealing the actual user identities. To find out the overall perception when it comes to location privacy, the Princeton Survey Research Associates International held a survey in 2013 and found that 46% of teen users and 35% of adults turn off location tracking features due to privacy concerns [36]. These privacy concerns need to be addressed so that users will allow

their devices to be discoverable and participate in content delivery through D2D communications. Fortunately, location privacy can be protected by using identity preserving techniques such as anonymous mutual authentication [22].

Furthermore, in combination with a multi-hop wireless network, D2D communications also brings data privacy challenges (e.g. eavesdropping) along with identity privacy (e.g. identity impersonation) and free-riding issues in the studied scenario architecture [22]. As previously discussed in Section 3.1, data privacy can be protected with the use of cryptographic techniques, where the role of key management is of utmost importance, whereas identity privacy can be protected by using techniques such as anonymous mutual authentication. In addition, free-riding means that a selfish mobile device is unwilling to send content to others, while it is still receiving demanded data, for the purpose of saving energy. Free-riding reduces fairness and transmission availability within the network. Thus, a stimulating cooperation mechanism is necessary to prevent free-riding within the network, and several solutions have been proposed to solve this problem [37, 38, 39, 40, 41].

3.4 Mobile small cells

The introduction of mobile small cells in the studied scenario architecture makes the network dynamic. Every mobile node inside the network is allowed to constantly be on the move. Certain mobile nodes could leave the macro cell, and other mobile nodes could join the macro cell. This network therefore has a constantly changing topology and thus, it poses a problem when it comes to key management. Traditional certificate-based public key cryptography (CB-PKC) relies on a trusted third party called a certifying authority (CA). The CA issues certificates to users inside the network. These certificates are used to verify the identity and provide a cryptographic key at the same time. This CA can be interpreted as the key manager, and it is a central control point that every node in the network trusts. However, a CA does not fit in the studied scenario architecture due to the lack of infrastructure [42, 43]. On the other hand, identity-based public key cryptography (IB-PKC) removes the requirement of certificates, since public keys in IB-PKC are equal to the identity of the mobile nodes. However, private keys are obtained from the Key Generation Center (KGC). KGC holds a master key from which it generates private keys. Consequently, a compromised KGC means that the entire system is compromised. This means that IB-PKC suffers from a single point of failure, along with the key escrow problem [44]. Finally, certificateless public key cryptography (CL-PKC) is introduced to solve these issues. With CL-PKC, private keys are constructed by both the KGC and the mobile user requesting the private key. The KGC generates the first part of the private key, and the mobile user completes the private key by combining it with his own private key. The tasks of the KGC can be distributed among mobile nodes using verifiable secret sharing [45]. A compromised KGC using CL-PKC only provides the attacker with partial private keys. CL-PKC not only solves the single point of failure and the key escrow problem, but it can also satisfy the dynamic topology of the network. Certificateless key management schemes therefore seem a good candidate for the studied scenario architecture, however many proposed schemes still suffer from

the private key distribution problem, or they lack key update or key revocation procedures.

4 Cryptographic Security Solutions

Having explored the challenges which are brought forth by the studied scenario architecture, this section discusses how these challenges can be solved. By allowing our scenario architecture to perform multi-hop D2D communication, a spectrum of security and privacy challenges arise. However, cryptographic techniques and anonymous mutual authentication are able to provide secrecy and anonymity. Parties wishing to communicate securely require a shared cryptographic key to take advantage of the cryptographic techniques and anonymous mutual authentication. Key management schemes are responsible for the generation, distribution, storage, use, revocation, and update of these cryptographic keys. It is therefore important to investigate the design of novel key management schemes that fit with our scenario architecture and provide all these functionalities in an efficient and effective manner.

Moreover, to fully exploit the advantages of network coding in our scenario architecture, novel key management schemes are required as most of the existing ones are not able to fully support the data integrity schemes proposed in the literature to prevent pollution attacks in network coding–enabled networks.

In addition, the security of mobile small cells is also affected by key management. The dynamic topology that mobile small cells bring to our scenario architecture poses the challenge of a suitable family of key management schemes. As discussed, CB-PKC and IB-PKC, and their respective key management schemes are not suitable. On the other hand, CL-PKC and certificateless key management schemes seem to be a good candidate. However, existing certificateless key management schemes either lack key update or key revocation procedures, or they require a safe channel for (partial) key distribution which is difficult to realize in our scenario architecture [43].

Therefore, it is of the utmost importance to design novel (certificateless) key management schemes for our scenario architecture. These schemes should provide robust and low complexity key management including secret key sharing among mobile nodes, key revocation, key update and mobile node authentication. Finally, they should also support existing and new integrity schemes against pollution attacks in network coding-enabled mobile small cells in an efficient and effective manner.

5 Conclusion

The studied scenario architecture is suitable to cover the urban landscape of high speed 5G mobile communication. This new scenario architecture exploits the advantages of D2D multi-hop communication and network coding-enabled mobile small cells. However, combining these technologies come with security and privacy challenges. For each technology, we explored their respective security and privacy challenges. We found that there are solutions against the identified security and privacy challenges assuming that there exists a key management scheme able to support cryp-

tographic techniques and protocols in an efficient and effective manner. However, no key management schemes seem to exist which satisfy all the requirements necessary to support all cryptographic techniques and protocols to ensure security and privacy in our scenario architecture. It is therefore of the utmost importance the design of novel key management schemes that can provide robust and low complexity key management including secret key sharing among mobile nodes, key revocation, key update, and mobile node authentication.

Acknowledgments

This research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-ITN-2016-SECRET-722424.

References

1. Ericsson: More than 50 Billion Connected Devices (white paper), (2011).
2. Cisco: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 (white paper), (2017).
3. Hossain, E., Hasan, M.: 5G Cellular: Key Enabling Technologies and Research Challenges. IEEE Instrumentation Measurement Magazine 18(3), 11-21 (2015).
4. Nokia Siemens Networks: 2020: Beyond 4G Radio Evolution for the Gigabit Experience (white paper), (2011).
5. Wang, C., Haider, F., Gao, X., You, X., Yang, Y., Yuan, D., Aggoune, H., Haas, H., Fletcher, S., Hepsaydir, E.: Cellular Architecture and Key Technologies for 5G Wireless Communication Networks. IEEE Communications Magazine 52(2), 122-130 (2014).
6. Chih-Lin, I., Rowell, C., Han, S., Xu, Z., Li, G., Pan, Z.: Toward Green and Soft: A 5G Perspective. IEEE Communications Magazine 52(2), 66-73 (2014).
7. Bangerter, B., Talwar, S., Arefi, R., Stewart, K.: Networks and Devices for the 5G Era. IEEE Communications Magazine 52(2), 90-96 (2014).
8. Sucasas, V., Mantas, G., Rodriguez, J.: Security Challenges for Cloud Radio Access Networks. In: Backhauling/Fronthauling for Future Wireless Systems, pp. 195-211. Wiley, Chichester (2016).
9. Mantas, G., Komninos, N., Rodriguez, J., Logota, E., Marques, H.: Security for 5G Communications. In: Fundamentals of 5G Mobile Networks, pp. 207-220. John Wiley & Sons, Chichester (2015).
10. Andrews, J., Buzzi, S., Choi, W., Hanly, S., Lozano, A., Soong, A., Zhang, J.: What Will 5G Be?. IEEE Journal on Selected Areas in Communications 32(6), 1065-1082 (2014).
11. Ahlswede, R., Cai, N., Li, R., Yeung, R.: Network Information Flow. IEEE Transactions on Information Theory 46(4), 1204-1216 (2000).
12. Esfahani, A., Mantas, G., Rodriguez, J., Neves, J: An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks. International Journal of Information Security 16(6), 627-639 (2017).
13. Iqbal, M., Dai, B., Huang, B., Hassan, A., Yu, S.: Survey of network coding-aware routing protocols in wireless networks. Journal of Network and Computer Applications 34(6), 1956-1970 (2011).

14. Chachulski, S., Jennings, M., Katti, S., Katabi, D.: Trading Structure for Randomness in Wireless Opportunistic Routing. SIGCOMM Computer Communication Review 37(4), 169-180 (2007).
15. Radwan, A., Rodriguez, J.: Cloud of Mobile Small-cells for Higher Data-rates and Better Energy-efficiency. In: European Wireless 2017; 23th European Wireless Conference, pp. 105-109. VDE, Dresden, Germany (2017).
16. Asadi, A., Wang, Q., Mancuso, V.: A Survey on Device-to-Device Communication in Cellular Networks. IEEE Communications Surveys & Tutorials 16(4), 1801-1819 (2014).
17. Zhang, Y., Pan, E., Song, L., Saad, W., Dawy, Z., Han, Z.: Social Network Aware Device-to-Device Communication in Wireless Networks. IEEE Transactions on Wireless Communications 14(1), 177-190 (2015).
18. SECRET Homepage, http://h2020-secret.eu/index.html, last accessed 2018/05/05.
19. Gupta, A., Jha, R.: A Survey of 5G Network: Architecture and Emerging Technologies. IEEE Access 3, 1206-1232 (2015).
20. Chou, S., Chiu, T., Yu, Y., Pang, A.: Mobile Small Cell Deployment for Next Generation Cellular Networks. In: Global Communications Conference (GLOBECOM), pp. 4852-4857. IEEE, Austin, TX, USA (2014).
21. Haus, M., Waqas, M., Ding, A., Li, Y., Tarkoma, S., Ott, J.: Security and Privacy in Device-to-Device (D2D) Communication: A Review. IEEE Communications Surveys & Tutorials 19(2), 1054-1079 (2017).
22. Zhang, A., Lin, X.: Security-Aware and Privacy-Preserving D2D Communications in 5G. IEEE Network 31(4), 70-77 (2017).
23. Lu, L., Han, J., Liu, Y., Hu, L., Huai, J., Ni, L., Ma, J.: Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps. IEEE Transactions on Parallel and Distributed Systems, 19(10), 1325-1337 (2008).
24. Kim, M., Lima, L., Zhao, F., Barros, J., Medard, M., Koetter, R., Kalker, T., Han, K.: On Counteracting Byzantine Attacks in Network Coded Peer-to-Peer Networks. IEEE Journal on Selected Areas in Communications 28(5), 692-702 (2010).
25. Esfahani, A., Mantas, G., Yang, D., Nascimento, A., Rodriguez, J., Neves, J.: Towards Secure Network Coding-Enabled Wireless Sensor Networks in Cyber-Physical Systems. In: Cyber Physical Systems: From Theory to Practice, pp. 395-414. CRC Press, Boca Raton, FL, USA (2015).
26. Esfahani, A., Yang, D., Mantas, G., Nascimento, A., Rodriguez, J.: Dual-Homomorphic Message Authentication Code Scheme for Network Coding-Enabled Wireless Sensor Networks. International Journal of Distributed Sensor Networks 11(7), 1-10 (2015).
27. Esfahani, A., Mantas, G., Rodriguez, J., Nascimento, A., Neves, J.: A Null Space-based MAC Scheme against Pollution Attacks to Random Linear Network Coding. In: International Conference on Communication Workshop (ICCW), pp. 1521-1526. IEEE, London, UK (2015).
28. Wu, X., Xu, Y., Yuen, C., Xiang, L.: A Tag Encoding Scheme against Pollution Attack to Linear Network Coding. IEEE Transactions on Parallel and Distributed Systems 25(1), 33-42 (2014).
29. Zhang, P., Jiang, Y., Lin, C., Yao, H., Wasef, A., Shen, X.: Padding for Orthogonality: Efficient Subspace Authentication for Network Coding. In: 2011 Proceedings IEEE INFOCOM, pp. 1026-1034. IEEE, Shanghai, China (2011).
30. Esfahani, A., Mantas, G., Rodriguez, J.: An Efficient Null Space-Based Homomorphic MAC Scheme Against Tag Pollution Attacks in RLNC. IEEE Communications Letters 20(5), 918-921 (2016).

31. Esfahani, A., Mantas, G., Silva, H., Rodriguez, J., Neves, J.: An Efficient MAC-based Scheme against Pollution Attacks in XOR Network Coding-Enabled WBANs for Remote Patient Monitoring Systems. EURASIP Journal on Wireless Communications and Networking 2016(113), 1-10 (2016).
32. Yang, D., Esfahani, A., Mantas, G., Rodriguez, J.: Jointly Padding for Subspace Orthogonality against Tag Pollution. In: 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 85-89. IEEE, Athens, Greece (2014).
33. Esfahani, A., Yang, D., Mantas, G., Nascimento, A., Rodriguez, J.: An Improved Homomorphic Message Authentication Code Scheme for RLNC-Enabled Wireless Networks. In: 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 80-84. IEEE, Athens, Greece (2014).
34. Esfahani, A., Mantas, G., Monteiro, V., Ramantas, K., Datsika, E., Rodriguez, J.: Analysis of a Homomorphic MAC-based Scheme against Tag Pollution in RLNC-Enabled Wireless Networks. In: 20th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 156-160. IEEE, Guildford, UK (2015).
35. Mu, B., Bakiras, S.: Private Proximity Detection for Convex Polygons. Tsinghua Science and Technology 21(3), 270-280 (2016).
36. Zickuhr, K.: Location-based services, http://www.pewinternet.org/2013/09/12/location-based-services/, last accessed 2018/03/13.
37. Li, Z., Shen, H.: Game Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing 11(8), 1287-1303 (2012).
38. Chen, T., Zhu, L., Wu, F., Zhong, S.: Stimulating Cooperation in Vehicular Ad Hoc Networks: A Coalitional Game Theoretic Approach. IEEE Transactions on Vehicular Technology 60(2), 566-579 (2011).
39. Sun, J., Chen, X., Zhang, J., Zhang, Y., Zhang, J.: SYNERGY: A Game-Theoretical Approach for Cooperative Key Generation in Wireless Networks. In: 2014 Proceedings IEEE INFOCOM, pp. 997-1005. IEEE, Toronto, ON, Canada (2014).
40. Chen, X., Proulx, B., Gong, X., Zhang, J.: Exploiting Social Ties for Cooperative D2D Communications: A Mobile Social Networking Case. IEEE/ACM Transactions on Networking 23(5), 1471-1484 (2015).
41. Jiang, L., Tian, H.: Secure Beamforming in Cooperative D2D Communications with Simultaneous Wireless Information and Power Transfer. In: 2016 IEEE/CIC International Conference on Communications in China (ICCC), pp. 1-6. IEEE, Chengdu, China (2016).
42. Zheng, J., Xu, S., Zhao, F., Wang, D., Li, Y.: A Novel Detective and Self-organized Certificateless Key Management in Mobile Ad Hoc Networks. In: 2013 IEEE International Conference on Granular Computing (GrC), pp. 443-448. IEEE, Beijing, China (2013).
43. Liu, Q., Bai, X.: Survey on Certificateless Key Management Schemes in Mobile Ad Hoc Networks. In: 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 334-339. IEEE, Macau, China (2017).
44. Anand, D., Khemchandani, V., Sharma, R.: Identity-Based Cryptography Techniques and Applications (A Review). In: 5th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 343-348. IEEE, Mathura, India (2013).
45. Gharib, M., Moradlou, Z., Doostari, M., Movaghar, A.: Fully Distributed ECC-based Key Management for Mobile Ad Hoc Networks. Computer Networks 113, 269-283 (2017).