Security in Hybrid Cryptographic Algorithm and Power Control Mechanisms for Device-to-Device Communications

Kavita Krishnan[1*], Munna Lal Jatav[2]
[1]M. Tech. Scholar, Electronics and Communication, Samrat Ashok Technological Institute, Vidisha, India,
[2]Assistant Professor, Electronics and Communication, Samrat Ashok Technological Institute, Vidisha, India.

ABSTRACT:-
Device to device Communication has been incorporated with predominant module schemes for AWGN channel. To attain the high data rates device to device communication has to be utilized. The smart mobile devices can be used to transfer the higher data with the help of device to device communication model with in the sphere of a distinct operator's network.The security in D2D communications can be incorporated with a Hybrid cryptographic system. Hybrid cryptosystems are predominantly incorporating the trustworthiness of the cellular networking technology specifically used in device to device communication. The security has been incorporated with the help of Huffman coding and binary coding. This coding mechanism can increase the crypto benefits of the data transmission over device to device communication channel. In addition to that the cryptographic algorithms with improved key transmission can give rise to the security in D2D communications.The proposed research work is to implement step by step incorporation of Interference reduction with Bit Error Rate analysis, Security Implementation by incorporating Hybrid cryptographic system, implementing the power control and management mechanism for efficient PRB allocation and finally Huffman coding and binary coding in association with cryptographic algorithms with improved key transmission in D2D communications to attain the optimum performance.

Keywords: - D2D Communication, Hybrid Cryptographic System, Power Control, Physical Resource Block (PRB)

I. INTRODUCTION

Device to device communication is regarded as a novel networking technology predominantly used for 5G networks. D2D communications are working using dedicated signaling and automatic handover of network routed traffic with in the nearby devices connected in wireless sensor networks. D2D communication can be incorporated between two or more nearby devices when the base station operator facilitates the permission to perform the data transmission between these devices [1, 2]. In general conditions, the data transmission is carried out in a sequential order that starts from subscriber station to base station and gateway etc.

The data requested by the user equipment (UE) should be accessed from the base station only. When the data is already available from a designated node then the same data can be requested by the nearby device or UE in the same network. Then the requested data is downloaded from the designated node through base station. This is called as evolved Node Base Station (eNBs). But, when the base station operator provides the permission to the specific devices to transmit the data between themselves, it will be creating the D2D communication in the long term evolution (LTE) architecture [3].

LTE is providing the direct wireless links between distinct smart mobile users. The direct link will be established between two distinct mobile user nodes without interacting with the base station or core network. This will avoid the increased traffic configured and enriched in the service provider's network. The link between two distinct mobile user nodes will be established beyond the conventional infrastructure based communication. D2D communication is enriched with the LTE components to meet extended range of communication service requirements. D2D communications in 4G and 5G communications are established with the LTE-Advanced [4, 5].

LTE-A enables the D2D communication to establish uninterrupted connectivity between two mobile user nodes to withstand against any congestion problems of wireless networks. LTE-A is facilitating direct communication between two nodes with greater throughput, increased spectrum efficiency, energy efficiency and reduced transmission delay. D2D communication can be established in LTE-A Band, Wi-Fi direct and heterogeneous networks.

D2D communications are enriched with the increased performance with the establishment of LTE-A licensed band with the transmission capacity of 1Gbps band width. The maximum transmission distance in D2D communication is limited to 1000 meters with a uniformity service provision. D2D communications enable the users to transmit the data, voice and multimedia files directly in a licensed band provided by the wireless communication service provider [6, 7].

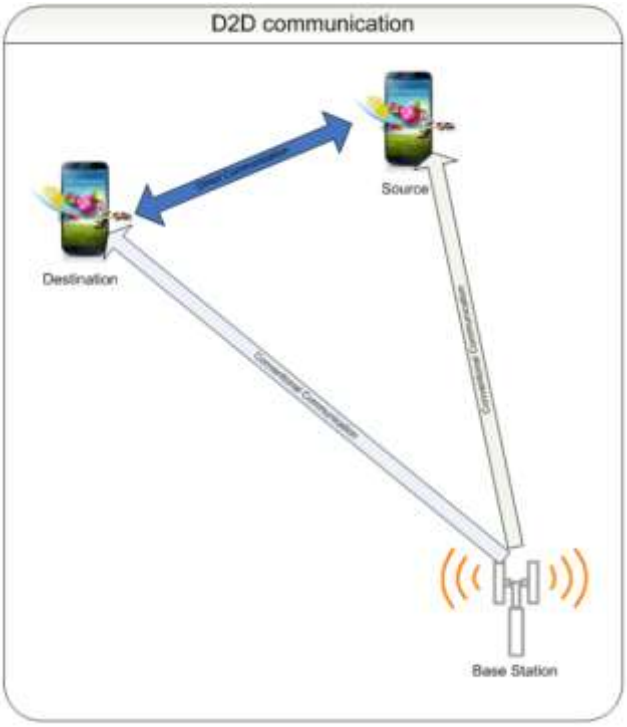

Fig. 1: D2D Communication Architecture

II. RELATED WORK

D2D communications are also designed to work in heterogeneous networks. Establishment of D2D communications is much effective than the wireless networks. Heterogeneous networks are configured with Macro Base Station [M-BS] and Micro Base Station [m-BS]. One Macro base station will be surrounded and supported by many m-BS. Heterogeneous wireless networks are rich with Multi-hop feature. M-BS will be surrounded by several m-BS. Every m-BS will be working as relay nodes [1].

Every Relay node will have the capacity to transmit the data with lowest power consumption to the designated node. The information transmitted from M-BS will reach to m-BS (Relay Node) and it will be transmitted to the User Equipment spanned across the network. The establishment of D2D communication in the heterogeneous networks enables the m-BS to relay the transmission between two direct nodes [2, 3]. D2D communications are established between two UEs. When the direct transmission is needed from one UE to other UE the communication will be relayed by m-BS to have effective and lossless transmission at lowest power consumption and with highest Quality of Service [4]. The transmission between two nodes configured in D2D communications are effectively done in both uplink and downlink.

Heterogeneous networks are established with several sectors and spanned across a vast area. To cover the area several m-BSs are incorporated. When D2D communications are established within the sectors of M-BS, the m-BSs will help the UEs connected in different sectors of Heterogeneous networks. The bandwidth is also distributed across D2D communications with the help of m-BS interaction only [5]. The support of m-BS will be continuous and allocates the needed bandwidth, power and spectrum efficiency with reusable mode. When the transmission is not happening in one pair of D2D communications in the networks, that power, bandwidth will be rolled back to the m-BS and it provides the same to the other D2D communication pair in the same network. This mechanism will increase the efficiency and performance of D2D communications in heterogeneous Networks [6].

D2D communication permits the smart phone users to transmit the data directly. This can be established when the network operator permits them to operate. In [7] a framework for D2D mode and resource allocation to D2D and non D2D users id discussed. A dynamically allocation of resources to the selected D2D communications in the wireless communication network is proposed in this work. A wireless communication network may have different D2D communicating pairs. The dynamic allocation of same frequency resources is possible by incorporating a framework to increase the throughput. When data transmission is not in force, the allocated resources will be rolled back by the proposed framework to optimize the resource allocation in the communication network [8].

A remarkable amount of interference can be established in D2D communication when radio resources are transmitted between them. A base station [BS] is surrounded by different User Equipment [9]. The UEs connected with the BS will have a channel to transmit the information. When D2D communications are established, a pair of UEs will be connected directly and use a separate channel for transmission [10]. The channel allocation is the critical issue when D2D communications are established in the wireless networks. The interference problem occurs when the channel is not properly allocated and it cannot withstand the traffic between two UEs in D2D communications [11]. UEs connected with BS will have direct channel and doesn't have any problem. The UEs established in D2D are supported by a wireless network service provider. The channels available and supporting to the network are allocated to the D2D communication UEs. The UE pair's working in D2D communications have a primary channel [12]. In this research work a mixed integer nonlinear programming is introduced to solve the interference problem in D2D communication [13]. This mechanism underlay a channel support, which provides dedicated support to the UEs incorporated in D2D communications. The main resource to transmit the data is considered to be the radio resources. This resource can increase the performance to transmit the data between two UEs in D2D communications [14, 15].

III. SECURITY MECHANISM IN D2D COMMUNICATION

The hybrid encryption mechanism is incorporated with in the channel used by D2D communications. Huffman coding is especially used for the image encryption and image compression. This coding is providing maximum security to the information passed from sender to receiver. Huffman coding is working in D2D communications with the following procedures. This coding takes only distinct symbols with shorter code words than symbols which frequently appear in the information transmission. The coding standards take two similar symbols and convert the same into encryption format and it compresses the image into symbol which frequently appears. Huffman coding is working with coding and decoding algorithms. Huffman coding converts the pain text into encrypted format and

then it also decodes the encryption format into plain text format.

In the proposed Hybrid cryptographic mechanism the binary coding is also playing a vital role. The binary code for wireless communications is predominantly used for extraction and interface identification for the encrypted format of plain text, image, voice or multimedia files. In some cases the binary code is re-used. Binary code is used for execution of a complete task. It does not take part in the complete task along with other encryption mechanisms.

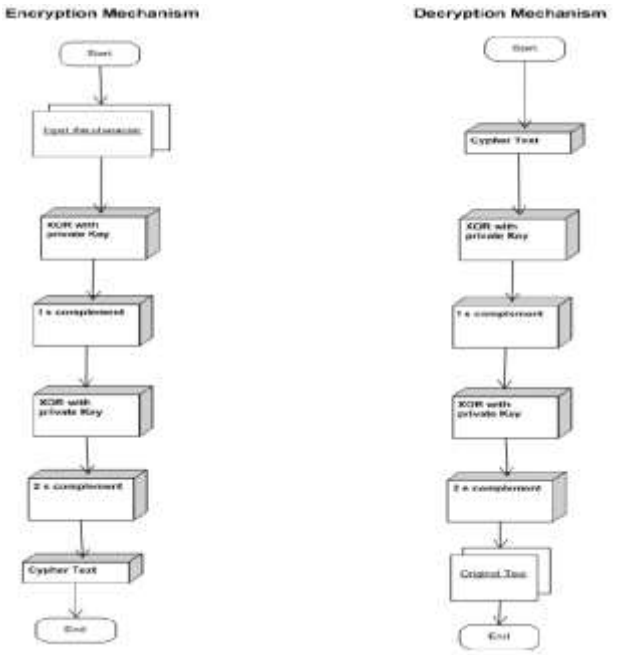

Fig. 2: Hybrid Cryptographic Algorithm

Binary code uses assembly functions of structured programming in accomplishing any task related to encryption or decryption. The information passes from UE and is influenced by the Binary code and sent to the destination node for decryption. It has a specific task like identification of specific key for specific information which is converted into cypher text (encrypted format).

The process of Hybrid Encryption algorithm is implemented in the following steps:

Encryption process:

- Takes the input data
- Transformation of plain text into binary mode
- The binary code transformation generate xor private key
- The algorithm identifies the 2's complement
- The algorithm identifies the 1's complement
- Identification of xor in association with public key
- Transformation of Cipher Text
- Applying Huffman Coding on cipher Text
- Extracting the relevant characters from database
- Replacement of cipher text characters into the matching characters with database
- Saving the set of characters into a file
- Formulation of cipher Text and ready for sending the functionality of Hybrid Decryption Algorithm at receiver's end.

Decryption Process:

- Extract the cipher text into reading pane
- Search the suitable characters for the cipher code from the database
- The code replacement with suitable characters from the database and positioning
- Identification of xor public key hidden from the message
- Identification of 1's complement
- Indemnification of 2's complement
- Identification of xor with private key
- Transformation of cipher text into original text.

IV. POWER CONTROL MECHANISM

Power control is focused in this research work to attain high data transmission rates in D2D communications. In this research work DUEs are configured to share SC-FDMA based UL PRBs OFDMA based DL PRBs associated with LTE-A supported D2D communications. In the event of sharing LTE-A PRBs the interference can be caused. The power control suggested can minimize the interference in sharing the LTE-A PRBs with the help of PF scheduling algorithms.

In this process the following calculations are presented.

PF metric value = Λ

Log Utility function = $\sum_u \log R_u$

Mean throughput of user u = R_u

Transmission time interval = TTI

User 'u' can use PRB in 'n' times = $\Lambda_{u,n} = {}^{r_{u,n}}/_{R_u}$

eNB calculation for Λ of CE = $\eta\varepsilon$ F_c, F1, F12, F3,F4, F5, F6

CE 'c' in j^{th} sector over nth UL and DL PRB usage calculated from the following equation.

$$\lambda_{c,nU}^{s_j} = 1 + \frac{r_{c,nU}^{s_j}}{R_{c,nU}^{s_j}} \quad (1)$$

And by using the following equation also we get

$$\lambda_{c,nD}^{s_j} = 1 + \frac{r_{c,nD}^{s_j}}{R_{c,nD}^{s_j}} \quad (2)$$

PRB utilized for UL and DL used for CE 'c' in sector 'j' in existing TTI

Achievable n^{th} PRB of UL and DL

$$= \quad R_{c,nU}^{s_j} \text{ and } R_{c,nD}^{s_j} \quad (3)$$

eNB calculation for Λ for every D2D pair (d) over n^{th} PRB of UL and DL is calculated as follows: the following equation is the calculation for UL

$$\lambda_{d,nU}^{s_{k,l}} = 1 + \frac{r_{d,nU}^{s_{k,l}}}{R_{d,nU}^{s_{k,l}}} \quad (4)$$

And it can also be expressed for DL in the following manner.

$$\lambda_{d,nD}^{s_{k,l}} = 1 + \frac{r_{d,nD}^{s_{k,l}}}{R_{d,nD}^{s_{k,l}}} \quad (5)$$

Resource Allocation:-

In the proposed research work, the PRB allocation scheme associated with PF scheduling algorithms allocates the UL and DL PRBs for DUEs. UL PRBs are allocated with high priority and DL PRBs are considered with low priority. The bandwidth sharing for UL as well as DL is not good enough to maintain the quality. Maintaining the quality of service in TCC is a challenging task. This has to be handled and sufficient bandwidth has to be allocated to the DUEs. Sharing the bandwidth between DUEs can be incorporated by the PF scheduling algorithms and PRB allocation scheme. DUEs are sharing the UL and DL PRBs of TCC for their communication transmission. When the DUEs are sharing single UL and DL PRBs severally for their communication transmission it will be working effectively as the communication channel is directly established. This advantage in DUEs has to be considered as the primary point. Using PF scheduling algorithm the resource allocation is done among all DUEs in the wireless communications. Every DL PRB is available with a specific UL PRB. When eNB allocates the DL PRB to a CE then it's corresponding UL is reserved with that CE only. DL PRB and UL PRB are essential to communicate with base station by CE. But we propose a UL PRB and a DL PRB be allocated a two pairs of DUEs. Each UE in D2D will take one UL PRB or DL PRB. This resource allocation with PF scheduling algorithm will efficiently distribute the band width among all D2D communications in the entire wireless communications.

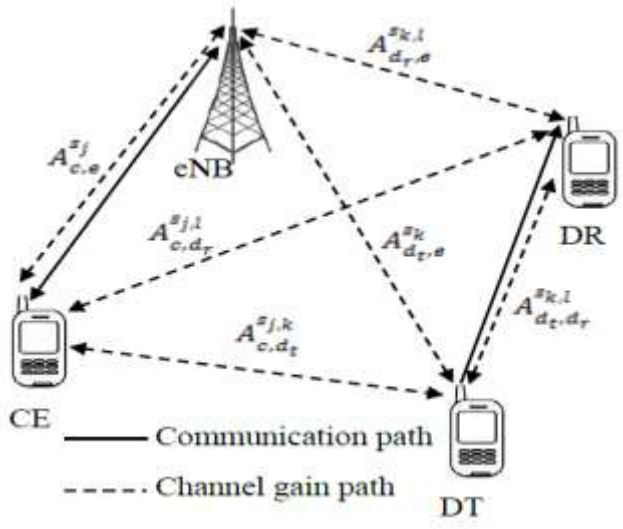

Fig. 3: Channel Gain in D2D Communications

V. SIMULATION RESULT

The simulation is conducted with different pairs of UE [User Equipment]. The simulation is incorporated with the distinct parameters to test the working condition of the pairs in the cellular network. The cell site is tested with 100 TTLs duration. The simulation is conducted for the utilization of Up Link and Down Link PRBs at a single instance for D2D communications. The following table describes the parameters used in the simulation results.

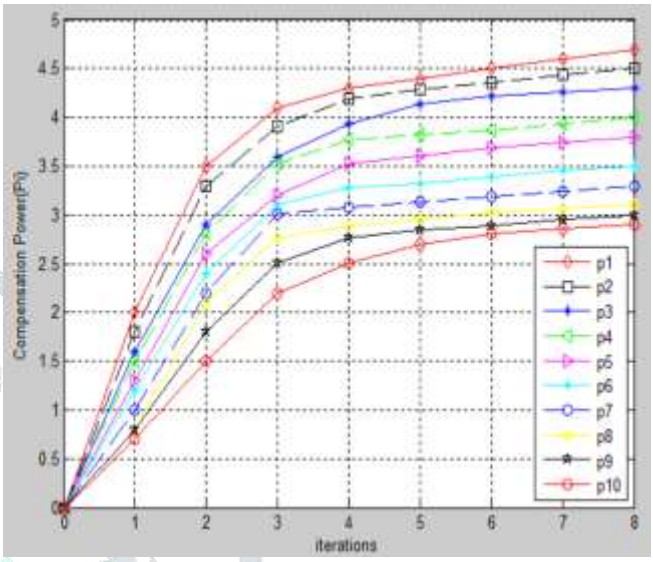

Fig. 4: Compensation power (in dBm) acquisition with iterations.

Fig. 4 is shown in compensation power (in dBm) acquisition for 10 D2D links with the distributed mechanism. The mechanism converges at the 5-th iteration.Fig. 4 is clearly show that the after three iteration compensation power almost same flow.

Table 1: Compensation (Com.)Power vs. Iterations for 10 D2D link

Com. Power (P_i)	Iterations								
	0	1	2	3	4	5	6	7	8
P1	0	2	3.5	4.1	4.3	4.4	4.5	4.6	4.7
P2	0	1.8	3.3	3.9	4.2	4.3	4.4	4.4	4.5
P3	0	1.6	2.9	3.6	3.9	4.1	4.15	4.2	4.3
P4	0	1.5	2.8	3.5	3.7	3.8	3.85	3.9	4.0
P5	0	1.3	2.6	3.2	3.5	3.6	3.65	3.7	3.8
P6	0	1.2	2.4	3.1	3.2	3.3	3.35	3.4	3.5
P7	0	1	2.2	3.0	3.1	3.2	3.25	3.3	3.4
P8	0	0.8	2.1	2.8	2.9	3.0	3.05	3.1	3.2
P9	0	0.8	1.8	2.5	2.7	2.8	2.85	2.9	3.0
P10	0	0.7	1.5	2.2	2.5	2.7	2.75	2.8	2.9

Compensation power vs. Iterations for 10 D2D link is shown in table 1. It is clearly that the D2D link is increase than power will decrease. The base station fully controls the allocationof compensation power for all D2D links via considering the individual need of each D2D link. For any D2D link, a better communication status will lead to a lower allocation of the compensation power for that link.

Security implementation with necessary mechanismis incorporating hybrid cryptographic system. Cryptographic algorithms are improved key transmission with the help of huffman coding and binary coding. Efficient PRB allocation is to control compensation power and management mechanism.

VI. CONCLUSION

D2D communications are novel and next generation networks which can facilitate high data transmission rates with the help of direct link between two User Equipment. Though D2D communications are playing a vital role in delivering the high data transmission rates, the recent experiences have revealed that D2D also have data transmission problems, high power consumption, resource management constraints when high data rates are recorded in the communication. The UEs in D2D communications are from public.To use higher modulation for data transmission the power control is essential. If the higher modulations are applied it may go beyond the receiver and lead to interference. To avoid interference with higher power utilization and use appropriate power for attaining desired modulation schemes the power control mechanism is needed to be incorporated. The power control mechanism is essential with resource management for D2D communications. To provide the security, hybrid crypto systems have been suggested with the combination of Huffman coding and binary coding.

REFERENCES

[1] Jun Huang, Shuai Huang, Cong-cong Xing, and Yi Qian, "Game-Theoretic Power Control Mechanisms for Device-to-Device Communications Underlaying Cellular System", IEEE Transactions on Vehicular Technology, IEEE 2018.

[2] Q. Wang, M. Hempstead, and W. Yang, "A realistic power consumptionmodel for wireless sensor network devices," in 2006 3rd Annual IEEECommunications Society on Sensor and Ad Hoc Communications andNetworks, vol. 1, Sept 2006, pp. 286–295.

[3] K. Fan, "Fixed-point and minimax theorems in locally convex topologicallinear spaces," Proceedings of the National Academy of Sciences ofthe United States of America, vol. 38, no. 2, p. 121, 1952.

[4] I. L. Glicksberg, "A further generalization of the kakutani fixed pointtheorem, with application to nash equilibrium points," Proceedings ofthe American Mathematical Society, vol. 3, no. 1, pp. 170–174, 1952.

[5] D. Simchi-Levi, S. D. Wu, and Z.-J. M. Shen, Handbook of quantitativesupply chain analysis: modeling in the e-business era. Springer Science& Business Media.

[6] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled deviceto-device communications in lte-advanced networks," IEEE WirelessCommunications, vol. 19, no. 3, pp. 96–104, June 2012.

[7] Q. Li, R. Hu, Y. Qian, and G. Wu, "Intracell cooperation and resourceallocation in a heterogeneous network with relays," IEEE Transactionson Vehicular Technology, vol. 62, no. 4, pp. 1770–1784, May 2013.

[8] G. Giambene, V. A. Le, T. Bourgeau, and H. Chaouchi, "Iterative multilevelsoft frequency reuse with load balancing for heterogeneous lteasystems," IEEE Transactions on Wireless Communications, vol. 16,no. 2, pp. 924–938, Feb 2017.

[9] S. Gong, P. Wang, and L. Duan, "Distributed power control with robustprotection for pus in cognitive radio networks," IEEE Transactions onWireless Communications, vol. 14, no. 6, pp. 3247–3258, June 2015.

[10] Y. Wu, J. Wang, L. Qian, and R. Schober, "Optimal power control forenergy efficient d2d communication and its distributed implementation,"IEEE Communications Letters, vol. 19, no. 5, pp. 815–818, May 2015.

[11] S. Gong, P. Wang, Y. Liu, and W. Zhuang, "Robust power control withdistribution uncertainty in cognitive radio networks," IEEE Journal onSelected Areas in Communications, vol. 31, no. 11, pp. 2397–2408,November 2013.

[12] J. Huang, Y. Sun, C.-C. Xing, Y. Zhao, and Q. Chen, "A distributedgame-theoretic power control mechanism for device-to-device communicationsunderlaying cellular network," in 2015 10th InternationalConference on Wireless Algorithms, Systems, and Applications (WASA),Aug 2015, pp. 222–231.

[13] N. Lee, X. Lin, J. Andrews, and R. Heath, "Power control for d2dunderlaid cellular networks: Modeling, algorithms, and analysis," IEEEJournal on Selected Areas in Communications, vol. 33, no. 1, pp. 1–13,Jan 2015.

[14] A. Ghazanfari, A. Tolli, and H. Pennanen, "Sum power minimization forcellular systems with underlay d2d communications," in 2014 9th InternationalConference on Cognitive Radio Oriented Wireless Networksand Communications (CROWNCOM), June 2014, pp. 45–50.

[15] G. Fodor and N. Reider, "A distributed power control scheme forcellular network assisted d2d communications," in 2011 IEEE GlobalTelecommunications Conference (GLOBECOM 2011), Dec 2011, pp. 1–6.

[16] G. Zhang, K. Yang, P. Liu, and J. Wei, "Power allocation for full-duplexrelaying based d2d communication underlaying cellular networks," IEEETransactions onVehicular Technology, vol. PP, no. 99, pp. 1–1, 2014.

[17] H. Zhou, Y. Ji, J. Li, and B. Zhao, "Joint mode selection, mcs assignment,resource allocation and power control for d2d communicationunderlaying cellular networks," in 2014 IEEE Wireless Communicationsand Networking Conference (WCNC), April 2014, pp. 1667–1672.

[18] S.-H. Yang, L.-C. Wang, J.-H. Huang, and A.-H. Tsai, "Networkassisteddevice-decided channel selection and power control for multipairdevice-to-device (d2d) communications in heterogeneous networks,"in 2014 IEEE Wireless Communications and Networking Conference(WCNC), April 2014, pp. 1356–1361.

[19] Q. Wang, W. Wang, S. Jin, H. Zhu, and N. Zhang, "Quality-optimizedjoint source selection and power control for wireless multimedia d2dcommunication using stackelberg game," IEEE Transactions on VehicularTechnology, vol. PP, no. 99, pp. 1–1, 2014.

[20] R. Yin, C. Zhong, G. Yu, Z. Zhang, K.-K. Wong, and X. Chen, "Jointspectrum and power allocation for d2d communications underlayingcellular networks," IEEE Transactions on Vehicular Technology, vol. PP,no. 99, pp. 1–1, 2015.

[21] N. Lee, X. Lin, J. Andrews, and R. Heath, "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," IEEE J. Sel. Areas Commun., vol. 33, no. 1, pp. 1–13, Jan. 2015.

[22] W. Cheng, X. Zhang, and H. Zhang, "Optimal power allocation with statistical QoS provisioning for D2D and cellular communications over underlaying wireless networks," IEEE J. Sel. Areas Commun., vol. 34, no. 1, pp. 151–162, Jan 2016.

[23] B. Kaufman and B. Aazhang, "Cellular networks with an overlaid device to device network," in Proc. Asilomar Conf. Signals, Syst. Comput., Oct. 2008, pp. 1537–1541.

[24] T. Peng, Q. Lu, H. Wang, S. Xu, and W. Wang, "Interference avoidance mechanisms in the hybrid cellular and device-to-device systems," in Proc. IEEE PIMRC, Sep. 2009, pp. 617–621.
[25] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products, 7th ed. Academic Press, 2007. [26] M. Haenggi, Stochastic Geometry for Wireless Networks. Cambridge University Press, 2012.
[26] Z. Liu, T. Peng, S. Xiang, and W. Wang, "Mode selection for device-todevice (D2D) communication under LTE-advanced networks," in Proc. IEEE ICC, Jun. 2012, pp. 5563–5567.
[27] P. Phunchongharn, E., Hossain, and D. I. Kim, "Resource allocation for device-to-device communications underlayinglte-advanced networks," IEEE Trans. Wireless Commun., vol. 20, no. 4, pp. 91–100, Aug. 2013.
[28] P. Mach, Z. Becvar, and T. Vanek, "In-band device-to-device communication in OFDMA cellular networks: A survey and challenges," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 1885–1922, Fourthquarter 2015.