IET Cyber-Physical Systems: Theory & Applications

Research Article

Enabling cyber-physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber-security

ISSN 2398-3396
Received on 24th January 2017
Revised on 15th February 2017
Accepted on 17th February 2017
doi: 10.1049/iet-cps.2017.0010
www.ietdl.org

Rachad Atat[1], *Lingjia Liu*[1] ✉, *Hao Chen*[1], *Jinsong Wu*[2], *Hongxiang Li*[3], *Yang Yi*[1]

[1]*Electrical Engineering and Computer Science (EECS) Department, University of Kansas, Lawrence, KS, USA*
[2]*Electrical Engineering Department, Universidad de Chile, Santiago, Chile*
[3]*Electrical and Computer Engineering Department, University of Louisville, Louisville, KY, USA*
✉ *E-mail: lingjialiu@gmail.com*

Abstract: Cyber-physical systems (CPS) help create new services and applications by revolutionising our world in different fields through their tight interactions and automated decisions. This is especially true with the ongoing increase in the number of physical things (sensors, actuators, smartphones, tablets, and so on) along with the explosive increase in the usage of online networking services and applications. Future fifth generation (5G) cellular networks will facilitate the enabling of CPS communications over current network infrastructure through different technologies such as device-to-device (D2D) communications. In this study, the authors discuss about the main challenges that cellular providers will face as the massive number of CPS devices attempt to access the cellular spectrum. A case study is presented on how to ease the spectrum access of these devices through D2D spatial spectrum sensing. Furthermore, the authors discuss about protecting these D2D links from eavesdropping, since security is becoming a critical aspect in the cyber-physical space, especially with the large amount of traffic that is constantly flowing through the network.

1 Introduction

With the world expecting over 50 billion sensors to be connected to the Internet by 2020 [1], whose wide deployments are made easier by the technological advancements in micro-electromechanical systems, along with the efficient low-cost designs of hardware architectures and components, the amount of data to be sensed, collected, and transmitted is expected to be growing at an unprecedented rate. In fact, this tsunami wave of new information, also known as big data, is foreseen to revolutionise our world through advancements in a wide variety of applications in health-care, military applications, city management, disaster event applications, environmental management, vehicular networks, industrial automation, and so on. This information revolution will create along with it new applications and services, as well as new opportunities for both consumers and businesses, where consumers would benefit from superior quality of services; while businesses would be able to boost their revenues by identifying customer needs and closing the gap between them and the consumers through uncovering hidden patterns, unknown correlations, and other useful information in the big data [2]. The ease of sensed data storage, processing, and analysis is facilitated by different techniques that are gaining a lot of attention by academia and industry such as cloud computing techniques, machine learning tools, data mining, artificial intelligence, and fog computing.

The massive number of physical objects such as embedded devices, smartphones, smart tablets, sensors, radio-frequency identification, and actuators along with the explosive increase in wireless data traffic driven by the popularity of video streaming, media sharing, and other networking services and applications have shaped the notion of cyber-physical systems (CPS). CPS mainly consists of interconnected physical objects and a cyber twin, where a cyber twin is considered as a simulation model such as a computer program, which can represent the physical things [3]. What interconnects the different CPS together is the Internet of Things, which helps facilitate their information transfer.

Acquiring the data from CPS is one of the easiest task, especially that recent advancements have allowed the pervasive presence of low-cost smart sensors. Data can be collected in different ways and from a variety of sources, such as physical sensors, virtual sensors which collect data from several sources using web services technology, or a combination of physical and virtual sensors, or global sensors which collect data from middleware infrastructures, or even remote sensors which collect remote sensed data for earth sciences applications [4, 5]. Data can also be collected from mobile users' smartphones rather than sensors, which is known under the terms of participatory sensing (PS) and mobile crowd-sensing (MCS). The main difference between PS and MCS is that the latter uses mobile social networking services along with mobile users' collected data to provide superior solutions to complicated queries [6]. An example of MCS is shown in Fig. 1, where users using their smartphones transmit warning messages (safe areas, areas to avoid etc.) among each other in case of a public safety event such as an earthquake or a flooding; in addition, governmental agencies' services transmit additional information such as number of injured and dead people, safest routes to flee, and so on. It is worth noting that both PS and MCS depend heavily on social mobility and users' behaviours and dynamics.

Data processing is an important aspect of CPS, but not as important as analysis and useful information extraction, which will be discussed afterwards. The large volume of data is first broken into workflows, so they can be easily distributed across multiple data centres, where different virtual machines can be run on them. This enables the parallel execution of tasks and queries for better data management, as well as the sharing of the computing and storage resources through rental by users in a pay-as-you-go fashion [7].

Data analysis and useful information extraction, also known as data mining, is what allows the automated decision making, an interesting feature of CPS. By extracting knowledge from large volume of data, we ease the process of finding solutions to complex problems, we enhance system performance, and we allow the creation of new applications and services [8]. To be able to realise all these benefits, one or a combination of different approaches can be taken to facilitate data mining, such as features selection, dimensionality

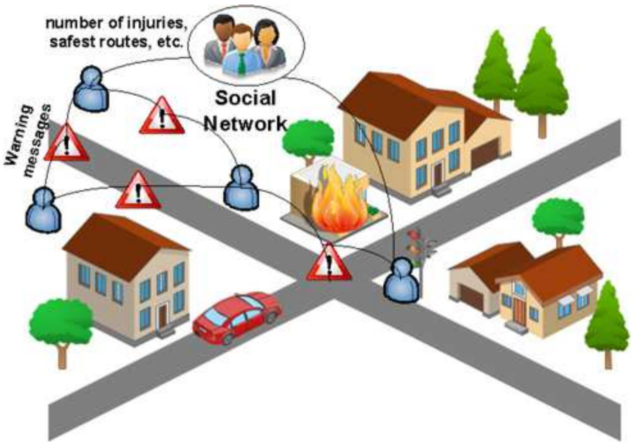

Fig. 1 *Example of a MCS in a disaster-related event*

reduction, knowledge discovery in databases, computer vision, information visualisation, classification/clustering, and real-time analysis, among others.

Security of CPS is also an interesting aspect that we specifically study in this paper. The security threats of CPS are made easier first with the large volume of data that is constantly flowing through the network, and second with the lack of qualified security experts. All this makes the monitoring of sensitive information a challenging task for analysts. Different approaches can be taken in this regard such as implementing advanced security controls (authentication), monitoring of real-time data streams, implementing advanced anomaly detection techniques by using neuromorphic computing for instance, real-time surveillance through computer vision and visualisation techniques, and so on [9].

On the other hand, interests and technical discussions about emerging technologies for the fifth generation (5G) cellular network have evolved into a full-fledged conversation capturing attention from researchers across the world [10]. It is envisioned that 5G technologies will be able to expand and support diverse usage scenarios and applications. To be specific, the usage scenarios include enhanced mobile broadband, ultra-reliable and low latency communications (URLLC), and massive machine-type communications (mMTC) [11]. For URLLC, the use case has stringent requirements for capabilities such as throughput, latency, and availability. Some examples include wireless control of industrial manufacturing or production processes, remote medical surgery, distribution automation in a smart grid, transportation safety, and so on. For mMTC, the use case is characterised by a very large number of connected devices typically transmitting a relatively low volume of non-delay-sensitive data. Devices are required to be low cost, and have a very long battery life requiring energy-efficient communication and computing. For the communication side, it is shown that local/short-range communication could significantly improve both the energy efficiency and spectral efficiency of a wireless system when circuit energy consumption is considered [12–14]. For the computing side, the recent developed concept of neuromorphic computing/reservoir computing can be a great candidate to significantly reduce the energy consumption [15, 16].

It is clear that the URLLC and mMTC aspects of 5G are clearly related to CPS and 5G cellular network may provide an ideal platform for CPS communications. On the other hand, enabling CPS communication in 5G cellular networks is far from being straightforward. For example, supporting coexistence between cellular users (CUs) and CPS links requires many new functionalities and control overhead which significantly complicates the network design. In this paper, we are going to shred some lights on this problem. To be specific, we summarise the contributions of this paper as follows:

- First, we provide a discussion on the benefits of running CPS communications over current cellular networks, followed by the main challenges and open issues that face cellular providers when it comes to supporting a large number of devices.
- Second, we discuss about some of the solutions proposed in literature. Then, through a case study we discuss about how spatial spectrum sensing in device-to-device (D2D) communications can help support the massive number of devices attempting to access the licensed cellular spectrum.
- Third, we present a low-complexity lightweight approach to secure the in-proximity CPS communications. Finally, we present some results to study the impact of spatial sensing region on the secure successful transmissions.

The rest of this paper is organised as follows. In Section 2, we discuss about how the integration of CPS can be realised over current cellular networks, the different challenges, open issues, and potential solutions that will enable CPS to shape future 5G networks. Then, in Section 3, we present a case study on D2D spatial spectrum sensing and cyber-security for in-proximity CPS communications, along with a brief discussion on some of the results obtained. Finally, conclusions are drawn in Section 4.

2 Enabling CPS communications in cellular networks

As discussed in the introduction, the pervasive global spread of physical devices (smartphones, tablets, sensors etc.) along with the increasing use of online social networking services and applications have led the way to a cyber-physical space with tight interaction and coordination among its physical components. This has overloaded the traditional network and made it impractical to support thousands of these devices that attempt to access the spectrum and communicate [17]. Even though cellular networks can provide several benefits to CPS such as ubiquitous coverage, global connectivity, reliability, and security, however, a set of challenges would face cellular providers before any of these benefits can be realised. First, current cellular networks follow a stratified structure where mobile devices follow the control from the base station (BS) (called eNodeB in Long-Term Evolution /Long-Term Evolution-Advanced networks) for spectrum access and communication. In this way, it is not designed to handle large volume of traffic, as CPS devices will rapidly cause congestion in the network from excess signalling overhead, leading to a failure of many of these communications. Second, the number of radio resources is already scarce and limited for traditional human communications; how about the anticipated massive number of devices? This means packet scheduling problems will occur and the network capacity and spectral efficiency will significantly degrade [18]. Third, there is a concern of excessive interference generated from the massive number of devices, add to that the multipath fading, which all lead to a performance degradation due to wireless channels becoming unreliable. So it is evident that we are facing several challenges when it comes to enabling CPS communications over current cellular networks; however many of these challenges can be addressed by the specifications and technologies of future 5G networks, as was discussed in [19].

Many of these devices are expected to be in close proximity to each other. To provide a potential solution to the above challenges, D2D communication can allow CPS devices in close proximity to communicate directly with each other. For faster data collection, research efforts need to focus on preconfiguring the network faster using dynamic on-the-fly D2D connectivity and without the need for controllers or infrastructure deployment. Relay-assisted D2D communications can help extend the limited communication range between CPS subnetworks [20], which in turn allows for a more efficient data collection. In our prior work [21], we analysed the spectral efficiency of the whole network if we offload machine-type communications (MTC) traffic on D2D links, where D2D relays are equipped with radio-frequency energy harvesting to compensate for the need to use their own limited energy reserves to forward data for MTC devices. We showed that by doing so, we can not only increase MTC spectral efficiency, but also achieve a balance and fairness in weighted spectral efficiency among D2D and CUs that are sharing the spectrum when there are enough number of available channels in the network and the D2D offloading factor is not set too high.

To support massive machine-type devices (MTDs) is one of the main driving force of 5G networks. In most of the current MTC systems, MTDs communicate directly with the eNodeB in one cell. This single-hop paradigm may not be able to support massive MTD where hundreds or thousands of MTDs attempt to set up communications. Furthermore, MTDs located at the boundary of a cell suffer from a high outage probability due to the interference from other MTDs. A costly solution is to deploy more eNodeBs and split the cell into multiple small cells. Instead of investing a huge amount of money on deploying extra eNodeBs or relays, cooperative communication has been demonstrated as an efficient and effective way to extend the coverage region and improve the throughput of cellular networks [22–24].

Conventionally, if an eNodeB fails to decode the packet, the MTD will retransmit the packet in the following available slot. However, it is with a high probability that the retransmission will fail again due to the correlated interference [25]. In paper [26], we designed and analysed a location-based cooperative strategy to improve the performance of massive MTC networks. One of the main idea of this paper is to select an inactive MTD acting as a relay for outage MTDs. Unlike the work in [27, 28] where the authors assumed the packet was known at the relay (BS) in prior, our paper considered the case where the relay has no prior information about the packet. To be specific, an inactive MTD is selected as a relay if it has successfully decoded the packet and if it is located within a circular area around the eNodeB. Otherwise, if there is no inactive MTD that can decode the packet, the source MTD will retransmit the packet. Both the simulation and numerical results demonstrate that spatiotemporal correlation of interference significantly affects the performance analysis of cooperative massive MTC networks and our designed cooperative strategy can significantly reduce the outage probability compared with conventional retransmission.

3 Spatial sensing and cyber-security for in-proximity CPS communications: a case study

With the tight and close interactions among the increasing number of physical objects such as smart phones, tablets, smart sensors, and others, D2D technology allows these in-proximity devices to communicate directly with each other bypassing the BS. This would allow the pervasive presence of massive number of devices, thereby creating a cyber-physical space where communications can run over current cellular networks, as was discussed in Section 2. In this case study, we address two major issues for enabling D2D communications for CPS: (i) efficient resource spectrum utilisation and cellular transmissions' protection through spatial spectrum sensing and (ii) D2D links' protection from eavesdropping. In what follows, we discuss and analyse these two issues in more details.

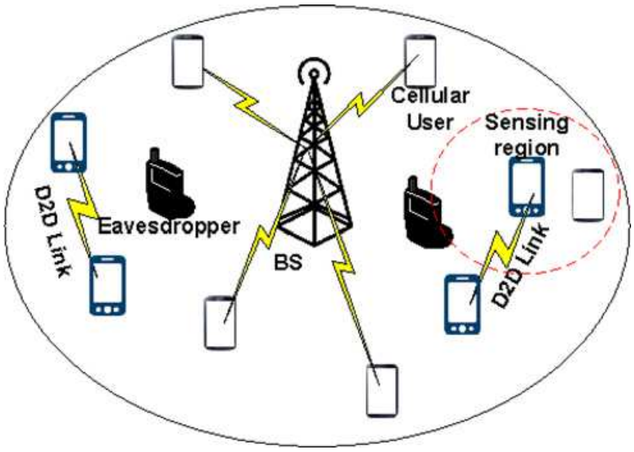

Fig. 2 *Example of a hybrid network with D2D and cellular links with eavesdroppers overhearing the D2D communication*

Realising CPS communications over D2D links can help achieve multiple benefits for future 5G networks. First, to relieve spectrum congestion from signalling overhead caused by massive number of physical objects attempting to communicate over licensed cellular bands, D2D technology solution allows the objects to share the cellular spectrum similar to cognitive radio networks (CRNs), but with some differences [29, 30]. First, while spectrum holes in CRNs are in the temporal domain, those in the cellular spectrum are in the spatial domain. This means that there is a spatial region around a D2D user where no cellular transmitter should be present to protect the cellular's transmissions [31]. By exploiting these spatial spectrum holes, both spectrum efficiency and power efficiency can be significantly increased. Second, CUs and D2D users are considered wireless users operating in two different modes: cellular mode and potential D2D mode; and therefore do not act as primary users and secondary users like in CRNs [31]. Finally, D2D users can rely on the BSs for assistance in spectrum sharing. It should be noted that when D2D users share the spectrum with CUs, the spectrum access is referred to as underlay in-band. Other D2D deployment scenarios exist such as overlay in-band D2D, and out-of-band D2D which have been thoroughly analysed and compared in [32]; however our main focus will be on the underlay model since it can achieve a higher throughput because it utilises the spectrum more efficiently compared with the overlay access [32].

In the realm of CPS, there is a large amount of data that is being sensed, collected, and transmitted, which place security threats under the spotlight of attention. This is especially true for the more vulnerable direct connections between proximity devices, which in turn degrade system's performance. There are different reasons why in-proximity D2D connections are more vulnerable to security flaws: D2D devices have (i) limited computational capabilities to employ data confidentiality, privacy preservation, and authentication; (ii) the semi- or fully-autonomous security management (mutual authentication, key arrangement etc.) [33]; and (iii) the high computational overhead cost of cryptographic solutions [34]. There have been some development of low-complex and lightweight ciphers such as PRESENT [35]; however such solutions can be time consuming and costly in terms of high power consumption as well as the complexity of key management [36, 37]; that is why research efforts should be pushed toward simpler solutions than cryptography.

To mitigate the potential D2D security threats such as eavesdropping, data fabrication, and privacy violation threats, we turn towards a lightweight low-complexity approach by exploiting the physical characteristics of the wireless channels, by defining a D2D spatial transmission region that can guarantee a minimum secrecy rate. By doing so, we are able to derive the detection probability that D2D link is secure.

Mode selection: A potential D2D user is a user with D2D traffic which can either use the cellular or the D2D mode for communications based on one or a combination of different selection criteria. This means that a potential D2D user can switch between D2D and conventional cellular communications. For this case study, we use distance-based selection threshold μ [32]. Let $L_{\rm C}$ and $L_{\rm D}$ be random variables representing the link lengths of a typical CU and D2D user, respectively. More specific, a user is in D2D mode if the transceiver distance $L_{\rm D}$ is smaller than μ. We assume that the D2D receiver is uniformly distributed within a circle centred at user i located at location x_i with a radius of D, as $\mathcal{B}(x_i, D)$ [32], with probability density function

$$f_{\rm D}(r) = \frac{2r}{D^2}, \quad 0 \le r \le D. \tag{1}$$

Fig. 2 illustrates a hybrid network of D2D links, cellular links, and a set of eavesdroppers that attempt to overhear the D2D transmissions. Furthermore, the figure shows a spatial sensing region around D2D users. We consider an uplink cellular network, where D2D users and CUs share the licensed spectrum. The use of stochastic geometry allows us to provide an accurate model of interferers' spatial locations by averaging over all their potential topological realisations [38]. The locations of the macro BSs are modelled by a homogeneous Poisson point process (HPPP), Φ_{B} of intensity λ_{B}. Let $\mathcal{A}(k, R_{\mathrm{B}})$ denotes the coverage region of a macrocell, approximated by a disk with radius $R_{\mathrm{B}} = \left(\pi\lambda_{\mathrm{B}}\right)^{-1/2}$ centred at a generic BS k [39]. User equipments (EUs) are uniformly distributed in the coverage region of the corresponding BS and form an HPPP, Φ_{U} of intensity λ_{U}. The eavesdroppers form an HPPP Φ_{E} of intensity λ_{E}.

We denote by $\| i - j \|$ as the distance between any two nodes i and j. We use a power-law path-loss model where the power of the signal transmitted by UEs decays at a rate of $l(i, j) = \| i - j \|^{-\alpha}$, and $\alpha > 2$ is the path-loss exponent of both cellular and D2D transmitters. To model the small-scale fading over each channel, we use Rayleigh fading with mean one, with h_{ij} denoting the channel coefficient between nodes i and j.

For reliable communication, we assume that all users use a truncated channel inversion power control [40, 41], which ensures the average received signal power at the intended receiver (i.e. D2D receivers and BSs) is at least equal to its sensitivity. Thus, UEs will use power control $P_i = \rho L_i^{\alpha}$, for $i = \{C, D\}$; and $\rho \ll 1$ is a constant that scales down the actual transmit power [32].

We differentiate between two different types of nodes τ_i with $i = \{D, C\}$, for D2D user and CU, respectively. Let $q \in [0, 1]$ be the probability that a user is a potential D2D user [32].

- *D2D user*: The UEs in D2D mode form a thinning PPP Φ_{D} from Φ_{U}, with intensity $\lambda_{\mathrm{D}} = q\lambda_{\mathrm{U}}\mathcal{P}\left(L_{\mathrm{D}} < \mu\right)$.
- *CU*: The UEs in cellular mode include both CUs and potential D2D users operating in cellular mode. Therefore, these users form a thinning PPP Φ_{C} from Φ_{U}, with intensity $\lambda_{\mathrm{C}} = (1 - q)\lambda_{\mathrm{U}} + q\lambda_{\mathrm{U}}\mathcal{P}\left(L_{\mathrm{C}} \geq \mu\right)$. Note that $\Phi_{\mathrm{U}} = \Phi_{\mathrm{C}} \cup \Phi_{\mathrm{D}}$, and $\Phi_{\mathrm{D}} \cap \Phi_{\mathrm{C}} = \emptyset$.

3.1 Spatial spectrum sensing

A sensing region $\mathcal{A}_{\mathrm{s}}$ is defined as a circular region centred at a D2D user x_i with sensing radius R_{s}. Without loss of generality, the D2D transmitter is assumed located at the origin. A D2D transmitter opportunistically accesses the spectrum by performing energy detection on the test statistics Γ, where $\Gamma = 1/N \sum_{n=0}^{N-1} |y[n]|^2$; and $y[n]$ is defined under two different hypotheses: (i) $\mathcal{H}_0$ when there are no active CUs inside $\mathcal{A}_{\mathrm{s}}$; and (ii) $\mathcal{H}_1$ when there is at least one active CU inside $\mathcal{A}_{\mathrm{s}}$. It is given as [42]

$$\mathcal{H}_0{:}y[n] = \sum_{i \in \phi_{\mathrm{C,a}} \cap \mathcal{A}_{\mathrm{s}}^{C}} \sqrt{P_{\mathrm{C},i} h_i \, \| x_i \|^{-\alpha}} s_i[n] + z[n], \tag{2}$$

$$\mathcal{H}_1{:}y[n] = \sum_{i \in \tilde{\phi}_{\mathrm{C,a}} \tilde{\phi}_{\mathrm{C,a}} \cap \mathcal{A}_{\mathrm{s}} \neq \emptyset} \sqrt{P_{\mathrm{C},i} h_i \, \| x_i \|^{-\alpha}} s_i[n] + z[n], \tag{3}$$

where $n = 0, 1, \ldots, N - 1$ is the sample index with N being the total number of samples; $s_i[n]$ is the nth sample of the received signal from cellular transmitter i by a typical D2D user; $z[n]$ is the Gaussian noise sample ($z[n] \sim \mathcal{N}(0, \sigma_n^2)$); and $\phi_{\mathrm{C,a}}$ is a realisation of $\Phi_{\mathrm{C,a}}$ denoting the set of active cellular transmitters' locations; and $\mathcal{A}_{\mathrm{s}}^{C}$ is the complementary set of $\mathcal{A}_{\mathrm{s}}$. Let ϵ denotes the underlying sensing threshold. The probabilities of false alarm P_{f} and spatial detection P_{d} are given in [31] as

$$\begin{aligned} P_{\mathrm{f}} &= \int_0^{\infty} \mathcal{Q}\left(\frac{\epsilon - x - \sigma_n^2}{\sqrt{\left(x + \sigma_n^2\right)^2 / N}}\right) \sqrt{\frac{\rho}{2\pi x^3}} \mathrm{e}^{-\rho(x-\upsilon)^2/2\upsilon^2 x} \, \mathrm{d}x, \\ P_{\mathrm{d}} &= \sum_{i=1}^{\infty} \frac{\Gamma(1 + i\delta)\sin(\pi i\delta)\pi^{2i-1}(\lambda_{\mathrm{B}}\delta\mathbb{E}[P_c^{\delta}])^i}{(-1)^{i+1}(1 - \mathrm{e}^{-\lambda_{\mathrm{B}}\pi R_{\mathrm{s}}^2})i!\sin(\pi\delta)^i} \\ &\quad \times \int_0^{\infty} \mathcal{Q}\left(\frac{\epsilon - x - \sigma_n^2}{\sqrt{\left(x + \sigma_n^2\right)^2 / N}}\right) \frac{dx}{x^{1+i\delta}} - \frac{\mathrm{e}^{-\lambda_{\mathrm{B}}\pi R_{\mathrm{s}}^2} P_{\mathrm{f}}}{1 - \mathrm{e}^{-\lambda_{\mathrm{B}}\pi R_{\mathrm{s}}^2}}, \end{aligned} \tag{4}$$

where $\rho = 2\mathbb{E}[P_c]^3 R_{\mathrm{s}}^{4-\alpha}(2\alpha - 2)/(\alpha - 2)^3 R_{\mathrm{B}}^4 \mathbb{E}[P_c^2]$, $\upsilon = 2\mathbb{E}[P_c] R_{\mathrm{s}}^{2-\alpha}/(\alpha - 2)R_{\mathrm{B}}^2$, $\delta = 2/\alpha$, $\mathcal{Q}(x) = (1/\sqrt{2\pi})\int_x^{\infty} \mathrm{e}^{-u^2/2} \, \mathrm{d}u$. In (4), $\mathbb{E}[P_c]$ is UE's average transmit power, R_{B} is the cell radius, and R_{s} is the sensing radius of spatial spectrum sensing.

3.2 D2D links' secrecy analysis

In this section, we obtain the probability of detecting that D2D link is secure by assuming that each D2D link is exposed to all the eavesdroppers. We also obtain the secure transmission region defined as the region within which eavesdroppers cannot intercept the communication with high probability.

The aggregate interference of an eavesdropper located at a distance $\| z \|$ away from the typical D2D link is the interference generated from active cellular transmitters and other active D2D transmitters, and is given by

$$I_{\mathrm{E}} = \sum_{k \in \Phi_{\mathrm{C},a}} P_{\mathrm{C},k} h_{k,z} l(k, z) + \sum_{k \in \Phi_{\mathrm{D},a} \backslash 0} P_{\mathrm{D},k} h_{k,z} l(k, z), \tag{5}$$

where $\Phi_{\mathrm{D},a}$ is approximated as an HPPP to model the locations of active D2D transmitters with intensity [31] $\lambda_{\mathrm{D},a} = \bar{\beta}\lambda_{\mathrm{D}}$; with $\bar{\beta} = \left(P_{\mathrm{d}} + \left(P_{\mathrm{f}} - P_{\mathrm{d}}\right)\mathrm{e}^{-\pi\lambda_{\mathrm{B}}R_{\mathrm{s}}^2}\right)\beta_1 \quad +\left(1 - P_{\mathrm{d}} - \left(P_{\mathrm{f}} - P_{\mathrm{d}}\right)\right.$ $\left.\mathrm{e}^{-\pi\lambda_{\mathrm{B}}R_{\mathrm{s}}^2}\right)\beta_0$; β_1 is the spectrum access probability if the spectrum hole is correctly detected or when a false alarm occurs, while β_0 is the probability when misdetection occurs. The Laplace transform of I_{E} is given by [43]

$$\mathcal{L}_{I_{\mathrm{E}}}(s) = \exp\left(\frac{-\lambda_{\mathrm{C},a}E\left[P_{\mathrm{C}}^{\delta}\right] - \lambda_{\mathrm{D},a}E\left[P_{\mathrm{D}}^{\delta}\right]}{\mathrm{sinc}\delta}\pi s^{\delta}\right). \tag{6}$$

Let $\max_{e \in \Phi_{\mathrm{E}}} \gamma_{e,0}$ denotes the eavesdropper with the most detrimental effect on D2D signal. In interference-limited networks, the average probability that a D2D link is secure is equal to the average probability that the rate of the most detrimental eavesdropper falls below a certain threshold ζ. It is expressed as [43]

$$\begin{aligned} P_{\mathrm{s}}(\zeta) &= \mathcal{P}\left(\log\left(1 + \max_{e \in \Phi_{\mathrm{E}}} \gamma_{e,0}\right) < \zeta\right) \\ &= \exp\left(\frac{-\lambda_{\mathrm{E}}\mathrm{sinc}\delta}{\left(\lambda_{\mathrm{C},a}E[P_{\mathrm{C}}^{\delta}] + \lambda_{\mathrm{D},a}E[P_{\mathrm{D}}^{\delta}]\right)E[P_{\mathrm{E}}^{-\delta}]\left(2^{\zeta} - 1\right)^{\delta}}\right), \end{aligned} \tag{7}$$

where P_{E} is the average transmit power of an eavesdropper. A D2D transmission is said to be secure if $P_{\mathrm{s}}(\zeta) \geq \upsilon_s$, where υ_s denotes the minimum required secrecy probability. Then, we can obtain an upper bound for the secrecy rate threshold for secure communication in high signal-to-interference-plus-noise ratio (SINR) regime as

$$\zeta \leq \delta^{-1}\log_2\left(\frac{-\lambda_{\mathrm{E}}\mathrm{sinc}\delta}{\left(\lambda_{\mathrm{C}}E[P_{\mathrm{C}}^{\delta}] + \lambda_{\mathrm{D},a}E[P_{\mathrm{D}}^{\delta}]\right)E[P_{\mathrm{E}}^{-\delta}]\log\upsilon_{\mathrm{s}}}\right). \tag{8}$$

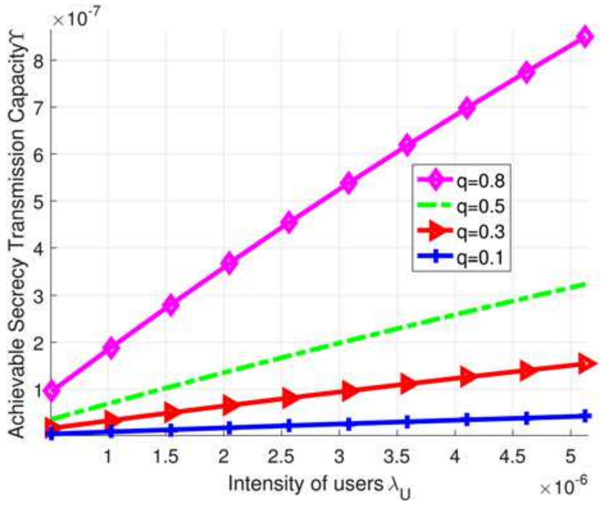

Fig. 3 *Achievable secrecy transmission capacity against the intensity of users for different values of q* ($\lambda_E = 0.1\lambda_U$; $R_s = 150$ *m)*

The secure transmission region, $\mathcal{A}_t(\mu_s, \upsilon_s) \subset \mathbb{R}^2$, around a typical D2D user is random and defined as the range within which eavesdroppers cannot intercept the communication with high probability. In other words, $\mathcal{A}_t(\mu_r, \upsilon_s)$ is the region where the set of all eavesdroppers are located outside a closed ball $\mathcal{B}(o, 2^{\zeta/\alpha}\|x_o\|)$ centred around the typical D2D user located at $\|x_o\|$ with radius $2^{\zeta/\alpha}\|x_o\|$ [44]. Therefore, we can use the upper bound on ζ defined in (8) to define $\mathcal{A}_t(\mu_r, \upsilon_s)$ as

$$\mathcal{A}_t(\mu_r, \upsilon_s) = \{x \in \boldsymbol{R}^2 : \|e - x_o\| > \mu_r = 2^{\zeta/\alpha}\|x_o\|\}. \tag{9}$$

Then

$$\mu_r \le \int_0^D 2^{\zeta/\alpha} r f_D(r)\,\mathrm{d}r = 2^{\zeta/\alpha}\frac{2D}{3}. \tag{10}$$

3.3 Achievable secrecy transmission capacity

In the case when the packets are not successfully decoded, we assume no re-transmissions. Let θ_D be the SINR threshold for successful transmission. We can then define the mathematical expectation of the achievable secrecy transmission capacity, i.e. the density of secure successful transmissions at a rate $\log(1+\theta_D)$ as [43]

$$\begin{aligned}\Upsilon &= \lambda_{D,a}\log(1+\theta_D)\mathcal{P}(\gamma_{i,0} \ge \theta_D)\\ &= \lambda_{D,a}\log(1+\theta_D)\frac{1 - \mathrm{e}^{-\mu_r^2(a_2+a_3)}}{(a_2+a_3)D^2},\end{aligned} \tag{11}$$

where $a_2 = (\pi\lambda_{C,a}\theta_D^\delta/\mathrm{sinc}\delta)E[P_C^\delta]P_D^{-\delta}$; $a_3 = \pi\lambda_{D,a}\theta_D^\delta/\mathrm{sinc}\delta$.

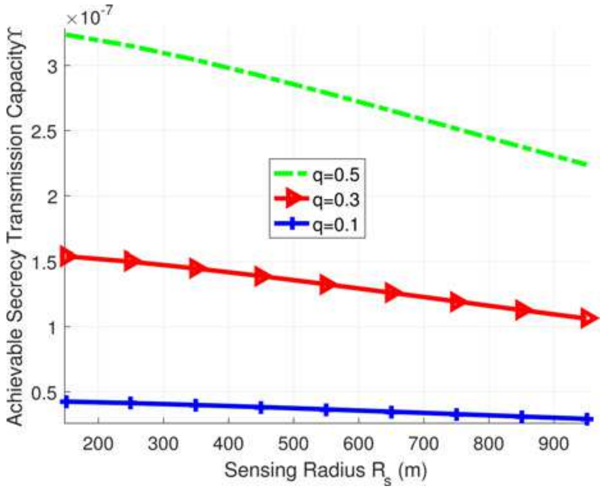

Fig. 4 *Achievable secrecy transmission capacity against the sensing radius for different values of q* ($\lambda_U = 10\lambda_B$ *and* $\lambda_E = 0.1\lambda_U$*)*

3.4 Performance evaluation

In this section, we present numerical results to study the achievable transmission capacity of secrecy-based D2D cellular networks with spatial spectrum sensing. Unless otherwise stated, we set the following system parameters: $R_B = 788$ m (which corresponds to an inter-BS distance of 1500 m), $\zeta = 0.5$, $D = 100$ m, $\alpha = 4$, $\lambda_B = 1/(\pi R_B^2) = 5.126 \times 10^{-7}$, $\theta_D = 20$ dB, $\upsilon_s = 0.5$, $N = 5000$, and $\rho = 10^{-11}$.

Fig. 3 shows the average achievable secrecy transmission capacity against λ_U for different values of q. In Fig. 3, λ_U changes from λ_B to $10 \times \lambda_B$. As more users are operating in the D2D mode (i.e. when q increases), the achievable transmission capacity becomes higher due to the receiver becoming closer in distance to the transmitter and eavesdroppers becoming far away. Moreover, as the intensity of users increases, the secrecy transmission capacity increases since the interference of a larger legitimate user population can be exploited in a beneficial way to protect D2D links from eavesdropping, from a physical layer security perspective.

Fig. 4 shows the average achievable secrecy transmission capacity against the sensing radius R_s for different values of q. We see that as R_s increases, the spatial sensing becomes more conservative and less aggressive. This means, the probability of detecting spatial spectrum holes decreases, leading to fewer active D2D transmissions. This in turn increases the distances between the D2D transmitters and receivers, thereby making the D2D links more susceptible to eavesdropping. That is why we see a decreasing behaviour in the secrecy transmission capacity as the sensing radius increases.

4 Conclusions

In this paper, we have discussed about the major challenges facing network providers when it comes to enabling CPS communications in cellular networks. We have provided a thorough discussion on D2D technology as a potential solution and driving force to support thousands of devices that attempt to access the cellular spectrum. More specific, we have provided a detailed discussion and analysis on spatial spectrum sensing and its effects on the density of successful secure transmissions. We showed that more aggressive sensing can better protect D2D links against eavesdropping since more D2D users become active, which reduce the distances between them.

5 Acknowledgment

The works of R. Atat, H. Chen, and L. Liu are supported by National Science Foundation (NSF) under grant NSF/ECCS-1509514.

6 References

1 Cisco: 'Fog computing and the internet of things: extend the cloud to where the things are'. Technical report, white paper, Cisco, 2015

2 Tsai, C.W., Lai, C.F., Chiang, M.C., *et al.*: 'Data mining for internet of things: a survey', *IEEE Commun. Surv. Tutor.*, 2014, **16**, (1), pp. 77–97

3 Lee, J., Bagheri, B., Kao, H.: 'A cyber-physical systems architecture for industry 4.0-based manufacturing systems', *Manuf. Lett.*, 2015, **3**, pp. 18–23

4 Perera, C., Zaslavsky, A., Christen, P., *et al.*: 'Context aware computing for the internet of things: a survey', *IEEE Commun. Surv. Tutor.*, 2014, **16**, (1), pp. 414–454

5 Chi, M., Plaza, A., Benediktsson, J.A., *et al.*: 'Big data for remote sensing: challenges and opportunities', *Proc. IEEE*, 2016, **104**, (11), pp. 2207–2219

6 Guo, B., Chen, C., Zhang, D., *et al.*: 'Mobile crowd sensing and computing: when participatory sensing meets participatory social media', *IEEE Commun. Mag.*, 2016, **54**, (2), pp. 131–137

7 Wang, D., Liu, J.: 'Optimizing big data processing performance in the public cloud: opportunities and approaches', *IEEE Netw.*, 2015, **29**, (5), pp. 31–35

8 Qu, F., Wang, F.Y., Yang, L.: 'Intelligent transportation spaces: vehicles, traffic, communications, and beyond', *IEEE Commun. Mag.*, 2010, **48**, (11), pp. 136–142

9 Mahmood, T., Afzal, U.: 'Security analytics: big data analytics for cybersecurity: a review of trends, techniques and tools'. 2013 second National Conf. on Information Assurance (NCIA), December 2013, pp. 129–134

10 5G RESEARCH IN HORIZON 2020

11 'Recommendation ITU-R M.2083-0: IMT vision – framework and overall objectives of the future development of IMT for 2020 and beyond' (International Telecommunication Union, 2015)

12 Liu, L., Miao, G., Zhang, J.: 'Energy-efficient scheduling for downlink multi-user MIMO'. 2012 IEEE Int. Conf. on Communications (ICC), June 2012, pp. 4394–4394

13 Liu, L., Yi, Y., Chamberland, J.F., *et al.*: 'Energy-efficient power allocation for delay-sensitive multimedia traffic over wireless systems', *IEEE Trans. Veh. Technol.*, 2014, **63**, (5), pp. 2038–2047

14 Mahmood, F., Perrins, E., Liu, L.: 'Modeling and analysis of energy consumption for RF transceivers in wireless cellular systems'. 2015 IEEE Global Communications Conf. (GLOBECOM), December 2015, pp. 1–6

15 Zhao, C., Wysocki, B.T., Liu, Y., *et al.*: 'Spike-time-dependent encoding for neuromorphic processors', *J. Emerg. Technol. Comput. Syst.*, 2015, **12**, (3), pp. 23:1–23:21

16 Yi, Y., Liao, Y., Wang, B., *et al.*: 'FPGA based spike-time dependent encoder and reservoir design in neuromorphic computing processors', *Microprocess. Microsyst.*, 2016, **46**, Part B, pp. 175–183

17 Socievole, A., Ziviani, A., De Rango, F., *et al.*: 'Cyber-physical systems for mobile opportunistic networking in proximity (MNP)', *Comput. Netw.*, 2016, **111**, pp. 1–5

18 Laya, A., Alonso, L., Alonso-Zarate, J.: 'Is the random access channel of LTE and LTE-A suitable for M2M communications? a survey of alternatives', *IEEE Commun. Surv. Tutor.*, 2014, **16**, (1), pp. 4–16

19 Andrews, J.G., Buzzi, S., Choi, W., *et al.*: 'What will 5G be?', *IEEE J. Sel. Areas Commun.*, 2014, **32**, (6), pp. 1065–1082

20 Atat, R., Liu, L., Ashdown, J., *et al.*: 'On the performance of relay-assisted D2D networks under spatially correlated interference'. 2016 IEEE Global Communications Conf. (GLOBECOM), December 2016, pp. 1–6

21 Atat, R., Liu, L., Mastronarde, N., *et al.*: 'Energy harvesting-based D2D-assisted machine-type communications', *IEEE Trans. Commun.*, 2016, **PP**, (99), pp. 1–1

22 Neonakis Aggelou, G., Tafazolli, R.: 'On the relaying capability of next-generation GSM cellular networks', *IEEE Pers. Commun. Mag.*, 2001, **8**, (1), pp. 40–47

23 Zhang, J., Shao, C., Wang, Y., *et al.*: 'Performance of a two-hop cellular system with different power allocation schemes'. 2004 IEEE 60th Vehicular Technology Conf. (VTC2004-Fall), September 2004, vol. 6, pp. 4538–4542

24 Sreng, V., Yanikomeroglu, H., Falconer, D.: 'Coverage enhancement through two-hop relaying in cellular radio systems'. 2002 IEEE Wireless Communications and Networking Conf. (WCNC 2002), March 2002, vol. 2, pp. 881–885

25 Haenggi, M., Smarandache, R.: 'Diversity polynomials for the analysis of temporal correlations in wireless networks', *IEEE Trans. Wirel. Commun.*, 2013, **12**, (11), pp. 5940–5951

26 Chen, H., Liu, L., Mastronarde, N., *et al.*: 'Cooperative retransmission for massive MTC under spatiotemporally correlated interference'. 2016 IEEE Global Communications Conf. (GLOBECOM), December 2016

27 Zhou, Y., Zhuang, W.: 'Opportunistic cooperation in wireless *ad hoc* networks with interference correlation', *Peer-to-Peer Netw. Appl.*, 2017, **10**, (1), pp. 238–252

28 Nigam, G., Minero, P., Haenggi, M.: 'Spatiotemporal cooperation in heterogeneous cellular networks', *IEEE J. Sel. Areas Commun.*, 2015, **33**, (6), pp. 1253–1265

29 Haykin, S., Thomson, D.J., Reed, J.H.: 'Spectrum sensing for cognitive radio', *Proc. IEEE*, 2009, **97**, (5), pp. 849–877

30 Yucek, T., Arslan, H.: 'A survey of spectrum sensing algorithms for cognitive radio applications', *IEEE Commun. Surv. Tutor.*, 2009, **11**, (1), pp. 116–130

31 Chen, H., Liu, L., Novlan, T., *et al.*: 'Spatial spectrum sensing-based device-to-device cellular networks', *IEEE Trans. Wirel. Commun.*, 2016, **15**, (11), pp. 7299–7313

32 Lin, X., Andrews, J.G., Ghosh, A.: 'Spectrum sharing for device-to-device communication in cellular networks', *IEEE Trans. Wirel. Commun.*, 2014, **13**, (12), pp. 6727–6740

33 Wang, M., Yan, Z.: 'Security in D2D communications: a review'. 2015 IEEE Trustcom/BigDataSE/ISPA, August 2015, vol. 1, pp. 1199–1204

34 Raychaudhuri, K., Ray, P.: 'Privacy challenges in the use of ehealth systems for public health management', *Int. J. E-Health Med. Commun.*, 2010, **1**, (2), pp. 12–23

35 Pospiil, J., Novotný, M.: 'Evaluating cryptanalytical strength of lightweight cipher present on reconfigurable hardware'. 2012 15th Euromicro Conf. on Digital System Design, September 2012, pp. 560–567

36 Li, Z., Oechtering, T.J.: 'Privacy-aware distributed Bayesian detection', *IEEE J. Sel. Top. Signal Process.*, 2015, **9**, (7), pp. 1345–1357

37 Canelo, F., Silva, B.M.C., Rodrigues, J.J.P.C., *et al.*: 'Performance evaluation of an enhanced cryptography solution for m-health applications in cooperative environments'. 2013 IEEE Global Communications Conf. (GLOBECOM), December 2013, pp. 1711–1716

38 ElSawy, H., Hossain, E., Haenggi, M.: 'Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey', *IEEE Commun. Surv. Tutor.*, 2013, **15**, (3), pp. 996–1019

39 Novlan, T.D., Dhillon, H.S., Andrews, J.G.: 'Analytical modeling of uplink cellular networks', *IEEE Trans. Wirel. Commun.*, 2013, **12**, (6), pp. 2669–2679

40 Sakr, A.H., Hossain, E.: 'Cognitive and energy harvesting-based D2D communication in cellular networks: stochastic geometry modeling and analysis', *IEEE Trans. Commun.*, 2015, **63**, (5), pp. 1867–1880

41 ElSawy, H., Hossain, E., Alouini, M.S.: 'Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks', *IEEE Trans. Commun.*, 2014, **62**, (11), pp. 4147–4161

42 Chen, H., Liu, L.: 'Resource allocation for sensing-based device-to-device (D2D) networks'. 2015 49th Asilomar Conf. on Signals, Systems and Computers, November 2015, pp. 1058–1062

43 Atat, R., Liu, L.: 'On the achievable transmission capacity of secrecy-based D2D cellular networks'. IEEE Global Communications Conf. (GLOBECOM), December 2016, pp. 1–6

44 Wang, H., Zhou, X., Reed, M.C.: 'Physical layer security in cellular networks: a stochastic geometry approach', *IEEE Trans. Commun.*, 2013, **12**, (6), pp. 2776–2787