Wireless Communications and Mobile Computing

Green Internet of Things (IoT): Enabling Technologies, Architectures, Performance, and Design Issues

Lead Guest Editor: Hina Tabassum
Guest Editors: Mahdi Ben Ghorbel, Hesham Elsawy, Wael Guibene, and Sudarshan Guruacharya

Green Internet of Things (IoT): Enabling Technologies, Architectures, Performance, and Design Issues

Wireless Communications and Mobile Computing

Green Internet of Things (IoT): Enabling Technologies, Architectures, Performance, and Design Issues

Lead Guest Editor: Hina Tabassum
Guest Editors: Mahdi Ben Ghorbel, Hesham Elsawy, Wael Guibene, and Sudarshan Guruacharya

Editorial Board

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3747562, 2 pages
https://doi.org/10.1155/2018/3747562

Editorial

Green Internet of Things (IoT): Enabling Technologies, Architectures, Performance, and Design Issues

Hina Tabassum,[1] **Mahdi Ben Ghorbel**,[2] **Hesham Elsawy**,[3] **Wael Guibene**,[4] **and Sudarshan Guruacharya**[5]

[1] *York University, Canada*
[2] *University of British Columbia (UBC), Canada*
[3] *King Abdullah University of Science and Technology (KAUST), Saudi Arabia*
[4] *Intel, USA*
[5] *University of Manitoba, Canada*

Correspondence should be addressed to Hina Tabassum; hina.tabassum@kaust.edu.sa

Received 12 August 2018; Accepted 12 August 2018; Published 2 September 2018

While research and development in the area of energy-efficient communications are now mature, energy-efficient solutions for emerging Internet of Things (IoT) are far from being explored. IoT systems are envisioned to revolutionize the telecommunication paradigm by allowing direct integration between the physical world and machine-based systems. IoT systems allow everything (household items, vehicles, sensors, and wearables) to be connected, remotely accessed, sensed, and collaboratively communicate over the Internet. All IoT devices are supposed to be equipped with additional sensory and communication add-ons and in turn consume extra energy to sense the world and communicate with each other. As such, new energy harvesting technologies, ambient backscattering, and energy-aware learning and cryptography techniques are of immediate relevance.

After a critical review process, we selected five articles for this special issue that elaborates the performance of some of the aforementioned techniques and in turn contribute to green IoT technology. An interesting contribution "Performance Analysis of RF-Powered Cognitive Radio Networks with Integrated Ambient Backscatter Communications" from L. Xu et al. utilizes backscatter communication for the activation of low power devices. Stochastic geometry tools have been used to evaluate the overall cognitive IoT network performance. Simple energy storage and reusing mechanisms have been designed to improve utilization of harvested energy. Another important contribution by M. Ozturk et al. is "Energy-Aware Smart Connectivity for IoT Networks: Enabling Smart Ports". This work is focused on providing a novel approach for energy-aware and context-aware IoT connectivity that jointly optimizes the energy, security, computational power, and response time of the connection. The proposed scheme employs reinforcement learning and manages to achieve a holistic gain of up to 283.54% compared to deterministic routes.

Another interesting research work "Mobility-Centric Analysis of Communication Offloading for Heterogeneous Internet of Things Devices" presented by D. Kozyrev et al. developed a framework to understand the network connectivity of wearable IoT devices such as smart watches and heart rate monitors. These devices are mobile and are connected via D2D-link to another device, usually a smart phone, which is connected to a base station. An aerial access point is assumed to provide a control link to the D2D pairs located in its coverage area, for offloading the cellular network load, whenever possible. Such an offloading scheme helps in reducing the overall energy consumed by the network.

Cooperative spectrum sensing in cognitive vehicular networks (CVNs) is investigated in the paper titled "Robust and Low-Complexity Cooperative Spectrum Sensing via Low-Rank Matrix Recovery in Cognitive Vehicular Networks" by X. Liu et al. Robust cooperative spectrum sensing using low-rank matrix recovery is proposed to address the uncertainty of the quality of potentially corrupted sensing data. The technique exploits the low-rank and joint-sparse structure of the real spectrum occupancy matrix and corrupted data matrix.

The technique is extended to dense cognitive vehicular networks using weighted low-rank matrix recovery to reduce the complexity. Clearly, reduced complexity of spectrum sensing in cognitive vehicular networks results in energy-efficient architecture and resource management solutions for green IoT.

Another work "Cryptographic Algorithm Invocation Based on Software-Defined Everything in IPsec" by X. Yang et al. proposes a simple and flexible method to add and switch between various cryptographic algorithms in Internet Protocol Security (IPsec) suite in IPv6. This is very important since IoT requires the support of IPv6 to provide enough IP addresses for IoT devices. However, the existing cryptographic algorithms in IPsec suite may not afford enough network security for specific IoT applications, or the default algorithms in IPsec may not be applicable in specific situations. Thus, addition and timely switching of customized algorithms are important in IPsec. Unfortunately, doing this in current IPsec is quite complicated. Thus, this work is important in remedying this situation. Such efficient security methods help to reduce energy consumption of the IoT devices.

This special issue opens new directions for the research on green IoT and highlights the benefits of ambient backscattering, energy-aware learning, energy-efficient spectrum sensing, and computational offloading in emerging IoT networks.

Conflicts of Interest

The author declare that there are no conflicts of interest regarding the publication of this article.

Hina Tabassum
Mahdi Ben Ghorbel
Hesham Elsawy
Wael Guibene
Sudarshan Guruacharya

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3761075, 11 pages
https://doi.org/10.1155/2018/3761075

Research Article

Mobility-Centric Analysis of Communication Offloading for Heterogeneous Internet of Things Devices

Dmitry Kozyrev,[1,2] Aleksandr Ometov,[3] Dmitri Moltchanov,[3] Vladimir Rykov,[1,4] Dmitry Efrosinin,[1,2] Tatiana Milovanova,[1] Sergey Andreev,[3] and Yevgeni Koucheryavy[3]

[1] *RUDN University, Moscow, Russia*
[2] *V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia*
[3] *Tampere University of Technology, Tampere, Finland*
[4] *Gubkin Russian State University of Oil and Gas, Moscow, Russia*

Correspondence should be addressed to Aleksandr Ometov; aleksandr.ometov@tut.fi

Received 6 April 2018; Revised 30 June 2018; Accepted 12 July 2018; Published 5 August 2018

Academic Editor: Sudarshan Guruacharya

Today, the number of interconnected Internet of Things (IoT) devices is growing tremendously followed by an increase in the density of cellular base stations. This trend has an adverse effect on the power efficiency of communication, since each new infrastructure node requires a significant amount of energy. Numerous enablers are already in place to offload the scarce cellular spectrum, thus allowing utilization of more energy-efficient short-range radio technologies for user content dissemination, such as moving relay stations and network-assisted direct connectivity. In this work, we contribute a new mathematical framework aimed at analyzing the impact of network offloading on the probabilistic characteristics related to the quality of service and thus helping relieve the energy burden on infrastructure network deployments.

1. Introduction and Motivation

The uncontrollable growth in the numbers of interconnected Internet of Things (IoT) devices has a tremendously adverse effect on the existing wireless networks [1]. It has been recently shown that there are more than four million base stations (BSs) each consuming an average of 2.3MWh per month [2], and the volume of newly deployed BSs is growing exponentially, especially in the developing counties. Such an extreme energy consumption burden has its influence on the energy costs, greenhouse effect, and global impact on climate in general [3].

One of the ways to control the increase in the numbers of newly deployed BSs is to efficiently utilize the existing system infrastructure [4] by, e.g., attempting to switch between the radio technologies instead of "densifying" the deployment area [5]. This paradigm is known as heterogeneous networking [6] as part of the next-generation (5G) systems and beyond. However, seamless implementation of this approach is associated with many practical difficulties, e.g., when the existing infrastructure is owned by different service providers.

Another potential enabler of green communication is device-to-device (D2D) connectivity [7, 8]. This technique allows reducing power consumption and improving network capacity and throughput by utilizing, e.g., unlicensed wireless spectrum controlled by the operator [9]. Basically, a mobile device equipped with two or more radio interfaces has an opportunity to utilize short-range wireless links to communicate with its neighboring nodes by reaching common goals, like data caching, edge computing, coverage extension, etc. [10]. As cellular spectrum remains expensive in terms of capacity and energy, it could be freed with D2D offloading, thus enabling green communication [11]. In this regime, the cellular network is only responsible for controlling the connection between the user equipment (UE) devices.

One more way to improve the communication quality is based on the use of unmanned aerial vehicles (UAVs). Historically, UAVs have already demonstrated their applicability for weather monitoring, forest fire detection, traffic control, etc.

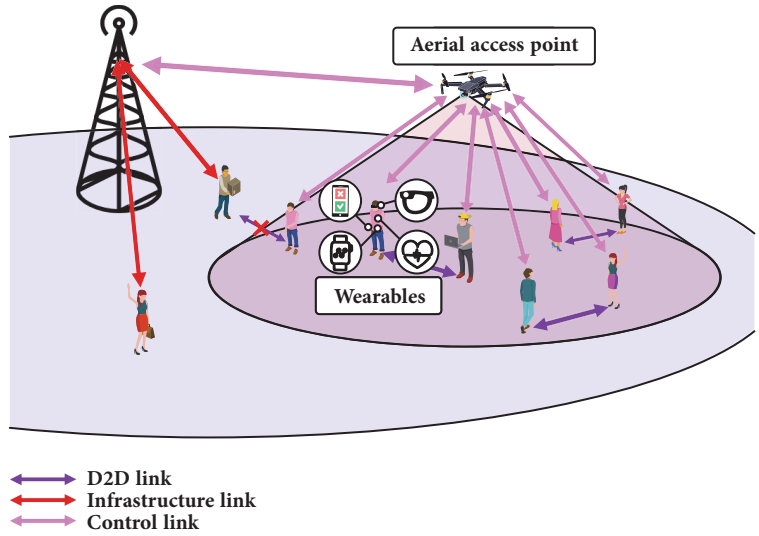


Figure 1: Joint operation of conventional and aerial cells serving D2D links.

[12, 13]. Among the many applications, the use of UAVs for achieving high data-rate wireless communication is expected to play an essential role in future wireless systems. In fact, UAV-aided wireless communication becomes a promising solution to provide wireless connectivity for devices without infrastructure coverage [14]. There has been recent interest in utilizing aerial access points (AAPs) mounted on drones, which could be utilized for offering on-demand connectivity in cases of imminent network overload. Further, AAPs may also be utilized to support the scenarios of Public Protection and Disaster Relief (PPDR) where the connectivity is unavailable due to an unpredictable situation [15].

In addition, a recent exciting trend that overtakes the market is a broad penetration of wearable devices, such as AR-glasses, smart watches, heart rate monitors, and many others. The functions of those are mostly related to human condition monitoring. Note that wearable devices typically have smaller form-factors and thus are limited in terms of computation and energy, which substantiates a natural step of employing one of the devices as a gateway for delivering wearables-generated data to the cloud. Most commonly, a smartphone is utilized as this more powerful node [16].

In this paper, we assess the architecture of (beyond-) 5G systems where a mobile user is equipped with many wearable devices that are continuously exchanging data with the surrounding nodes as well as the cloud via a gateway node. For this purpose, the conventional cellular infrastructure is typically employed, augmented with a D2D-based caching-enabled relay or utilizing other heterogeneous networking solutions. In our scenario, an AAP is further used together with D2D communication to achieve the ultimate goal of offloading the existing cellular network as much as possible. Here, the AAP is expected to provide a control link to the D2D pairs located within the overloaded area of interest, thus relieving the limited cellular spectrum to some extent. This work proposes a new mathematical model to evaluate the probabilistic characteristics of the proposed system architecture.

The rest of the paper is organized as follows. Our system model of the considered scenario is introduced in Section 2. This model is solved for the performance metrics of interest in Section 3. An example illustrating the applicability of the proposed approach is offered in Section 4. The last section concludes the paper.

2. System Model

2.1. Deployment Model. Consider a city square with a mass event (e.g., a concert) in progress, which is shown in Figure 1. The area of interest has a certain number of heterogeneous UEs acting as gateways for their proximate wearable devices and is partially covered by the AAP's connectivity providing aid in communication offloading via D2D link management. New mobile UE can arrive in the cell according to a stochastic process and leave it after a certain random time due to user mobility. All objects in the cell can disseminate their content of interest by utilizing the D2D links.

Since the AAP coverage within the area of interest is limited and potentially provided by the event holders, wireless connectivity outside of this zone is only available through the conventional infrastructure links. The primary goal of the network in the considered scenario is to offload as many communication sessions as possible onto the direct links, thus enabling more power efficient content dissemination. Note that the D2D capacity regarding the quality of service is constrained due to a limited number of channels in one collision domain; i.e., one can estimate the number of D2D pairs that can operate simultaneously under the AAP coverage for a given application.

Since the conventional metrics in such a scenario are well studied in numerous works [17, 18], the primary focus of this paper is set on less popular performance indicators. First, we consider *connection unavailability*, i.e., a situation where one of UE nodes intends to connect to another UE over a D2D link but that second UE is already occupied or a certain UE attempts to reach another device outside of the cell but there

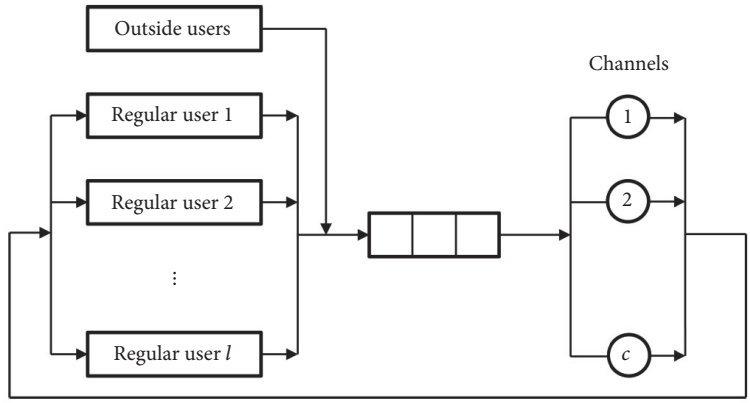


Figure 2: Proposed queuing model.

are no more available D2D links. Another metric of interest is the probability of a connection to be discarded, i.e., when one of the UE nodes leaves the AAP coverage while still having an active connection with another UE inside the same cell.

2.2. Mobility Model. We assume that the initial UE positions follow a Poisson point process (PPP) in $\Re^2$ with the spatial density of λ_U. Let $\lambda_A = \lim_{t \longrightarrow 0} p_A(0,t)/t$, where $p_A(t)$ is the probability of a session initiation over the interval $(0,t)$. It is the temporal intensity of the arrival process from a single UE. Using the superposition property of the point processes, we note that the session arrival process is Poisson with the intensity of $\lambda_A \lambda_U S_A$ sessions per second [19], where S_A is the area of the zone of interest. The choice of the UE that initiates a session is random. Hence, the geometric locations of users associated with a session are distributed uniformly within the AAP's coverage area [20].

To capture the mobility behavior, we assume that humans move according to a random direction model (RDM, [21]), since it characterizes the essentials of random movement while still allowing for a tractable analysis. According to the RDM formulation, the UE first chooses its direction of movement uniformly within $(0, 2\pi)$ and then travels in the selected direction for an exponential amount of time with the parameter ν at the constant speed of v.

2.3. Model Formalization. We assess the AAP service process by utilizing a queuing system model illustrated in Figure 2. We assume that l sessions exist in the system, while there is a certain external flow of impatient heterogeneous sessions, which arrive from the outside of the system according to a Poisson process. Consider that the regular users can connect directly over D2D, while the external users may employ both the infrastructure and the D2D connections.

We also assume that the AAP-served UE arrivals follow a marked point process:

$$Z = \{Z_n = (\xi_n, M_n),\ n = 1, 2, \ldots\}, \tag{1}$$

where ξ_n is the arrival time of n^{th} user and M_n is the UE type, $M_n = i \in \{1, 2, \ldots l\}$. The service times of type-i UE, i.e., the duration of an active session initiated by the i-th UE, and B_i are all random variables with the cumulative distribution function (CDF):

$$B_i(t) = \mathbf{P}\{B_i \leq t\} \quad (i = 1, 2, \ldots, l). \tag{2}$$

Each external session requires exactly one server. The duration of time spent by the i-th user in the D2D service zone is a random variable G_i with the CDF:

$$G_i(t) = \mathbf{P}\{G_i \leq t\} \quad (i, j = 1, 2, \ldots, l). \tag{3}$$

A session is lost during service if the corresponding UE leaves the cell before this session is completed. An arriving session is lost when there are no vacant servers (channels) at the time of its arrival. Finally, a session can be lost if the distance between the communicating users becomes higher than a specified value. We remind that, for the introduced model, we are interested in the performance metrics that characterize the reliability of the system. Primarily, we derive the following parameters: session loss probability, system unavailability, and reliability of a connection.

3. Performance Analysis

In this section, we analyze the proposed system. First, we follow a stochastic geometry approach to characterize the input parameters. Then, we proceed by assessing the specified queuing system for the performance metrics of interest.

3.1. System Parametrization. To completely parametrize our model, we need to provide the following input parameters: (i) distribution of the time interval between UE entries into the D2D service zone, (ii) distribution of the time spent in the D2D service area, (iii) probability that UE having an active D2D session is going to leave the D2D zone before this session ends.

Following [22], the time distribution between the cases when the UE moving according to the RDM model and being initially distributed uniformly in a certain area of interest hits a certain subspace follows an exponential distribution. Note that this result holds when the mean run length in the RDM

model, v/ν, is at least 1/4 of the zone of interest; see [22] for more details. Recall that the stationary distribution of UEs moving in a certain zone is uniform [21].

To determine the parameter of an exponential distribution, we consider an area increment of the D2D service zone ΔS that corresponds to the unit speed v. Assuming a circularly shaped D2D service zone and recalling that the direction of the UE movement is distributed uniformly in $(0, 2\pi)$, we have the following approximation for the temporal intensity of users entering the D2D service zone:

$$\lambda = \frac{1}{2}\lambda_U \left(\pi (r+v)^2 - \pi r^2\right) = \frac{1}{2}\lambda_U \pi v (2r+v), \quad (4)$$

where λ_U is the spatial intensity of UE in the area of interest and r is the radius of the D2D service zone. Observe that the factor 1/2 accounts for a fraction of UEs moving towards the D2D service zone.

The exact distribution of time spent by the UE moving according to the RDM in a certain enclosed subspace is unknown even for simple configurations of the subspace [23]. In this case, the common procedure is to use a diffusion approximation with a suitable diffusion coefficient [24]. However, taking into account our assumptions regarding the mean run length and the diameter of the D2D service zone, we observe that in most cases the UE crosses the D2D service zone without changes in its direction. The length of a random chord, L, which specifies the distance traveled within the D2D service zone, is given by [25]

$$f_L(x) = \frac{2}{\pi\sqrt{4r^2 - x^2}}, \quad 0 < x < 2r, \quad (5)$$

with the mean value of $E[L] = 4r/\pi$, where r is the radius of the D2D service zone. The distribution of time spent in the D2D service zone is obtained by scaling the pdf $f_L(x)$ by the movement speed v [26], which leads to

$$f_T(x) = \frac{2v}{\pi\sqrt{4r^2 - (xv)^2}}, \quad 0 < x < \frac{2r}{v}, \quad (6)$$

where T is the time spent in the D2D service zone.

Finally, we require the probability that the UE leaves the D2D service zone before its active session expires. We have two cases to consider: (i) the session has been initiated before entering the D2D service area and (ii) the session has been initiated when the UE is already in the service area. In the former case, owning to the memoryless property, we do not need to track the backward recurrence time of the session and the sought probability is $p_1 = \mathbb{P}\{T - D > 0\}$, where D is the service duration. Since T and D are independent, by employing a convolution we obtain

$$\begin{aligned} p_1 &= \int_0^\infty \int_0^t f_T(t)\, f_D(t-x)\, dtdx \\ &= \int_0^{2r/v} \int_0^t \frac{2v}{\pi\sqrt{4r^2 - (xv)^2}} \lambda e^{-\lambda(t-x)} dtdx, \end{aligned} \quad (7)$$

which can be produced with a numerical integration.

Let us now determine the probability that the UE leaves the D2D service zone before its session is completed given that it was initiated after entering the zone, p_2. Observe that since a session is assumed to be initiated randomly and should progress over the time the UE spends in the D2D service zone, it is distributed uniformly over T. Then, the forward recurrent time that the UE spends in the zone once its session was initiated at the time instant x is [26]

$$f_T(t + x \mid x) = \frac{f_T(t+x)}{1 - F_T(x)}, \quad (8)$$

where $F_T(x)$ is the CDF of time spent by the UE in the D2D service zone, which is given by

$$F_T(x) = \frac{1}{\pi} 2v \tan^{-1}\left(\frac{x}{\sqrt{4r^2v^2 - x^2}}\right), \quad 0 < x < 2rv. \quad (9)$$

Substituting (9) into (8), we obtain

$$f_T(t + x \mid x) = \frac{2\left(4r^2 - (t+x)^2/v^2\right)^{-1/2}}{2v \tan^{-1}\left(x/v\sqrt{\pi - 4r^2 - x^2/v^2}\right)}. \quad (10)$$

The unconditional pdf of time that the UE spends in the D2D coverage zone after initiating its session is given by

$$f_{T_R}(t) = \int_0^\infty f_T(t + x \mid x)\, f_T(x)\, dx. \quad (11)$$

Further, the sought probability is given by

$$p_2 = \int_0^\infty \int_0^t f_{T_R}(t)\, f_D(t-x)\, dtdx, \quad (12)$$

which can be produced with a numerical integration.

3.2. Problem Setting. To solve the problem formulated above, we introduce the system state space E. Let us denote the system state by the following triplet:

$$x = \left(k, i, \vec{d}\right), \quad (13)$$

where $k = 0, 1, 2, \ldots$ is the number of infrastructure controlled UEs, i $(0 \le i \le \min\{c, k + [l/2]\})$ is the number of occupied channels, and $\vec{d} = (d_1, \ldots d_l)$ is the vector of states of the UE. The value of d_j is set according to the following rules: (i) $d_j = 0$ when the j-th user does not have any ongoing sessions; (ii) $d_j = i$ when the j-th UE is currently connected to the i-th UE directly; and (iii) $d_j = \star$ when the j-th UE utilizes one of the infrastructure links.

The overall state space E is then defined as a set of triplets: $E = \{x = (k, i, \vec{d}) : k \in \mathbb{Z}, i \in \mathbb{Z}, \vec{d} = (d_1, \ldots d_l)\}$. We introduce a random process $X(t) = \{K(t)I(t), \vec{D}(t), t \in R_+\}$ evolving over E, which enters the state $x \in E$ if the system at time t is in the state x. We also introduce the state probabilities of the system $\pi(x,t) = \mathbb{P}\{X(t) = x\}$ and the

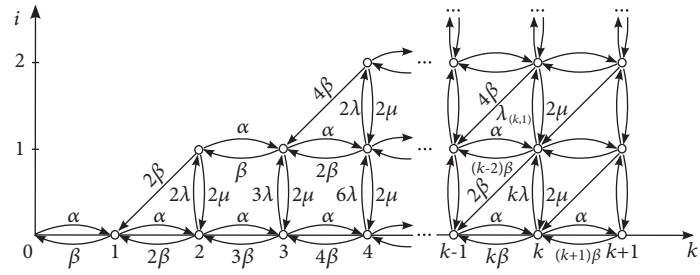


Figure 3: Transition graph of the process X.

steady-state probabilities $\lim_{t\longrightarrow\infty}\pi(x,t)=\pi(x)$. The steady-state distribution of this process $\overrightarrow{\pi}$ is characterized by linear equations in the following form:

$$\begin{aligned}\overrightarrow{Q}\overrightarrow{\pi}&=\overrightarrow{0}^{\mathsf{T}},\\ \overrightarrow{\pi}^{\mathsf{T}}\overrightarrow{e}&=1,\end{aligned}\tag{14}$$

where $\overrightarrow{e}$ is the vector of ones of the appropriate size and Q is the infinitesimal generator of the Markov process. One may solve it by using the conventional techniques; see, e.g., [27].

4. A Numerical Example

To demonstrate the applicability of the proposed model, consider the simplest case without the pure infrastructure connected UEs, when

(i) the users arrive into the system according to a Poisson flow of intensity α;

(ii) the distribution of the sojourn time of any user in the cell is exponential with the parameter β:

$$B(t)=\beta e^{-\beta t};\tag{15}$$

(iii) the process of contacts between the users is also Poisson with the intensity of λ;

(iv) the duration of the user sessions G has an exponential distribution with the parameter μ:

$$G(t)=\mu e^{-\mu t};\tag{16}$$

(v) only $c=3$ infrastructure links are available for the connections.

We also assume full control of the D2D links as managed by the network operator. To characterize the system behavior, consider a two-dimensional stochastic process $X=\{X(t)=(K(t),I(t)),t\in R_+\}$ with the state space:

$$E=\bigcup_{k\geq 0}E_k,\quad \text{with } E_k=\left\{x=(k,i):\ i=\overline{0,3}\right\},\tag{17}$$

where k is the number of users in the system and i is the number of occupied D2D links. The state space of the process X is demonstrated in Figure 3 together with its transition graph.

The subsets $E_0=\{(0,0)\}$ and $E_1=\{(1,0)\}$ represent a single state, the subsets $E_2=\{(2,0),(2,1)\}$ and $E_3=\{(3,0),(3,1)\}$ contain two states, the subsets $E_4=\{(4,0),(4,1),(4,2)\}$ and $E_5=\{(5,0),(5,1)\ (5,2)\}$ contain three states, and only for $k\geq 6$ the number of states is equal to four. Note that in case where the servers and/or users are heterogeneous, to describe the system behavior with a Markov process, the subsets of states E_k with a fixed number k of users in the system should be detailed in order to show the configuration of the busy servers. With the help of the constructed stochastic process $X(t)$, we will study the quality-of-service (QoS) metrics in the considered system, i.e., the probability of a connection loss (when a user with no ongoing session leaves the service area), the probability of connection unavailability (when there are no vacant channels in the system), and the average number of busy channels.

Under the given assumptions, the process $X(t)$ may be considered as Markov, and its transition intensities have the following forms:

(1) α_k is the transition intensity from the state (k,i) to the state $(k+1,i)$, which occurs when a user enters the system.

(2) $\beta_{(k,i)}$ is the transition intensity from the state (k,i) to the state $(k-1,i)$, which occurs when a user with no ongoing session leaves the system.

(3) $\beta^{-}_{(k,i)}$ is the transition intensity from the state (k,i) to the state $(k-1,i-1)$, which occurs when a user with an ongoing session leaves the system.

(4) $\lambda_{(k,i)}$ is the transition intensity from the state (k,i) to the state $(k,i+1)$, which occurs when a user with no ongoing session initiates a session.

(5) $\mu_{(k,i)}$ is the transition intensity from the state (k,i) to the state $(k,i-1)$, which occurs when a user with an ongoing session ends this session.

Consider the state (k,i). Since i channels are occupied by exactly $2i$ users (2 users are connected via a single D2D link), the number of users with no ongoing session is $k-2i$, the number of users with an ongoing session is $2i$, and the number of possible ways to choose a pair of users out of $k-2i$ nonbusy users to initiate a session is $\binom{k-2i}{2}$. Therefore,

we arrive at the following expressions for the transition intensities:

$$\begin{aligned} \alpha_k &= \alpha, \\ \beta_{(k,i)} &= (k-2i)\,\beta, \\ \beta^{-}_{(k,i)} &= 2i\beta, \\ \lambda_{(k,i)} &= \binom{k-2i}{2}\lambda, \\ \mu_{(k,i)} &= 2i\mu, \end{aligned} \tag{18}$$

where $i = 0$ for $k = 0, 1$, $i = 0, 1$ for $k = 2, 3$, $i = 0, 1, 2$ for $k = 4, 5$, and $i = 0, 1, 2, 3$ for $k \geq 6$.

The process transition intensity matrix has the following blockwise structure

$$Q = \begin{pmatrix} B_0 & C_0 & 0 & 0 & 0 & \dots \\ A_1 & B_1 & C_1 & 0 & 0 & \dots \\ 0 & A_2 & B_2 & C_2 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{19}$$

where the k-th blockwise row corresponds to the subset E_k of states for which k users are present in the system, A_k describes the output from this subset to the subset with $k-1$ users in the system, B_k describes the transitions inside the subset with k users in the system, and C_k contains the output intensities from the subset E_k to the subset E_{k+1}. Transition matrices for the considered example are as follows:

$$\begin{aligned} B_0 &= -\alpha, \\ C_0 &= \alpha. \end{aligned} \tag{20}$$

$$\begin{aligned} A_1 &= \beta, \\ B_1 &= -(\alpha+\beta), \\ C_1 &= (\alpha \;\; 0). \end{aligned} \tag{21}$$

$$\begin{aligned} A_2 &= \begin{pmatrix} 2\beta \\ 2\beta \end{pmatrix}, \\ C_2 &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}. \end{aligned} \tag{22}$$

$$B_2 = \begin{pmatrix} -(\alpha+2\beta+\lambda) & \lambda \\ 2\mu & -(\alpha+2\beta+2\mu) \end{pmatrix}. \tag{23}$$

$$\begin{aligned} A_3 &= \begin{pmatrix} 3\beta & 0 \\ 2\beta & \beta \end{pmatrix}, \\ C_3 &= \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \end{pmatrix}. \end{aligned} \tag{24}$$

$$B_3 = \begin{pmatrix} -(\alpha+3\beta+3\lambda) & 3\lambda \\ 2\mu & -(\alpha+3\beta+2\mu) \end{pmatrix}. \tag{25}$$

$$\begin{aligned} A_4 &= \begin{pmatrix} 4\beta & 0 \\ 2\beta & 2\beta \\ 0 & 4\beta \end{pmatrix}, \\ C_4 &= \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \end{pmatrix}. \end{aligned} \tag{26}$$

$$B_4 = \begin{pmatrix} -(\alpha+4\beta+6\lambda) & 6\lambda & 0 \\ 2\mu & -(\alpha+4\beta+2\lambda+2\mu) & 2\lambda \\ 0 & 2\mu & -(\alpha+2\mu+4\beta) \end{pmatrix}. \tag{27}$$

$$A_5 = \begin{pmatrix} 5\beta & 0 & 0 \\ 2\beta & 3\beta & 0 \\ 0 & 4\beta & \beta \end{pmatrix},$$
$$C_5 = \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \end{pmatrix}. \tag{28}$$

$$B_5 = \begin{pmatrix} -(\alpha + 5\beta + 10\lambda) & 10\lambda & 0 \\ 2\mu & -(\alpha + 5\beta + 3\lambda + 2\mu) & 3\lambda \\ 0 & 4\mu & -(\alpha + 4\mu + 5\beta) \end{pmatrix}. \tag{29}$$

Further, for $k \geq 6$, the matrices have the form

$$A_k = \begin{pmatrix} k\beta & 0 & 0 & 0 \\ 2\beta & (k-2)\beta & 0 & 0 \\ 0 & 4\beta & (k-4)\beta & 0 \\ 0 & 0 & 6\beta & (k-6)\beta \end{pmatrix},$$
$$C_k = \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}. \tag{30}$$

$$B_k = \begin{pmatrix} -b_{(k,0)} & \binom{k}{2}\lambda & 0 & 0 \\ 2\mu & -b_{(k,1)} & \binom{k-2}{2}\lambda & 0 \\ 0 & 4\mu & -b_{(k,2)} & \binom{k-4}{2}\lambda \\ 0 & 0 & 6\mu & -b_{(k,3)} \end{pmatrix}, \tag{31}$$

where the diagonal elements are

$$b_{k,0} = \left(\alpha + k\beta + \binom{k}{2}\lambda\right),$$
$$b_{k,1} = \left(\alpha + k\beta + \binom{k-2}{2}\lambda + 2\mu\right),$$
$$b_{k,2} = \left(\alpha + \binom{k-4}{2}\lambda + 4\mu + k\beta\right), \tag{32}$$
$$b_{k,3} = (\alpha + 6\mu + k\beta).$$

The blockwise form of the matrix Q represents the steady-state probability (s.s.p.) vector in the blockwise form of the appropriate dimensions that provides $\overrightarrow{\pi}^{\mathsf{T}} = (\pi_0, \pi_1, \overrightarrow{\pi}_2, \ldots, \overrightarrow{\pi}_k, \ldots)$. Hence, the balance equations may be represented as

$$\begin{aligned} 0 &= -\alpha\pi_0 + \beta\pi_1, \\ 0 &= \alpha\pi_0 - (\alpha + \beta)\pi_1 + 2\beta(\pi(2,0) + \pi(2,1)), \\ 0 &= \pi_1 C_1 + \overrightarrow{\pi}_2^{\mathsf{T}} B_2 + \overrightarrow{\pi}_3^{\mathsf{T}} A_3, \\ 0 &= \overrightarrow{\pi}_{k-1}^{\mathsf{T}} C_{k-1} + \overrightarrow{\pi}_k^{\mathsf{T}} B_k + \overrightarrow{\pi}_{k+1}^{\mathsf{T}} A_{k+1}, \quad k \geq 3 \end{aligned} \tag{34}$$

with the normalizing condition

$$\pi_0 + \pi_1 + \sum_{k=2}^{\infty} \overrightarrow{\pi}_k^{\mathsf{T}} \overrightarrow{1} = 1, \tag{35}$$

where $\overrightarrow{1}$ is a column-vector, while its components are equal to 1.

By using A_k, B_k, C_k for $k \geq 3$, we arrive at

$$\begin{aligned} A_{k-1}\overrightarrow{1} &= (k-1)\beta\overrightarrow{1}, \\ B_k\overrightarrow{1} &= -(\alpha + k\beta)\overrightarrow{1}, \\ C_{k+1}\overrightarrow{1} &= \alpha\overrightarrow{1}. \end{aligned} \tag{36}$$

Further, we multiply (34) by $\overrightarrow{1}$ as

$$\pi_k = \overrightarrow{\pi}_k^{\mathsf{T}} \overrightarrow{1}, \tag{37}$$

with the following birth-and-death s.s.p. equation:

$$\alpha\pi_{k-1} - (\alpha + k\beta)\pi_k + (k+1)\beta\pi_{k+1} = 0. \tag{38}$$

For $k \geq 3$, this gives us

$$\alpha\pi_{k-1} k\beta\pi_k = \alpha\pi_k (k+1)\beta\pi_{k+1}. \tag{39}$$

However, the same equalities can be obtained from (34), thus confirming it for $k \leq 3$:

$$0 = \alpha\pi_0\beta\pi_1 = \alpha\pi_1 2\beta\pi_2 = \alpha\pi_k (k+1)\beta\pi_{k+1}. \tag{40}$$

The solution to this system of equations for all $k \geq 0$ with the normalizing condition (35) and with $\rho = \alpha/\beta$ is

$$\pi_k = \frac{\alpha}{k\beta}\pi_{k-1} = \frac{\rho^k}{k!}\pi_0 = \frac{\rho^k}{k!}e^{-\rho}, \tag{41}$$

which is a Poisson distribution of the number of users in the system.

In order to calculate the probabilities of interest, there is a need to evaluate $\pi_{(k,i)}$, which requires a more detailed analysis. To achieve this goal, the process X on the separate subset of states should be considered as $E_k = \{(k,0);(k,1);(k,2);(k,3)\}$. Taking into account X and its transition graph (see Figure 3), it is clear that each of the subsets E_0, E_1 contains only one state; hence, the corresponding probabilities are given with (41) as

$$\begin{aligned} \pi_0 &= e^{-\rho}, \\ \pi_1 &= \rho e^{-\rho}. \end{aligned} \tag{42}$$

For the subsets E_k, the process X is a birth-death process with the birth $\lambda_{(k,i)} = \binom{k-2i}{2}\lambda$ and death $\mu_{(k,i)} = 2i\mu$ (see Figure 3) intensities. Therefore, the detailed balance equations may be utilized to establish the results for $k = 2, 3$:

$$\binom{k}{2}\lambda\pi_{(k,0)} = 2\mu\pi_{(k,1)}, \tag{43}$$

additionally for $k = 4, 5$

$$\binom{k-2}{2}\lambda\pi_{(k,1)} = 4\mu\pi_{(k,2)}, \tag{44}$$

at least for all $k \geq 6$, and

$$\binom{k-4}{2}\lambda\pi_{(k,2)} = 6\mu\pi_{(k,3)}. \tag{45}$$

For the probabilities of the subsets E_k, by taking into account (41) and using the notation $\gamma = \lambda/\mu$, the following expressions for the probabilities $\pi_{(k,i)}$ for $k \geq 2$ can be derived:

$$\begin{aligned} \pi_{(2,0)} &= \frac{1}{1+\gamma/2}\frac{\rho^2}{2!}e^{-\rho}, \\ \pi_{(2,1)} &= \frac{\gamma/2}{1+\gamma/2}\frac{\rho^2}{2!}e^{-\rho}, \end{aligned} \tag{46}$$

$$\begin{aligned} \pi_{(3,0)} &= \frac{1}{1+(3/2)\gamma}\frac{\rho^3}{3!}e^{-\rho}, \\ \pi_{(3,1)} &= \frac{(3/2)\gamma}{1+(3/2)\gamma}\frac{\rho^3}{3!}e^{-\rho}, \end{aligned} \tag{47}$$

$$\begin{aligned} \pi_{(4,0)} &= \frac{1}{1+3\gamma\left(1+(1/4)\gamma\right)}\frac{\rho^4}{4!}e^{-\rho}, \\ \pi_{(4,1)} &= \frac{3\gamma}{1+3\gamma\left(1+(1/4)\gamma\right)}\frac{\rho^4}{4!}e^{-\rho}, \\ \pi_{(4,2)} &= \frac{(3/4)\gamma^2}{1+3\gamma\left(1+(1/4)\gamma\right)}\frac{\rho^4}{4!}e^{-\rho}, \end{aligned} \tag{48}$$

$$\begin{aligned} \pi_{(5,0)} &= \frac{1}{1+5\gamma\left(1+(3/4)\gamma\right)}\frac{\rho^5}{5!}e^{-\rho}, \\ \pi_{(5,1)} &= \frac{5\gamma}{1+5\gamma\left(1+(3/4)\gamma\right)}\frac{\rho^5}{5!}e^{-\rho}, \\ \pi_{(5,2)} &= \frac{(15/4)\gamma^2}{1+5\gamma\left(1+(3/4)\gamma\right)}\frac{\rho^5}{5!}e^{-\rho}. \end{aligned} \tag{49}$$

For $k \geq 6$, the following holds:

$$\begin{aligned} \pi_{(k,0)} &= c_k\frac{\rho^k}{k!}e^{-\rho}, \\ \pi_{(k,1)} &= c_k\frac{k(k-1)}{4}\gamma\frac{\rho^k}{k!}e^{-\rho}, \\ \pi_{(k,2)} &= c_k\frac{k(k-1)}{4}\gamma\left(1+\frac{(k-2)(k-3)}{8}\gamma\right)\frac{\rho^k}{k!}e^{-\rho}, \\ \pi_{(k,3)} &= c_k\frac{k(k-1)}{4} \\ &\quad\cdot\gamma\left(1+\frac{(k-2)(k-3)}{8}\gamma\left(1+\frac{(k-4)(k-5)}{12}\gamma\right)\right) \\ &\quad\cdot\frac{\rho^k}{k!}e^{-\rho}, \end{aligned} \tag{50}$$

where

$$\begin{aligned} c_k = \Bigg[1+\Bigg(\frac{k(k-1)}{4}\gamma\Bigg(3 \\ +\frac{(k-2)(k-3)}{8}\gamma\left(2+\frac{(k-4)(k-5)}{12}\gamma\right)\Bigg)\Bigg)\Bigg]^{-1}. \end{aligned} \tag{51}$$

Based on the above set of probabilities, it is possible to calculate the sought QoS characteristics, such as the following.

(1) Probability of a connection loss π_{loss} due to leaving the AAP coverage area by one of the users: Here, a loss of connection occurs in case where the process transitions from the state (k,i) to the state $(k-1,i-1)$, which is only possible for the states (k,i) with $i > 0$

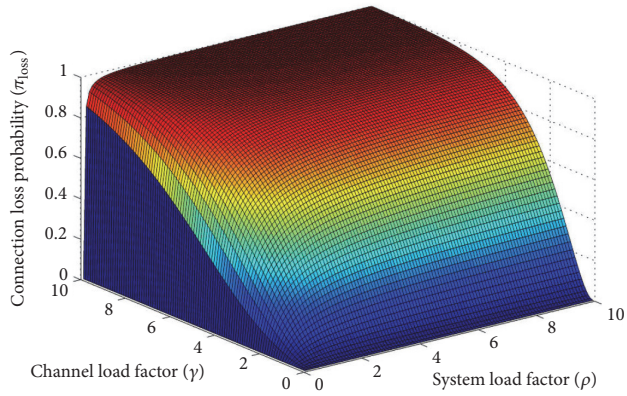


FIGURE 4: Probability π_{loss} versus different values of γ and ρ.

and $k \geq 2$. Hence, the connection loss may be derived as

$$\begin{aligned}\pi_{\text{loss}} &= \pi_{(2,1)}\frac{2\beta}{\alpha+2\beta+2\mu} + \pi_{(3,1)}\frac{2\beta}{\alpha+\beta+2\mu+2\beta} \\ &+ \pi_{(4,1)}\frac{2\beta}{\alpha+4\beta+\lambda+2\mu} + \pi_{(4,2)}\frac{4\beta}{\alpha+4\beta+2\mu} \\ &+ \pi_{(5,1)}\frac{2\beta}{\alpha+5\beta+3\lambda+2\mu} + \pi_{(5,2)}\frac{4\beta}{\alpha+5\beta+4\mu} \\ &+ \sum_{k\geq 6}\left(\pi_{(k,1)}\frac{2\beta}{\alpha+k\beta+\binom{k-2}{2}\lambda+2\mu}\right. \\ &+ \pi_{(k,2)}\frac{4\beta}{\alpha+k\beta+\binom{k-4}{2}\lambda+4\mu} \\ &\left.+ \pi_{(k,3)}\frac{6\beta}{\alpha+k\beta+6\mu}\right).\end{aligned} \tag{52}$$

The plots of the loss probabilities π_{loss} versus the parameters ρ and γ are given in Figure 4. Since the parameter γ is defined as a ratio between the session initiation intensity λ and the intensity of the session termination flow μ, the physical meaning of this parameter is the channel load. The parameter $\rho = \alpha/\beta$ is the system load factor (or traffic load), which can be interpreted as a relative rate of populating the cell by the outside users.

Then, it is obvious that, at the zero level of ρ, i.e., when no users are entering the cell, the connection loss probability π_{loss} remains zero for any value of the parameter γ. However, as the system load factor ρ increases, the probability π_{loss} also grows, as it can be observed in Figure 4: the higher the value of the parameter γ is, the steeper the curve of π_{loss} on γ becomes. This behavior is easily explained by the fact that both parameters affect the occupation intensity for the free channels, which are limited in their number, by the users entering the cell. Since the users leave the cell regardless of whether they occupy the server (channel) or not, the probability of a connection loss increases with the growth of either parameter.

(2) Probability that i D2D channels are currently occupied is

$$\pi_{i,\text{busy}} = \sum_{k\geq 2}\pi_{(k,i)}, \tag{53}$$

while the mean number of busy channels is

$$\pi_{\text{busy-mean}} = \sum_{1\leq i\leq 3} i\pi_{i,\text{busy}}, \tag{54}$$

and the connection unavailability intensity is $\beta\pi_{\text{busy-mean}}$.

(3) Probability of a connection unavailability state is possible to derive only if the number of users is not less than 6. Hence, the probability of a connection unavailability becomes

$$\pi_{\text{unav}} = \sum_{x:i=3}\pi(x) = \sum_{k\geq 6}\pi_{(k,3)}, \tag{55}$$

while the intensity of unavailable connections is $\lambda\pi_{\text{unav}}$.

The plots for the unavailability probabilities π_{unav} versus the parameters ρ and γ are displayed in Figure 5. The behavior of the curves of the connection unavailability probability π_{unav} is similar in many ways to that of π_{loss}, as π_{unav} directly correlates with the parameters γ and ρ. If the value of any of the associated parameters is zero, the probability of a connection unavailability is also zero, since either the system lacks users (parameter ρ), or there are no users willing to initiate a connection session, i.e., zero loads on the channels (parameter γ). As each of these parameters grows, the probability to have an available unoccupied channel for establishing another connection between the activating users decreases.

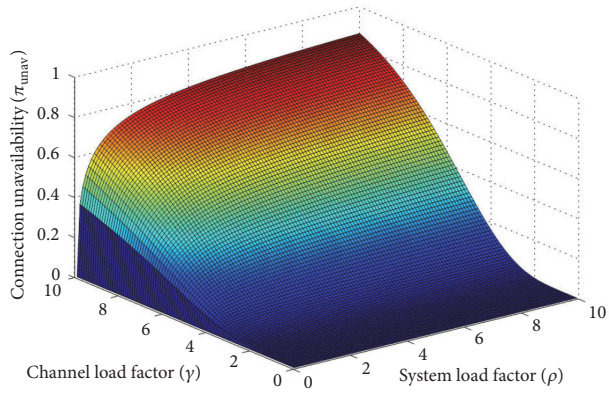


FIGURE 5: Probability π_{unav} versus different values of γ and ρ.

The considered model admits useful generalizations that may include different types of heterogeneous users, different types of input processes for the outside users, and different mechanisms of their service.

5. Conclusion

In today's wireless networks, multiple enablers are available to offload the expensive cellular spectrum, thus allowing utilization of more efficient short-range radio technologies for user content dissemination. This work proposed a novel mathematical framework that enables assessing the impact of network offloading on the probabilistic characteristics related to the quality of service. We demonstrated that our developed model may be employed when an aerial access point conducts D2D link management based on the channel and system loads. The results reported useful knowledge of connection unavailability and connection loss probabilities.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The publication was supported by the Ministry of Education and Science of the Russian Federation (Project no. 2.882.2017/4.6).

References

[1] M. Z. Shakir, K. A. Qaraqe, H. Tabassum, M.-S. Alouini, E. Serpedin, and M. Imran, "Green heterogeneous small-cell networks: Toward reducing the CO2 emissions of mobile communications industry using uplink power adaptation," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 52–61, 2013.

[2] C. Gao, X. Sheng, J. Tang, W. Zhang, S. Zou, and M. Guizani, "Joint mode selection, channel allocation and power assignment for green device-to-device communications," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 178–183, Sydney, NSW, June 2014.

[3] B. Lee, "Energy Efficiency Gain of Cellular Base Stations with Large-Scale Antenna Systems for Green Information and Communication Technology," *Sustainability*, vol. 9, no. 7, p. 1123, 2017.

[4] T. Zhou, N. Jiang, D. Qin, Z. Liu, and C. Li, "Joint Cell Selection and Activation for Green Communications in Ultra-Dense Heterogeneous Networks," in *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 32–37, Guangzhou, China, July 2017.

[5] U. Siddique, H. Tabassum, E. Hossain, and D. I. Kim, "Wireless backhauling of 5G small cells: challenges and solution approaches," *IEEE Wireless Communications Magazine*, vol. 22, no. 5, pp. 22–31, 2015.

[6] V. Jungnickel, K. Manolakis, W. Zirwas et al., "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 44–51, 2014.

[7] J. An, K. Yang, J. Wu, N. Ye, S. Guo, and Z. Liao, "Achieving Sustainable Ultra-Dense Heterogeneous Networks for 5G," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 84–90, 2017.

[8] A. H. Sakr, H. Tabassum, E. Hossain, and D. I. Kim, "Cognitive spectrum access in device-to-device-enabled cellular networks," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 126–133, 2015.

[9] S. Andreev, J. Hosek, T. Olsson et al., "A unifying perspective on proximity-based cellular-assisted mobile social networking," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 108–116, 2016.

[10] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3GPP device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 40–48, 2014.

[11] E. Yaacoub, H. Ghazza, and M.-S. Alouini, "A game theoretic framework for green hetnets using D2D traffic offload and renewable energy powered base stations," *Game Theory Framework Applied to Wireless Communication Networks*, pp. 333–367, 2015.

[12] G. Pajares, "Overview and current status of remote sensing applications based on unmanned aerial vehicles (UAVs)," *Photogrammetric Engineering and Remote Sensing*, vol. 81, no. 4, pp. 281–329, 2015.

[13] L. Wang, B. Hu, and S. Chen, "Energy Efficient Placement of a Drone Base Station for Minimum Required Transmit Power," *IEEE Wireless Communications Letters*, pp. 1-1, 2018.

[14] K. Gomez, S. Kandeepan, M. M. Vidal et al., "Aerial base stations with opportunistic links for next generation emergency communications," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 31–39, 2016.

[15] T. J. Tanzi, M. Chandra, J. Isnard, D. Camara, O. Sebastien, and F. Harivelo, "Towards "drone-based" disaster management: future application scenarios," *ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. III-8, pp. 181–189, 2016.

[16] G. Aloi, G. Caliciuri, G. Fortino et al., "Enabling IoT interoperability through opportunistic smartphone-based mobile gateways," *Journal of Network and Computer Applications*, vol. 81, pp. 74–84, 2017.

[17] K. Gomez, A. Hourani, L. Goratti, R. Riggio, S. Kandeepan, and I. Bucaille, "Capacity evaluation of Aerial LTE base-stations for public safety communications," in *Proceedings of the European Conference on Networks and Communications, EuCNC*, pp. 133–138, France, July 2015.

[18] S. Chandrasekharan, S. Kandeepan, R. J. Evans et al., "Clustering approach for aerial base-station access with terrestrial cooperation," in *Proceedings of the IEEE Globecom Workshops, GC Wkshps 2013*, pp. 1397–1402, USA, December 2013.

[19] J. F. Kingman, *Poisson processes*, vol. 3 of *Oxford Studies in Probability*, The Clarendon Press, Oxford University Press, New York, 1993.

[20] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.

[21] P. Nain, D. Towsley, B. Liu, and Z. Liu, "Properties of random direction models," in *Proceedings of the Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, pp. 1897–1907, Miami, FL, USA.

[22] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Performance Evaluation*, vol. 62, no. 1-4, pp. 210–228, 2005.

[23] G. H. Weiss and R. J. Rubin, "Random Walks: Theory and Selected Applications," in *Advances in Chemical Physics*, Advances in Chemical Physics, pp. 363–505, John Wiley & Sons, Inc., Hoboken, NJ, USA, 1982.

[24] S. Redner, *A Guide to First-Passage Processes*, Cambridge University Press, Cambridge, UK, 2001.

[25] A. M. Mathai, *An introduction to geometrical probability*, vol. 1 of *Statistical Distributions and Models with Applications*, Gordon and Breach Science Publishers, Amsterdam, 1999.

[26] S. M. Ross, *Introduction to probability models*, Elsevier/Academic Press, Amsterdam, Eleventh edition, 2014.

[27] G. Bolch, S. Greiner, H. de Meer, and K. S. Trivedi, *Queueing networks and Markov chains*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., 1998.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8728424, 11 pages
https://doi.org/10.1155/2018/8728424

Research Article

Cryptographic Algorithm Invocation Based on Software-Defined Everything in IPsec

Ximin Yang,[1] Deqiang Wang,[1] Wei Feng,[1] Jingjing Wu,[2] and Wan Tang [1]

[1]*College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China*
[2]*Tongfang Computer Co., Ltd., Wuxi 214000, China*

Correspondence should be addressed to Wan Tang; tangwan@scuec.edu.cn

Received 26 January 2018; Revised 1 May 2018; Accepted 21 May 2018; Published 2 July 2018

Academic Editor: Sudarshan Guruacharya

IPsec was initially developed for IPv6 to ensure the communication security. With the development of Internet of Things (IoT) and the mounting importance of network security, increasing numbers of applications require IPsec to support the customized definition of cryptographic algorithms and to provide flexible invocation of these algorithms. To address this issue, an invocation mechanism for cryptographic algorithms is proposed in this paper and applied to IPsec, entitled Free to Add (FTA), based on the concept of software-defined everything. Using the idea of interface opening, the addition of a new cryptographic algorithm and updating of the existing algorithms in the algorithm library both can be achieved through the opening interfaces provided by FTA. Switching the cryptographic algorithm to be used in the FTA framework can avoid the unnecessary consumption. Besides, using the subalgorithm interface and algorithm-control interface designed here, FTA provides several software-defined invocation modes (e.g., combination and switching according to the control instruction sent by the control program) to implement hybrid encryptions or change the cryptographic algorithms for communication. Finally, the feasibility and availability of the proposed FTA mechanism are evaluated by StrongSwan.

1. Introduction

With the maturity of technologies like software-defined networking, big data, and cloud computing, the Internet of Things (IoT) affects people's lives in many areas. Software-defined mobile network (SDMN) is presented as a promising solution for IoT and works on improving wireless networking, resource management, performance, and scalability [1, 2]. However, these technologies also raise the risk of privacy leakage when creating more convenient conditions [3], and the IoT security becomes more and more prominent and severe. The development of the IoT needs the support of IPv6 technology [4–6], which provides sufficient IP addresses for IoT devices and guarantees the security of communication links through Internet protocol security (IPsec). On the basis of an IoT security architecture, IPsec can provide data security and authentication during the communication process and enhance the security of IoT [7].

Following the evolution of IPv6 in IoT and its support for IPsec, the number of applications of IPsec is constantly increasing [8–10]. Based on the open framework provided by IPsec, users can choose appropriate cryptographic algorithms for communication security [11]. However, the various public cryptographic algorithms that IPsec supports by default are not applicable in certain specialized fields. Besides, due to the increasing awareness of network security [1, 12], applications are emerging that require the addition and timely switching of customized cryptographic algorithms in IPsec to ensure higher security and confidentiality for the IPv6 networks and especially for the IoT [12].

The optional and flexible use of a cryptographic algorithm can efficiently improve the performance of IPsec and reduce the consumption of the IoT employing IPsec when the key is long enough. In recent years, the flexibility and scalability of IPsec have become more critical than before, following the rise of the concept of software-defined everything [13–15]. Meanwhile, the method of changing the cryptographic algorithms applying in IPsec for different application scenarios is becoming inefficient and complicated. At present, relevant work is mostly focused on adding IPsec cryptographic algorithms,

establishing a security gateway for network communication, and the impacts of IPsec on network applications [16–18]. However, to the best of our knowledge, there is little research on the simplification and flexibility of algorithm invocation in IPsec.

To address this issue, in this paper, we propose an algorithm invocation mechanism applied to IPsec, entitled Free to Add (FTA), by introducing the idea of software-defined everything. The contributions of this paper are as follows:

(i) To employ two opening interfaces that are first designed in FTA, introducing the concept of software-defined everything: the control program can be seen as a part of the controller in the software-defined network (SDN), and the instructions are sent to the FTA module by employing the opening interfaces

(ii) To improve the implementation of adding and switching cryptographic algorithms avoiding the unnecessary consumption caused by the traditional IPsec processes

(iii) To provide a software-defined way of invoking multiple cryptographic algorithms by constructing a combined-policy and performing a hybrid encryption process based on the combined-policy: the policy is combined in a similar manner to an entry of flow table in the OpenFlow switch in SDN.

The remainder of this paper is organized as follows. Section 2 describes the issue addressed in this paper. Section 3 presents the details of the mechanism of FTA. Section 4 explains the implementation of the FTA module and compares the performance of FTA-based IPsec with traditional IPsec. Finally, this paper concludes with Section 5.

2. Description of Problem

IPsec is a compute-intensive work which consumes more resources and requires high-performance IoT devices. Nonetheless, if the security architecture of IoT is sufficiently improved, proper invocations of low-strength cryptographic algorithms can provide sufficient security with lower resource consumption. That is to say, it is crucial and efficient for the IoT security to add appropriate customized cryptographic algorithms in IPsec and reasonably invoke these algorithms.

IPsec encryption consists of two processes: Internet key exchange (IKE) and the subsequent encryption in session (ES) carried out in the kernel [18, 19]. As shown in Figure 1, the IKE process establishes an IKE security association (SA) and negotiates the key and algorithm required for the IPsec SAs of the ES process using the IKE SA, which is performed mostly in the user layer. Then, in the ES process, the kernel establishes IPsec SAs with the negotiated key and algorithm and achieves encrypted end-to-end communication. As the cryptographic algorithms used in the two processes are implemented in different locations and provide security services in different phases, the addition of new cryptographic algorithms to IKE SA and IPsec SAs is also considered in terms of two separate cases.

Because the Linux kernel supports IPsec, mainstream IPsec virtual private networks (VPNs), such as StrongSwan and OpenSwan mainly implement the IKE process, pass the key and algorithm to the kernel, and establish IPsec SAs in the kernel layer. Thus, the addition of a new algorithm for the IKE SA can be implemented efficiently simply by adding it to the IPsec VPN.

Unfortunately, when adding an algorithm to IPsec SA, the identifier of the algorithm is required in both the IPsec VPN and the kernel for negotiation and identification, and a module for performing the algorithm is also needed for the kernel or encrypted card, requiring recompilation of all related kernel modules. Moreover, the IPsec VPN typically adopts a configuration file to invoke cryptographic algorithms and uses them in an inflexible and nonuniversal way, making the addition of cryptographic algorithms more difficult (note that the analysis and design of our work are mainly based on StrongSwan [20] since it is a widely used and mature open-source IPsec VPN with proper maintenance of version updates).

To guarantee the stability of cryptographic communication, the IPsec VPN must add the cryptographic algorithms to be used in the configuration file in advance, and then it recognizes the selected algorithm by reading the file. Nevertheless, the use of algorithms in this way is inflexible; for instance, if attackers can identify the cryptographic algorithm, they can decrypt the communication data quickly and efficiently with the relevant methods, especially when the algorithm is public. That is to say, updating the algorithms more frequently can make attacks harder and more costly, thus increasing the strength of security. A mechanism that implements flexible and extensible addition and invocation of an algorithm is therefore crucial for IPsec.

Furthermore, because IPsec can be a part of the security architecture of IoT, it will help the security architecture of IoT to be in control of the overall system security and energy consumption if the cryptographic algorithms in IPsec can be invoked using a more flexible and low-cost mechanism. The communication efficiency will be improved well while the cryptographic algorithms can be adaptively switched and changed according to the complex environment. However, the asymmetric cryptographic algorithms with high strength are often employed to ensure the security of keys in the IKE process; it means that more resources will be required. Moreover, the frequent execution of IKE process also increases the resource consumption.

It is vital and crucial for wireless networks to provide secure communications with flexible and customized encryption schemes in a wide variety of situations, especially, the secure communication between base stations and the core network. Therefore, our work in this paper is to study and attain an invocation mechanism providing flexible and expandable addition and switching of IPsec cryptographic algorithms with low resource consumption.

3. Invocation Mechanism for Cryptographic Algorithms

At its core, encrypted communication relies on cryptographic keys and algorithms. To enable the addition and switching

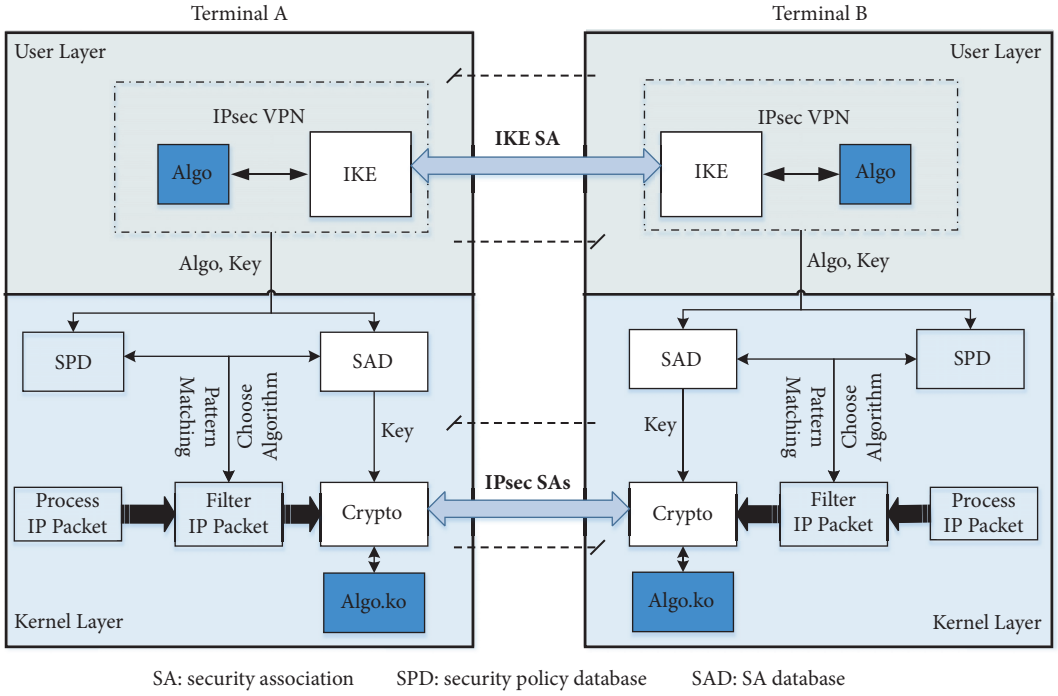


Figure 1: Communication encryption processes in IPsec.

of cryptographic algorithms on demand during an IPsec SA negotiation, an invocation mechanism of cryptographic algorithms called FTA is presented in this section. In FTA, the concepts of *opening interface* and *combined-policy* are introduced, in order to reduce the complexity of adding and switching cryptographic algorithms and the resource consumption on the basis of software-defined everything. The combined cryptographic algorithms are multigrained, and can be flexibly invoked to meet the demand for applications with a higher level of security.

3.1. Invocation Mechanism: FTA

3.1.1. Basic Introduction of the FTA Process. In the traditional IPsec, the process of algorithm identification, module addition, and recompilation of related modules is repeatedly carried out when adding a new algorithm. As shown in Figure 1, the encryption policy is fetched by an IPsec daemon (a program running as a background process) during the ES process from the security policy database (SPD) in the kernel. The IPsec daemon then invokes the algorithm module according to the corresponding algorithm identifier in the policy to perform encryption or decryption.

The process is the same as that of traditional IPsec before invoking the FTA module. The FTA mechanism makes some modifications on the basis of traditional invocation mechanism in IPsec, and the IPsec kernel directly invokes the FTA module rather than the implementing modules of algorithms. In FTA, the algorithms can be switched by the control program, with no need for reading the configuration file and negotiating again on the IPsec layer. Besides, IKE process regularly negotiates long-enough keys and no longer involves the algorithm renegotiation, which can eliminate the consumption of the duplication of IKE process caused by algorithm renegotiation.

Furthermore, the FTA mechanism simplifies the process of algorithm addition using the opening interfaces and combined-policies to enhance the flexibility of IPsec. Based on the inputting policy ID from the control program, FTA invokes a combined-policy which provides the specific encryption mode including the algorithm(s) and the location of encryption. All these are done in the kernel layer and more secure and time-effective than the process in IPsec that implements encryption by invoking Crypto API using af-alg in the user layer. As the encryption module in IPsec, af-alg is invoked in the user layer, but the encryption process of af-alg is executed in the kernel layer. In contrast, in FTA, all the operations are executed in the kernel layer, and the synchronizing signal is sent into the kernel by the control program using the algorithm-control interface without affecting the execution efficiency of the kernel.

Based on the existing IPsec workflow, the FTA mechanism just needs to add an algorithm-control interface and a subalgorithm interface to the last-invoked kernel module of a cryptographic algorithm; this is convenient and flexible for the addition and invocation of cryptographic algorithms.

3.1.2. Features of the FTA Mechanism. Compared with the method of adding algorithms in the convenient IPsec (Figure 2(a)), the FTA mechanism (Figure 2(b)) introduces certain changes, mainly in terms of the addition and invocation of cryptographic algorithms through opening interfaces.

(i) The FTA mechanism changes the invocation mode for the specific cryptographic algorithm; it does not

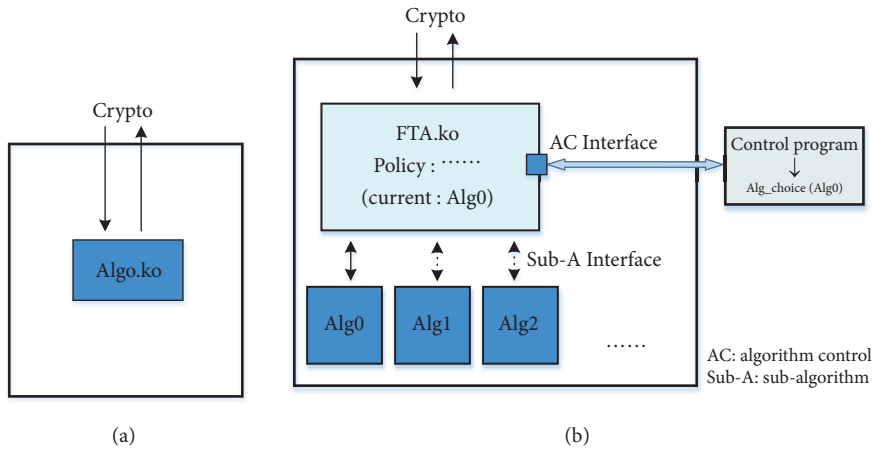


Figure 2: Algorithm addition in (a) traditional IPsec and (b) FTA-based IPsec with additive opening interfaces.

invoke the cryptographic module *Algo.ko* directly but invokes the FTA module *FTA.ko* including a cryptographic instruction and subalgorithm invocation in order to perform encryption. Then, the FTA module invokes the module of a specific cryptographic algorithm to perform encryption or decryption.

(ii) Alg_choice is a control message sent from the control program by employing opening interfaces. The control program can be seen as a part of the SDN controller.

(iii) A cryptographic instruction, given from the external control program through the algorithm-control interface, is either a single specific cryptographic algorithm or an ordered combination of multiple cryptographic algorithms, e.g., Alg1 and Alg2, through the subalgorithm interface of *FTA.ko*.

(iv) Based on the cryptographic instruction, the sender invokes the relevant cryptographic algorithm to encrypt the communication data in order, and the receiver implements the decryption in reverse. The implementation of these algorithms can be seen an encryption device controlled by the control program.

(v) The cryptographic algorithm library may be composed of multiple algorithm modules in the kernel or may be performed using a unified subalgorithm library.

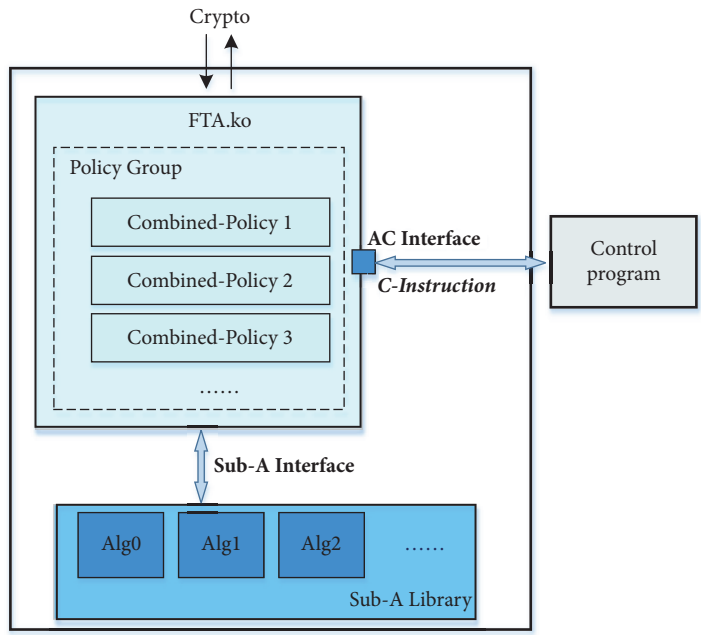
It is possible to substitute and synchronize the cryptographic algorithm through the algorithm-control interface. The combined cryptographic algorithm for an encryption/decryption operation can also be defined by adding a combined-policy of encryption algorithms or more flexible policy interfaces to the FTA module. This software-defined mechanism makes the invocation of cryptographic algorithms in IPsec more scalable and flexible.

3.2. Adding a Cryptographic Algorithm Based on FTA. In the FTA mechanism, after obtaining the encryption information from the SPD, a specific cryptographic algorithm from the algorithm library is not directly invoked by the kernel module but by the FTA module according to predefined encryption instructions. While there are more algorithms to be added to IPsec, only the implement modules of these algorithms need to be inserted into the FTA module and to be invoked through the algorithm-control interface (see Figure 3). In the same way as a plug-in device, a new cryptographic algorithm must conform to a unified interface standard, which is the only requirement for the cryptographic algorithm added or switched in the FTA mechanism. Thus, in subsequent processes, the new algorithm can be invoked through the external control program of FTA via the algorithm-control interface and policy definition. Synchronizing with the algorithm-control interface, FTA can also invoke other cryptographic algorithms without the IKE process.

Compared with the traditional method, the proposed FTA mechanism no longer has to repeatedly add the identifier of a new algorithm to the IPsec VPN, recompile *pfkey*, *xfrm*, or other modules, and modify the configuration file. The addition of the algorithm identifier and the invocation of the algorithm can be performed by using the software development method in the FTA module, thus simplifying the process of adding cryptographic algorithms without the IKE process. This approach also avoids some system-level errors caused by maloperation of the related kernel modules.

3.3. Software-Defined Invocation of Cryptographic Algorithms. The FTA mechanism invokes the combined-policy and the subalgorithms through the algorithm-control and subalgorithm interfaces, respectively; the cryptographic instructions for algorithm invocation can be software-defined using these interfaces.

3.3.1. Combining Cryptographic Algorithms. Since the flexible combination of algorithms (i.e., a combined-policy) and multiple encryptions supported by the subalgorithm and algorithm-control interfaces are possible in FTA, a subalgorithm invoking hybrid encryption can be implemented. First, two or more related algorithms are integrated into a combined-policy which is to be added to the FTA module.



AC: algorithm control, Sub-A: sub-algorithm, C-Instruction: cryptographic instruction

Figure 3: Structure of the scheme for combining and switching cryptographic algorithms.

Then, when the control program defines an alg_choice, one or more of these combined-policies is chosen through the algorithm-control interface, and data is encrypted or decrypted by invoking the corresponding algorithms through the subalgorithm interface. There are various methods to form and invoke a combined-policy. The policy can be predefined and stored in the FTA module and directly invoked based on its ID. It can also be defined using a specific format and sent to the FTA module by the control program. The following is an example of a combined-policy in JavaScript object notation (JSON), which is similar to an entry of the flow table in a OpenFlow switch in SDN:

```
{ “match”: {“src”:“IP”, “dst”:“IP”, “porto”:“http”},
  “actions”:
  [
    { “action”:“DES”,
      “params”:
          { “fragment”: {“start”:0,“end”:“63” }}
    },
    { “action”: “3DES”,
     “params”:
          { “fragment”: {“start”:64,“end”:“127” }}
    },
    { “action”:“AES128”
    “params”:
          { “fragment”: {“start”:0,“end”:“127” }}
    },
    { “action”:“out” }
  ]
}
```

Corresponding to Figure 3, the combined-policy defined above means a process of 128-bit data encryption in IPsec with following steps.

Step 1. Match the information of data (e.g., the IP addresses) to the corresponding field; if there is no match, go to Step 4.

Step 2. Encrypt the first and last 64 bits using DES and 3DES, respectively.

Step 3. Encrypt the 128-bit data again using the AES algorithm.

Step 4. Output the data and exit.

Step 5. Operate the data using the default encryption algorithm.

The process can be implemented in sequence or parallel. The decryption based on the policy is implemented in the reverse process. This method can refine the usage of cryptographic algorithms and create more flexible encryption schemes. Compared with the traditional approach to IPsec, the FTA mechanism can implement the customized invocation more easily without certain convenient customized processes such as rewriting the algorithm module and updating the configuration file.

Although the algorithm combination scheme creates extra resource overheads and decreases the efficiency of the

cryptographic processes, it can enhance the confidentiality and security of cryptographic algorithms, and the cracking and attacks using a single specific decryption algorithm are mitigated.

3.3.2. Switching Cryptographic Algorithms. FTA switches the algorithms to be used in the IPsec SA by resending the cryptographic instruction through the reserved algorithm-control interface. There is no need to design a new cryptographic algorithm or to implement the workflow of traditional IPsec, i.e., to update the configuration file of IPsec and then restart IPsec. Since the FTA module supports the policy group, algorithm switching can be achieved simply by switching the corresponding combined-policies instead of the algorithms themselves, through the algorithm-control interface; that is to say, a combined-policy can be regarded as a specific cryptographic algorithm. For instance, in Figure 3, Combined-Policy 0 can be defined as an encryption method of AES128 in the following pattern, and it will be invoked through the algorithm-control interface:

```
{
  “match”: {“src”:“IP”,“dst”:“IP”},
  “actions”:
    [
     {“action”:“AES128”
       “params”:
            { “fragment”: {“start”:0, “end”:“127” }}
     },
     { “action”:“out” }
    ]
}
```

Algorithm switching is more flexible in FTA-based IPsec than in traditional IPsec and does not require interrupting IPsec session and updating IPsec SAs. If the system should switch the cryptographic algorithm being used for data encryption to be another algorithm according to the encryption demand, the only thing the control program needs to do is update the algorithm name and the corresponding parameters in the combined-policy. Algorithms are reencapsulated in the combined-policy and synchronized as the FTA module synchronizes the policy. The attacker cannot decrypt the cryptographic algorithm to be replaced in the FTA, even if its identifier can be obtained, and the FTA mechanism therefore makes attacks costlier and more difficult.

3.4. Discussion on the Complexity of FTA. The complexity of the FTA mechanism mainly includes the space and time complexity. The space complexity primarily depends on the space requirements of combined-policies and subalgorithm library. Because the execution of the cryptographic algorithm is not implemented in the FTA module, the time complexity associated with FTA is affected by the scheme of policy query and algorithm invocation. In FTA, the invocation process is finished by only three steps and the time complexity of each step is O(1), which means the time complexity of the algorithm invocation can be negligible. Therefore, the policy query is becoming the dominant factor.

Because the data being processed by IPsec is not fine-grained, the FTA mechanism does not take up much storage space for policies and subalgorithm library and the time for searching a policy. Here, the time of policy query is decided by the volume of the policies stored in the FTA module. In the work of this paper, the policies are stored in a simple linear list, and the time complexity is mainly related to the number of policies n. The maximum value is O (n). The query method also affects the time of policy query. Several techniques, such as tree matching and parallel processing, can be used to improve the query efficiency, but we have not considered the issue yet.

As a note, in our work, we assume that the security of the network devices is ensured. In the circumstance, the customization of cryptographic algorithms is implemented by the network administrator in a software-defined manner. That is, the network operating environment applying the FTA mechanism would not be worse than that of traditional IPsec.

4. Experiment and Evaluation

4.1. Experimental Environment. In this work, the experimental environment is built on a virtual machine with an Ubuntu installation, to evaluate the performance of the FTA mechanism. The network topology and corresponding simulation environment are shown in Figure 4 and Table 1, respectively. New cryptographic algorithms and the control module developed here were installed in advance on terminals A and B.

4.2. Adding FTA Module. As mentioned in Section 2, the FTA module is added to IPsec as a new algorithm, using the traditional method in IPsec. The open architectures of StrongSwan and Linux make it straightforward to add new IPsec algorithms. Each functionality is inserted into StrongSwan as a plug-in, and the Linux kernel also provides some operations for new modules, e.g., registration, insertion, and invocation.

Furthermore, the IPsec VPN and the kernel manage to add the identifier of the FTA module. The corresponding modules need to be inserted into the kernel or encrypted card, so that the IPsec SA can negotiate the key and algorithm with the IPsec VPN and implement encryption and decryption in the kernel. Here, we give an example to illustrate this process. A modification was made to the configuration file *ipsec.conf* (as shown in Figure 5(a)) after the new algorithm *fta* (i.e., the FTA module) was added to IPsec. Its corresponding kernel module *FTA.ko* was also inserted and connected to IPsec. The results, as displayed in Figure 5(b), show that the IPsec connection was successfully established and that the FTA module was added to IPsec as a new algorithm.

Since StrongSwan supports the complete implementation of the IKE process without involving the kernel of the operating system, the addition of new algorithms into IKE is easy and convenient. Furthermore, IKE is seldom employed, and algorithm switching is seldom required in IKE. In this

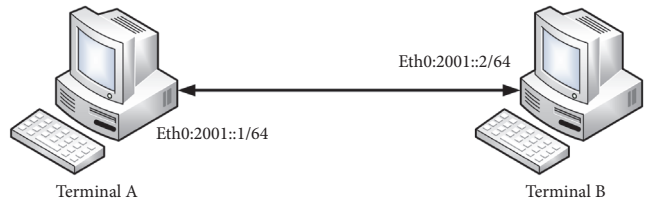


Figure 4: Topology of the testing network.

Table 1: Simulation software and hardware.

Device	Configuration
PC	CPU: Intel(R) Core(TM) i5-4200H @ 2.80 GHz memory: 16 GB, hard disk: SSD 250 GB, OS: Win10 64 bits
Virtual software	VMware Workstation 12.1.0
Virtual machine	OS: Ubuntu 14.04.3, CPU: 1∗2, memory: 2 GB, hard disk: SSD 30 GB
IPsec VPN	StrongSwan 5.4.0

paper, we therefore do not consider the ways of switching the algorithm in IKE.

4.3. Feasibility of the FTA Mechanism. In the FTA mechanism, there are two methods for adding a new cryptographic subalgorithm: one is to add this directly into the subcryptographic library, and the other is to insert the relevant implementation module of the algorithm into the FTA module. For example, algorithms AES128, DES, and 3DES are inserted into the FTA module *FTA.ko* using the second method, and Table 2 lists the combined-policies based on these three algorithms.

Figure 6 shows the two communication terminals (the Receiver and Controller) establishing an IPsec encrypted tunnel based on StrongSwan 5.4.0, in which new algorithms have been successfully added. The Server and Client of the control program communicate based on TCP, and the security of the sessions between them is also ensured, due to the existing encrypted channel. To control the algorithms synchronously, the Server and Client communicate with the FTA module through *netlink*, a mechanism that implements a certain type of datagram socket for communication between the kernel and the user space.

After establishing an IPsec SA using the FTA mechanism, cryptographic algorithm switching can be performed by the control program. This uses 0, 1, and 2 as the policy group IDs for switching the FTA encryption policies, where each number corresponds to a combined-policy group. As shown in Figure 7, these combined-policies perform well, and combinations can easily be switched. The results indicate that (1) it is feasible to add a new algorithm for IPsec via the FTA subalgorithm interface; (2) the encrypted policies can be switched flexibly via the algorithm-control interface; and (3) a hybrid encryption can be implemented when invoking a policy group consisting of multiple cryptographic algorithms in FTA.

4.4. Availability of the FTA Mechanism. Compared with the conventional method, the invocation of the cryptographic algorithm in the FTA mechanism is somewhat complicated and requires greater consumption of resources. The performance of both FTA and the traditional IPsec invocation for cryptographic algorithms AES128, DES, and 3DES is tested on the simple network given in Figure 4. This experiment evaluates the performance in terms of Ping response time and CPU occupancy rate via tools *ping*, *iperf3*, and *top*, and the results are shown in Figures 8 and 9 and Table 3, respectively.

Figure 8 shows the average Ping response time of 20 crypto-operations. From the results, it is evident that the Ping response time of the FTA mechanism is slightly longer than that of the traditional IPsec in the three cases due to the additional operations brought by FTA (e.g., the selection and switching of algorithms), but the fluctuations are all within a reasonable range. For the AES128 case, the difference between the Ping response time of the FTA mechanism and that of the traditional approach is only 0.0072 ms, which is the largest one of the three cases.

Based on the testing network given in Figure 4, we test the impact on the CPU occupancy of communication terminals when translating TCP traffic at a constant rate. Only the CPU occupancy of the sending end A is collected, since the sending end A has to consume more resources for not only generating but also sending data.

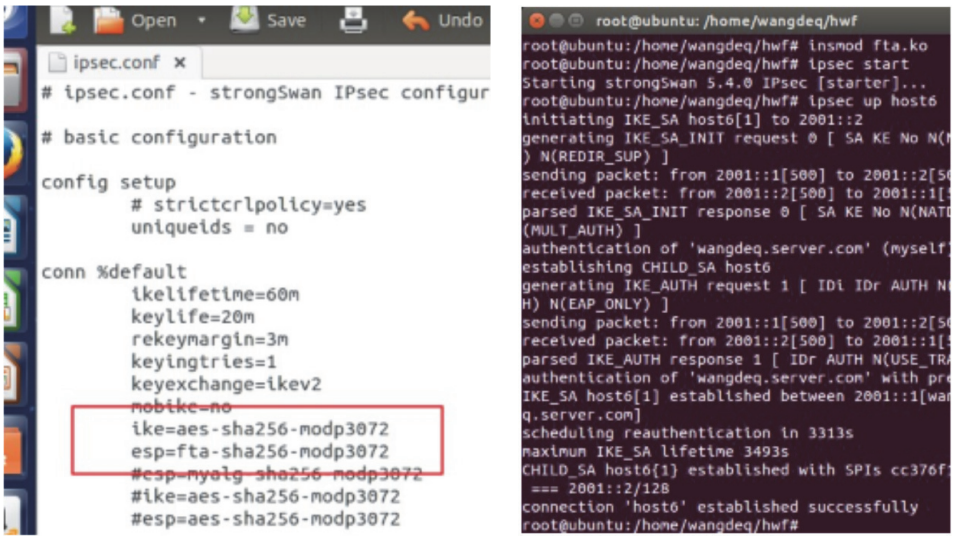
The results depicted in Figure 9 indicate that each mechanism causes the CPU occupancy rate to be increased with increasing data volume, and the trend of change is almost the same in the six cases. Even though different cryptographic algorithms, e.g., AES128, DES, and 3DES, are invoked for encryption, the CPU occupancy rates of the traditional and FTA-based IPsec scenarios are approximated. Integrating the results depicted in the three subfigures of Figure 9, the type of cryptographic algorithm has a primary influence on the CPU occupancy, while the FTA mechanism which modifies and

Table 2: Examples of combined-policies.

Policy ID	Cryptographic algorithm	Combined-policy description
0	AES128	Encrypt 128 bits of data using AES128.
1	DES, 3DES	Encrypt the first 64 bits and the last 64 bits of data using DES and 3DES, respectively.
2	AES128, DES, 3DES	Encrypt the first 64 bits and the last 64 bits of data using DES and 3DES, respectively, and then encrypt the 128 bits of data again using AES128.

Table 3: Average processing rate under full-load CPU (Mbps).

Method	Cryptographic algorithm		
	AES128	DES	3DES
Traditional IPsec	270	182	123
FTA-based IPsec	263	180	120



(a) (b)

Figure 5: Modification to (a) the configuration file for adding a new algorithm and (b) the established IPsec connection.

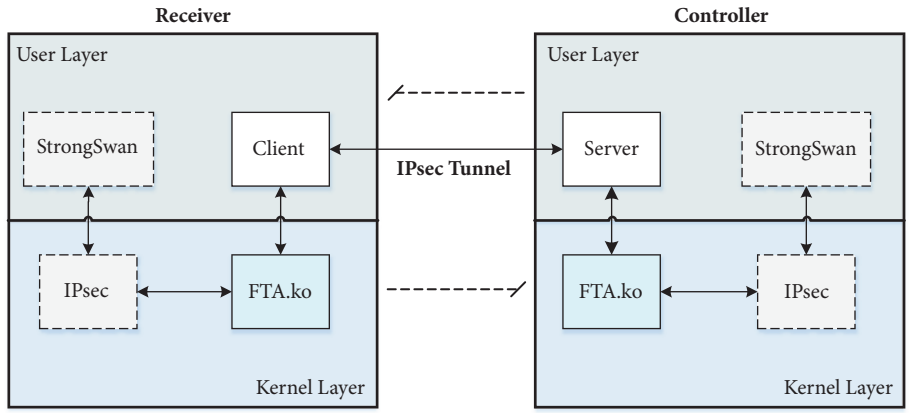
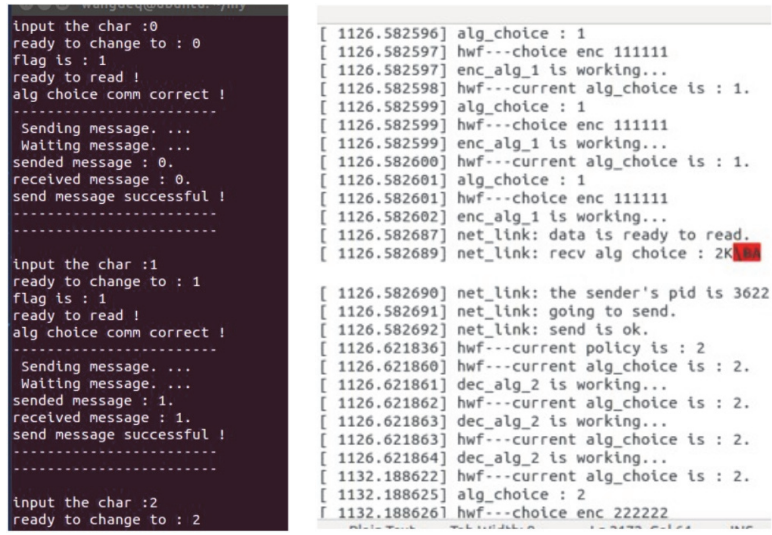


Figure 6: Frame of the designed control program for switching the combined-policies.



(a) (b)

Figure 7: Results of switching the policies of combined algorithms: (a) controlling program for switching; (b) policy switching records in the log file.

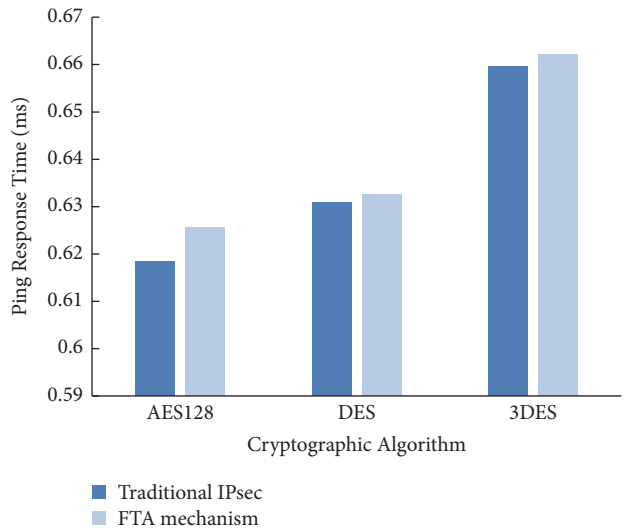


Figure 8: Average Ping response time during 20 seconds.

improves the IPsec algorithm invocation had no noticeable impact on the CPU occupancy.

Moreover, the results listed in Table 3 indicate that the average processing rate when applying the FTA-based IPsec is 97.4% of that in traditional IPsec when the CPU is at full load. Here, the data processing consists of packet generation via *iperf3*, encryption using IPsec, and forwarding to the link, and the average processing rate stands for the amount of data processed per second.

5. Conclusions

To ensure high security and confidentiality for IPv6 networks and especially for the IoT under diverse application environments, in this paper, we proposed an algorithm invocation mechanism FTA with simplified processes of the invocation of customized cryptographic algorithms in IPsec, avoiding the unnecessary consumption caused by traditional IPsec processes. In the verification experiment, FTA made the addition and switching of cryptographic algorithms and hybrid encryption in IPsec more convenient, and the algorithm invocation is more flexible. The results indicated that the definition and invocation of policy were software-defined and configurable. Furthermore, the availability of the FTA mechanism was also proven. The use of the FTA mechanism had no noticeable impact on the system performance regarding Ping response time and CPU occupancy rate.

Based on a quantitative analysis of the candidate cryptographic algorithms and the construction of a parameterized module, further work will examine the methods of

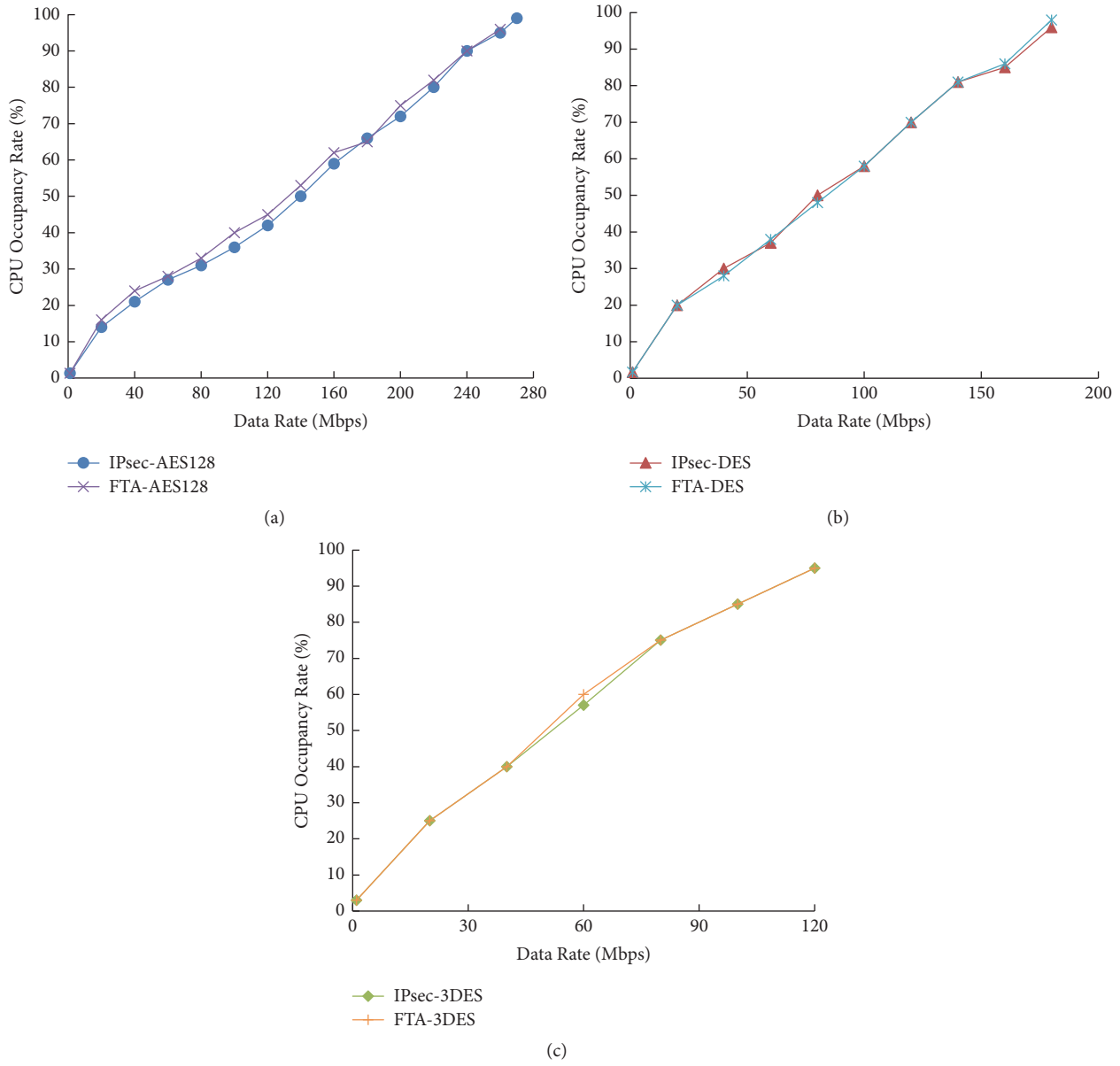


Figure 9: Trend of CPU occupancy rate influenced by data volume of traditional IPsec and FTA-based IPsec using (a) AES128, (b) DES, and (c) 3DES.

automatically generating the policy group after the standard of encryption policy is imported via the algorithm-control interface. We will also study the optimized scheme of policy query and storage in the future.

Data Availability

The data (i.e., simulation results, .xls, and resource code files, .c, .conf, and .sh) used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

The work described in this paper was carried out with the support of the National Natural Science Foundation of China (61772562), China Education and Research Network (CERNT) Innovation Project (NGII20150106), and the Fundamental Research Funds for the Central Universities, South-Central University for Nationalities (CZY18014).

References

[1] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, 2016.

[2] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[3] M. R. Bashir and A. Q. Gill, "IoT enabled smart buildings: A systematic review," in *Proceedings of the 2017 Intelligent Systems Conference (IntelliSys)*, pp. 151–159, London, UK, September 2017.

[4] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in *Proceedings of the 6th International Conference on Internet Technologies and Applications, ITA 2015*, pp. 219–224, Glyndŵr University, Wrexham, North Wales, UK, September 2015.

[5] X. w. Wu, E. H. Yang, and J. Wang, "Lightweight security protocols for the Internet of Things," in *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–7, Montreal, Canada, October 2017.

[6] A. J. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[7] M. Irshad, "A Systematic Review of Information Security Frameworks in the Internet of Things (IoT)," in *Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 1270–1275, Sydney, Australia, December 2016.

[8] M. Rao, J. Coleman, and T. Newe, "An FPGA based reconfigurable IPSec ESP core suitable for IoT applications," in *Proceedings of the 2016 10th International Conference on Sensing Technology (ICST)*, pp. 1–5, Nanjing, China, November 2016.

[9] S. K. Majhi and S. K. Dhal, "Placement of security devices in cloud data centre network: analysis and implementation," *Procedia Computer Science*, vol. 78, pp. 33–39, 2016.

[10] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling secure mobility with OpenFlow," in *Proceedings of the 2013 Workshop on Software Defined Networks for Future Networks and Services, SDN4FNS 2013*, pp. 1–5, Trento, Italy, November 2013.

[11] B. C. V. Camilo, R. S. Couto, and L. H. M. K. Costa, "Assessing the impacts of IPsec cryptographic algorithms on a virtual network embedding problem," *Computers & Electrical Engineering*, July 2017.

[12] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, 2011.

[13] A. Gupta, E. Katz-Bassett, L. Vanbever et al., "SDX: a software defined internet exchange," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 579-580, 2014.

[14] J. Esch, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 10–13, 2015.

[15] IEEE 5G, "IEEE 5G and beyond technology roadmap white paper," *IEEE*, https://5g.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf.

[16] V. H. F. Tafreshi, E. Ghazisaeedi, H. Cruickshank, and Z. Sun, "Integrating IPsec within OpenFlow architecture for secure group communication," *ZTE Communications*, vol. 12, no. 2, pp. 41–49, 2014.

[17] S. Samoui, I. El Bouabidi, M. S. Obaidat, F. Zarai, K. F. Hsiao, and L. Kamoun, "Improved IPSec tunnel establishment for 3GPP-WLAN interworking," *International Journal of Communication Systems*, vol. 28, no. 6, pp. 1180–1199, 2015.

[18] A. A. Al-Khatib and R. Hassan, "Impact of IPSec protocol on the performance of network real-time applications: a review," *International Journal of Network Security*, vol. 19, pp. 800–808, 2017.

[19] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet key exchange protocol Version 2 (IKEv2) RFC 7296," 2014, https://tools.ietf.org/html/rfc7296.

[20] StrongSwan, https://www.strongswan.org/.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5379326, 11 pages
https://doi.org/10.1155/2018/5379326

Research Article

Energy-Aware Smart Connectivity for IoT Networks: Enabling Smart Ports

Metin Ozturk,[1] **Mona Jaber**,[2] **and Muhammad A. Imran**[1]

[1]*School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK*
[2]*Fujitsu Laboratories of Europe, Hayes UB4 8FE, UK*

Correspondence should be addressed to Muhammad A. Imran; muhammad.imran@glasgow.ac.uk

Received 7 March 2018; Revised 5 June 2018; Accepted 10 June 2018; Published 28 June 2018

Academic Editor: Manuel Fernandez-Veiga

The Internet of Things (IoT) is spreading much faster than the speed at which the supporting technology is maturing. Today, there are tens of wireless technologies competing for IoT and a myriad of IoT devices with disparate capabilities and constraints. Moreover, each of many verticals employing IoT networks dictates distinctive and differential network qualities. In this work, we present a context-aware framework that jointly optimises the connectivity and computational speed of the IoT network to deliver the qualities required by each vertical. Based on a smart port application, we identify energy efficiency, security, and response time as essential quality features and consider a wireless realisation of IoT connectivity using short range and long-range technologies. We propose a reinforcement learning technique and demonstrate significant reduction in energy consumption while meeting the quality requirements of all related applications.

1. Introduction

The Internet of Things (IoT) is today's buzzword, often coupled with *Big Data* and *Artificial Intelligence* (AI). However, there is a lot of ambiguity of what is meant by that and scepticism about the actual value generated by the IoT. IoT devices have become pervasive but cover a broad range of technologies and standards. Wireless technology is key to connect these devices through gateways or aggregation points; but, similarly, a wide range of wireless protocols and standards are available and competing [1]. Once these devices are connected, they start reporting the sensed or measured data to the platform. Again, multiple choices are possible in this aspect with different strengths and weaknesses. Reporting raw data to the cloud is very costly as every bit gets charged and may also exhaust the battery of the device; this results in *massive* data. On the other hand, running scripts locally in the device and reporting the resulting events to the cloud reduce the cloud service cost but limits the visibility to the actual data; this still results in *big* data. Moreover, local scripts result is real-time actions and do not expose the privacy of the data, whereas cloud computing incurs latency due to the transmission network and requires stringent security measures to protect the data.

An environment, which is rich in IoT devices that are connected to a platform, qualifies as *digitised*, and often as *intelligent*. Analytics, which uses AI, is the added layer that transforms such an environment into a *smart* one. The default application of AI is to draw actionable insights from the data in order to generate value to the given vertical. In this work, we argue that IoT solutions should not be addressed through a layered perspective but, instead, a holistic optimisation approach is needed to generate the desired added value efficiently. In such a holistic approach, AI, among other machine learning tools, is employed in every stage of the solution including connectivity, storage, computing, and analytics.

Since there are many use-cases of the IoT paradigm [2], it should be approached from a given vertical perspective, e.g., smart health, smart cities, smart manufacturing (Industry 4.0), smart transport, etc. Each of these verticals comprises multiple IoT-based applications with various requirements. In [3], for example, signalling measurements and modelling are performed for both static and vehicular machine-to-machine (M2M) applications, as

both have different signalling overhead characteristics. As another example, remote monitoring in smart cities requires full compliance with privacy regulations, whereas security-related applications rank response time highest among all key performance indicators (KPI).

In this article, we adopt the smart port use-case to demonstrate the context-aware smart connectivity, since it includes various types of applications and has a determined need for monetisation (as opposed to smart cities that are primary developed for the well-being and productivity of the society). According to figures from the World Trade Organization, 80% of worldwide freight is transported through ports (https://www.wto.org/). The smart port concept entails the use of technologies to transform the different public services at ports into interactive systems with the purpose of meeting the needs of port users with a greater level of efficiency, transparency, and value. European smart port initiatives include the following among many others:

(i) *The port of Rotterdam* where IoT-sensors are used to generate a digital twin and enable augmented intelligence.

(ii) *The port of Hamburg* which exploits 5G networks to enable virtual reality for vital infrastructure monitoring.

(iii) *The port of Antwerp* employs blockchain technology to enable a secure transfer of rights to be exchanged between often competing parties.

(iv) *The port of Seville* through the Tecnoport 2025 project uses mobile network technology for traffic and goods tracking on port and their logistical transfer on land.

Smart ports present a particular challenge due to the necessity of information exchange among competing stakeholders including port authorities, port operators, terminal operators, logistics companies, shipping companies, etc. It is then likely that multiple IoT networks would coexist and would consist of partly private and partly public or shared infrastructure. As described in [4], there are various communication standards, with different strengths and weaknesses, which may be used for connecting IoT networks in the context of smart ports. Mobile IoT, i.e., connectivity over licensed mobile wireless networks, is often the preferred solution for handling private data, since it is reliable, end-to-end secure (owing to the eSIM card), scalable, ubiquitous, and mature. Two main technologies have been introduced by mobile networks to connect IoT devices: eMTC and NB-IoT [5]. Both of these technologies are compatible with LTE (state-of-the-art commercial mobile network technology) which means that a software update suffices to deploy the IoT options. The former is geared towards higher rates (> 1 Mbps) and supports VoIP (Voice over IP based on ITU H.323 protocol (https://www.itu.int/rec/T-REC-H.323/e)) and flexile mobility. The latter is designed for low data rates (20 kbps) and long range (100 km) but with limited mobility. The NB-IoT technology consists of restricting the energy of an LTE normal carrier in a narrow band, hence allowing a maximum coupling loss that is 20 dB higher (164 dB) than LTE [6]. Mobile IoT is a public service enabled by telecom carriers and may be used by any party who subscribes to it. Other long-range and low-power solutions, such as LoRa(https://www.lora-alliance.org/) and Sigfox(https://www.sigfox.com/en), are unlicensed and can reach similar coverage and data rates as NB-IoT and eMTC. These may be privately owned but require the usage of a gateway to connect to the Internet and are often considered less secure. Many short range unlicensed wireless connectivity solutions are available, such as WiFi (IEEE 802.11g), Bluetooth, ZigBee, etc., as described in [7], and may be shared, public, or private.

In the presence of multiple wireless technologies, disparate IoT applications, competing parties, and a broad range of static and moving IoT devices with multiple connectivity options, it is of key importance to identify the best way to collect, store, cache, and process the IoT data. What qualifies as *the best way* depends on the device capabilities (e.g., connectivity options, available battery); the wireless conditions; the security requirements; the processing complexity and availability; the cost of storage/caching/uploading, etc.

2. Related Work

As the energy consumption is one of the challenges for IoT networks [8], recent works, such as [9, 10], study the trade-off between local and cloud computing in terms of device energy consumption. The former proposes an analytical framework that minimises the energy consumption by optimising the offloading decision of multiple user devices. The latter elaborates a theoretical framework for establishing trade-offs in the energy consumption and IoT infrastructure billing comprising cloud computing. Mobile wireless networks are a prime contender in the race to connect IoT networks owing to their well-established and ubiquitous coverage and secure communication based on the subscriber identity module (eSIM card). In [11], authors investigate the connectivity of NB-IoT and LoRa in terms of both area and population coverage in order to highlight the importance of the network deployments. In [12], big data analytics based user-centric smart connectivity is argued by providing corresponding research challenges.

Although data aggregation seems a promising solution to ease the signalling overhead, it is one of the causes of the transmission delay. In [13], authors discuss the trade-off between delay and signalling overhead in order to demonstrate the impacts of data aggregation. Authors in [14] analyse the joint optimisation of caching and task offloading in such networks with mobile edge computing. They present an efficient online algorithm based on Lyapunov optimisation and Gibbs sampling that succeeds in reducing computation latency while keeping the energy consumption low. In [15], a recommendation system is proposed to address the challenge of link selection in a cloud radio access network. A data-driven scheme is introduced that results in optimised classification of link strengths between remote radio heads and IoT devices.

A deep learning algorithm for edge computing is introduced in [16] to boost the learning performance in IoT

networks. They also attempt to increase the amount of edge tasks by considering the edge capacity constraints. An open-source database is designed in [17] for the edge computation of Industrial IoT (IIoT) networks. The authors use a time-series analysis for predicting conditions of IIoT machines in order to decrease the amount of condition reports to be sent to the cloud. A holistic view of communication, computation, and caching is presented in [18] using graph-based representations as learning methods for innovative resource allocation techniques. The performance of the edge-caching as well as the energy efficiency and delivery time is investigated in [19] with quality of service (QoS) constraints.

In this work, we employ machine learning techniques, based on reinforcement learning, in order to manage multiple optimisation objectives jointly and to dynamically identify *the best connection* and route for each device. We identify four key quality features that dominate IoT applications in general and smart ports in particular: *security, energy, latency*, and *cost*. This work is the first to address these multiple IoT optimisation objectives jointly using reinforcement learning. We compare our novel approach to the state-of-the-art connectivity solutions and demonstrate significant gains in all aspects (ranging from 95.9% to 283.54%). Moreover, our approach is the only one that is able to meet the context-aware requirements fully, while minimising the cost and the energy consumption. The advantage of the machine learning scheme adopted is primarily its low complexity and its ability to optimise in a dynamic environment such as a smart port.

The rest of the paper is organised as follows. In Section 3 we define the system model of our research. In Section 4, we present our novel machine-learning-based solution for solving the multiobjective problem. Section 5 elaborates the results and analysis, and in Section 6 we conclude the article.

3. System Model

The energy-aware smart connectivity novel approach proposed in this work applies to any IoT network with diverse options of connectivity and processing. For the sake of clarity in the presentation, we build the system model around a smart port scenario such as the one shown in Figure 1. All IoT devices are battery operated and have different battery lives. They all have some processing power to perform basic tasks and can either offload the task to the gateway (or fog), i.e., the WiFi access point or to the evolved node B (eNB or cloud).

Differently from the state-of-the-art research, we propose to decide simultaneously on the best connectivity and the best location for processing the tasks by jointly optimising energy, response time, security, and cost. A two-stage approach, which describes the decision and optimisation processes, is presented in Figure 2. It is assumed that every IoT device is controlled by a given application and they jointly determine the context-aware constraints. Each combination of connectivity option and processing location offers specific characteristics and limitations. Stage 1 consists of optimising these decisions based on the context-aware constraints, while Stage 2 refines the trade-off between energy consumption and cost. In the following paragraphs, we describe the models adopted

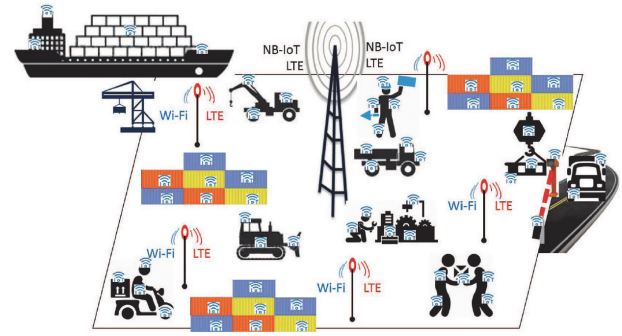


Figure 1: Smart port diagram with two overlapping networks: NB-IoT and WiFi. WiFi access points use LTE for backhauling. All IoT devices are capable of both wireless technologies.

to capture the propagation loss, energy consumption, and response time for the proposed system. Table 1 lists all the parameters that are pertinent to our simulations.

3.1. Propagation Model. There are three wireless connections that require modelling: (a) Device-to-Gateway (WiFi), (b) Device-to-eNB (NB-IoT), and (c) Gateway-to-eNB (LTE). Connections (a) and (c) are often interference limited, as the employed spectrum is likely to be shared by other neighbouring connections. Connections of type (b) are, however, considered to be noise limited, as we assume that there are no other eNB in the surrounding employing NB-IoT technology. The objective of the propagation modelling is to determine the transmission power required to cater for each of the wireless connection types. Accordingly, the energy consumption will be calculated. We start with the propagation loss L which is modelled as a function of two technology-specific parameters, the propagation constant K and the propagation exponent α, and the distance of the wireless hop δ measured in *km*, as shown below:

$$L = K \cdot \delta^{\alpha}. \tag{1}$$

Moreover, the probability of having line of sight between the device and the gateway is much higher than in the case of the other types of wireless connections; hence the propagation loss per decade is less [20]. On the other hand, NB-IoT connections suffer the same propagation loss per decade as LTE links, however, are successfully received with 20 dB less power (threshold receiver sensitivity is −141 dBm). For all types of links, the received power at a distance d_x from the transmitting device can be expressed as $P_r = P_t/L$ in mWatt. Next, we calculate the required received power P_r (in mWatt) in order to achieve the target data transmission D in bits:

$$D = T \cdot B \cdot \log_2\left(1 + \frac{P_r}{P_I + N_0 \cdot B}\right), \tag{2}$$

where T is the time period, B is the channel bandwidth, and P_I is the cumulative interference power on the given channel during time period T. Please note that P_I is null for wireless connections of type (b). Using (2) and solving for P_r, we get

$$P_r = \left(2^{D/(T \cdot B)} - 1\right) \times \left(P_I + N_0 \cdot B\right). \tag{3}$$

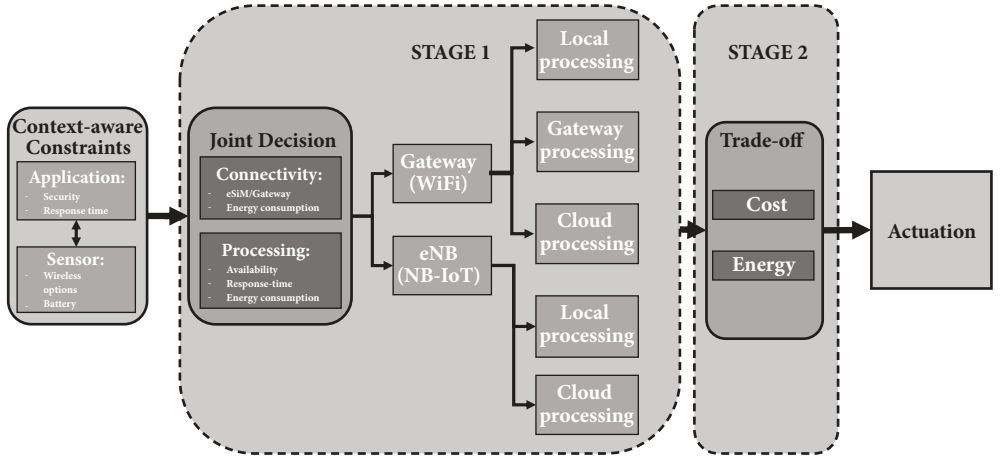


Figure 2: Decision and optimisation processes in a two-stage approach to optimise four performance criteria: energy, response time, security, and cost.

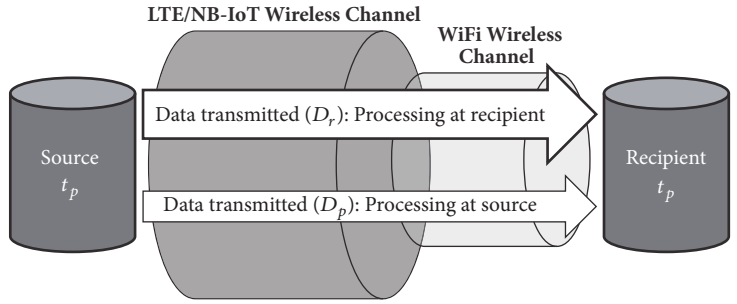


Figure 3: Uplink delay model capturing the factors affecting both processing and transmission delays over any hop in our system.

3.2. Energy Consumption Model. There are two major processes that consume energy in an IoT network: wireless transmission and task computation. The energy consumption of the former is E_t and the latter is E_p; thus the total energy consumption is the sum of both. Depending on the route of communication taken by the device, the energy consumed due to transmission power can be a result of either one hop using NB-IoT (E_{t_b}) or two hops using WiFi for the first link and LTE for the second ($E_{t_a} + E_{t_c}$). The energy consumed for processing the task is a function of the data rate requirement of device d, θ_d, and the computational power of the processor, E_{p_i} $\forall i = \{d, f, c\}$ (see Table 1), and is expressed as $E_p = \theta \cdot E_{p_i}$.

3.3. Response Time Model. The response time perceived by the IoT device is the combination of the uplink and downlink delays between the IoT device and the server. In this work, the uplink delay is modelled, while the downlink delay is assumed the same for all devices.

The uplink delay is caused by two phenomena: task processing (processing delay, t_p) and data transmission (transmission delay, t_t). The processing delay depends on the processor's computational power, which is measured in the number of computational cycle per data element (η); i.e., the higher η, the less computational power. Naturally, a server has higher computational power than a small gateway and much higher than a simple IoT device ($\eta_c < \eta_f < \eta_d$). Thus, in this work, t_p is modelled based on the computational powers of the processing locations: $t_{p_d} = 10 \times t_{p_f} = 100 \times t_{p_c}$. In addition, while the input to the task processing stage is large raw data, the output is compressed data with comparably less volume. To that end, the compression rate between the input and output data volumes is given as C; $D_r = C \cdot D_p$, where D_r and D_p are the volumes of raw and processed (compressed) data, respectively.

The transmission delay is affected by the type of radio access technology and the volume of data to be transmitted. Since WiFi access employs the unlicensed frequency bands, it often suffers from higher retransmission rates, which results in increased transmission delays, due to frequent collisions. Therefore, in this work, this effect is captured by the factor $F > 1$ whereby the delay incurred for transmitting the same volume of data over WiFi is F times higher than that over LTE or NB-IoT; $t_{t,a} = F \cdot t_{t,b} = F \cdot t_{t,c}$. This model is represented in Figure 3, in which the source could be either the IoT device or the gateway, and the recipient could be either the gateway or the cloud.

Consequently, the overall response time for each action is calculated for $C = 200$ and $F = 2$ as follows:

$$R = t_p + \sum_{i=1}^{N_h} t_{t_i} \cdot D_i, \tag{4}$$

Table 1: System model parameters and simulation values.

Parameter	Value	Description
r_n	200 m	eNB cell radius
r_w	30 m	WiFi cell radius
N_G	10	Number of IoT devices per gateway
χ_d	30 Kbps	Computational capacity (device)
χ_f	10^2 Kbps	Computational capacity (fog)
χ_c	10^3 Kbps	Computational capacity (cloud)
ϵ	5×10^{-9} Joule	Energy consumption per computational cycle
η_d	10^2	Required amount of computational cycle per data element (device)
η_f	10	Required amount of computational cycle per data element (fog)
η_c	1	Required amount of computational cycle per data element (cloud)
N_0	-204 dBW/Hz	Noise density
B	180 kHz	Bandwidth
$\overline{P_{t,d}}$	10^{-8} W	Average transmit power of the IoT devices in the gateways #2, #3, #4, and #5
T	1 s	Time period
λ	0.5	Q-table update parameter
ϕ	0.9	Q-table update parameter
ε_1	0.8	Action selection parameter for Stage 1
ε_2	10^4	Action selection parameter for Stage 2
ρ	0.8	Decaying rate for ε_1 and ε_2
S	8	Number of bits in each data element
ϑ	$10^3/S$	Conversion of kbps data rates to number of data elements
E_{p_d}	$\epsilon \cdot \eta_d \cdot \lambda$	Data processing energy consumption per data rate in kbps (device)
E_{p_f}	$\epsilon \cdot \eta_f \cdot \lambda$	Data processing energy consumption per data rate in kbps (fog)
E_{p_c}	$\epsilon \cdot \eta_c \cdot \lambda$	Data processing energy consumption per data rate in kbps (cloud)
Γ_d	10^{-4}	Cost of processing per kbps (device)
Γ_f	10^{-1}	Cost of processing per kbps (fog)
Γ_c	1	Cost of processing per kbps (cloud)
b	20	Budget
β_1	10^2	Constant coefficient for penalty comparison.
β_2	10^{12}	Constant coefficient for penalty comparison.
$K_w = K_l = K_n$	128.1 dB	Propagation loss constant for all wireless connection types (a, b, and c).
$\alpha_l = \alpha_n$	3.76	Propagation loss exponent for NB-IoT and LTE wireless connection types (b and c).
α_w	3	Propagation loss exponent for Wi-Fi (802.11g) wireless connection type (a).

where $N_h = \{1, 2\}$ is the number of hops and $D = \{D_r, D_p\}$. Besides, t_{t_i} and D_i represent the values of t_t and D for the i^{th} hop, respectively. Then, the calculated values populate Table 2 after the application of feature scaling into the range of [0, 1] using the function given as

$$f(x) = \frac{x - \min(X)}{\max(X) - \min(X)}, \tag{5}$$

where X is the set of x. Note that both (a) and (b) type connections constitute the first hop, while the connection type (c) is the second hop.

4. Machine Learning-Based Solution

In this work, we propose to employ reinforcement learning (RL), a machine learning technique based on a goal-seeking approach. It is a trial and error approach in which the agent (or learning device) learns to take the correct action by interacting with its surroundings and being rewarded or penalised in each iteration. RL is selected in this work due to its great applicability to the presented problem. For example, IoT devices need to interact with its environment in order to assess the circumstances and to take subsequent actions, which is determination of the connection type and the data processing location. Therefore, RL maps to this requirement very well, since it allows optimisation with environmental interactions.

Being one of the most prominent reinforcement learning techniques, Q-learning aims to find the optimum policy for a given problem, that is, the best action to take at any given state. To do this, the agent takes an action and evaluates the subsequent reward/cost of taking that action given that it was

Table 2: Stage one action list.

Action	Connection	Processor	Tuple
A_1	Wi-Fi	Device	$A_1 = [0.004, 1, \chi_d, (E_{t_a} + E_{t_c} + E_{p_d} \cdot \theta), \Gamma_d]$
A_2	Wi-Fi	Fog	$A_2 = [0.62, 1, \chi_f, (E_{t_a} + E_{t_c} + E_{p_f} \cdot \theta), \Gamma_f]$
A_3	Wi-Fi	Cloud	$A_3 = [1, 1, \chi_c, (E_{t_a} + E_{t_c} + E_{p_c} \cdot \theta), \Gamma_c]$
A_4	NB-IoT	Device	$A_4 = [0, 0, \chi_d, (E_{t_b} + E_{p_d} \cdot \theta), \Gamma_d]$
A_5	NB-IoT	Cloud	$A_5 = [0.2, 0, \chi_c, (E_{t_b} + E_{p_c} \cdot \theta), \Gamma_c]$

in a certain state. This reward/cost is then used to update a look-up-table known as the Q-table, which is later utilised by the agent to select the best action. Further, the agent calculates the Q-value for every possible state/action pair. Therefore, a simple implementation can result in the agent learning online the best actions, regardless of the policy.

Moreover, Q-learning offers two key features which enable an efficient solution to our problem. First, as it is a model-free learning approach [21, 22], it is (1) capable of operating in dynamically changing environments, (2) a low-complexity algorithm which does not require a lot of power, thus reducing the energy consumption of the IoT network. Second, Q-learning is known to converge in most cases [23], which has also been demonstrated in multiagent noncooperative environments [24], as are IoT networks.

We propose a two-stage approach to solve the energy-aware smart IoT connectivity where each of the stages employs Q-learning.

4.1. First Stage Learning. Stage 1 consists of learning the best combination of connectivity and processing location in view of the device and application requirements and the limitations offered by each of these options. Thus, there are five possible actions that may be taken by each device as described in Table 2. As a side note, all the variables in Table 2 are the feature scaled values (into the range of [0, 1]) calculated through (5). The tuples shown represent the limitations of each action, e.g., $A_i = [R, \Sigma, \chi_l, E_t + E_p, \Gamma_l]$, where R and $E_t + E_p$ are described in Sections 3.3 and 3.2, respectively, χ_l is the available processing capacity, and Γ_l is the processing cost where $l = \{d, f, c\}$ as defined in Table 1. The parameter $\Sigma = \{1, 2\}$ refers to the level of data security offered by the wireless technology, whereby, the value 1 indicates eSIM protection (only provided by NB-IoT) and 2 the absence of that. Moreover, each device may be in four different states, as shown in Table 3, depending on the context-aware constraints defined jointly by the device and application. These constraints are R', Σ', and χ' which represent the response time, security level, and computational power requirements, respectively.

4.1.1. Penalty Function Determination. Each device will estimate the penalty function associated with each possible action it is able to take, following the system shown in Table 3, where $\varphi_p = \{R - R', \Sigma - \Sigma', \chi - \chi' \mid p = 1, 2, 3\}$ is the difference between the available and required characteristics. The fourth penalty is $\varphi_4 = \chi' \cdot A_i^{(5)} - b$, where $A_i^{(5)}$ is the fifth index of i^{th} action and the parameter b is the available budget.

The penalty function determination policy aims to satisfy the optimisation objective by including the elements that are desired to be minimised. As seen from Table 3, the penalty functions consist of three main elements: constant term, dissatisfaction level, and energy consumption. The constant value is the cost of being in the states and it decreases while the level of state increases. This element compels the agent try to achieve the highest possible level of states, as it is one of the objectives of the optimisation problem. The element of dissatisfaction level, as a supportive of the constant value, incurs cost for not satisfying the device requirements in order to improve the satisfaction levels. Lastly, the energy consumption element provides minimisation in the end-to-end energy consumption (connection and data processing). The parameter $0 \leq \nu \leq 1$ is the battery level, where 0 represents an empty battery and 1 represents the full charge. In the expressions in Table 3, the parameter ς specifies the priority level of the energy consumption. For instance, low values of ς prioritise the energy consumption once the battery level, ν, is very low (e.g., 5%), while high values prioritise the energy consumption even when the battery level is high (e.g., 50%).

In addition to all these, normally, the algorithm tends to select an option with a cloud processing, as it is the most energy efficient one. However, some amount of data will not be offloaded due to budget constraints, and will then be processed locally, which is the most energy consuming option. Note that this amount is evaluated by the second stage learning. Thus, the selected option by the first stage would be more energy consuming than the fog processing-included option, as the processing will be the combination of the cloud and device. Therefore, the last parts of the penalty functions (inside the square brackets) prevent the algorithm from making blind decisions, which ignores the budget availability, by including an average energy consumption of the actions with the device processing. The reason of taking the average value is that the final action is yet to be taken during the learning process. The coefficients of these three elements are determined empirically. However, they can be used to prioritise any element that is desired to be minimised more.

The Q-table entries are then updated according to the following expression, where s, s', P, and a are the current state, next state, penalty function, and action under evaluation:

$$Q(s,a) \longleftarrow Q(s,a) + \lambda \left(P(s) + \phi \min\left(Q\left(s', a\right)\right) - Q(s,a)\right). \quad (6)$$

Table 3: List of possible states of each device in Stage one and corresponding penalty calculation.

State	Description	Penalty function (P)
σ_1	None of the constraints are satisfied	$10^4 + \sum_{p=\{1-3\}} \varphi_p + 10^{\varsigma/\nu} \cdot \beta_1 \cdot A_i^{(4)} \cdot \left[\left(1 - \frac{\varphi_4}{\chi' \cdot A_i^{(5)}}\right) + \frac{\varphi_4 \cdot \left(\left(A_1^{(4)} + A_4^{(4)}\right)/2\right)}{\chi' \cdot A_i^{(5)}}\right]$
σ_2	One constraint is satisfied	$5 \times 10^3 + 0.8 \sum_{p=\{1-3\}} \varphi_p + 10^{\varsigma/\nu} \cdot \beta_1 \cdot A_i^{(4)} \cdot \left[\left(1 - \frac{\varphi_4}{\chi' \cdot A_i^{(5)}}\right) + \frac{\varphi_4 \cdot \left(\left(A_1^{(4)} + A_4^{(4)}\right)/2\right)}{\chi' \cdot A_i^{(5)}}\right]$
σ_3	Two constraints are satisfied	$2 \times 10^3 + 0.6 \sum_{p=\{1-3\}} \varphi_p + 10^{\varsigma/\nu} \cdot \beta_1 \cdot A_i^{(4)} \cdot \left[\left(1 - \frac{\varphi_4}{\chi' \cdot A_i^{(5)}}\right) + \frac{\varphi_4 \cdot \left(\left(A_1^{(4)} + A_4^{(4)}\right)/2\right)}{\chi' \cdot A_i^{(5)}}\right]$
σ_4	Three constraints are satisfied	$0.8 \sum_{p=\{1-2\}} \varphi_p + \varphi_3 + 10^{\varsigma/\nu} \cdot \beta_1 \cdot A_i^{(4)} \cdot \left[\left(1 - \frac{\varphi_4}{\chi' \cdot A_i^{(5)}}\right) + \frac{\varphi_4 \cdot \left(\left(A_1^{(4)} + A_4^{(4)}\right)/2\right)}{\chi' \cdot A_i^{(5)}}\right]$

Table 4: List of possible states of each device in Stage two and corresponding penalty calculation.

State	Description	Penalty function
$\ddot{\sigma}_1$	No availability in cloud or fog for χ'	$10^3 + \beta_2 \left(A_i^{(4)} \cdot \left(1 - \ddot{A}_i\right) + \chi' \cdot \ddot{A}_i \cdot A_i^{(5)}\right)$
$\ddot{\sigma}_2$	Enough availability in cloud or fog but no budget for χ'	$10^3 + \beta_2 \left(A_i^{(4)} \cdot \left(1 - \ddot{A}_i\right) + \chi' \cdot \ddot{A}_i \cdot A_i^{(5)}\right)$
$\ddot{\sigma}_3$	Enough availability and budget for χ'	$\beta_2 \left(A_i^{(4)} \cdot \left(1 - \ddot{A}_i\right) + \chi' \cdot \ddot{A}_i \cdot A_i^{(5)}\right)$

4.2. Second Stage Learning. The second stage aims to find the best policy for task offloading by considering the budget and availability of the fog or cloud. To this end, the second stage is activated only when the action taken in Stage 1 does not result in local processing (i.e., A_1 and A_4). In Stage 2, Q-learning is also employed with 21 possible actions = [0 : 0.05 : 1], and the constraints are the available budget b and the availability of the fog and/or cloud. The resulting states and penalty functions for this stage are listed in Table 4.

4.2.1. Penalty Function Determination. The penalty function of this stage is determined with a similar procedure to the first stage; hence, there are three cost elements: constant term, energy consumption, and monetary cost. Similar to the first stage, the constant value ensures ending up with the highest possible level of state. Having the energy consumption and monetary cost elements simultaneously provides finding the best trade-off between the two. However, unlike the first stage, these elements are calculated for a piece of data that is planned to be transferred, as specifying the best amount is the objective of this stage learning. Similarly, the coefficients are obtained empirically.

The interaction between Stage 1 and Stage 2 in the learning process is depicted in Algorithms 1 and 2, respectively.

5. Results and Analysis

In this section, we implement the proposed reinforcement learning approach in a simulation environment, as shown in Figure 4, using the parameter values defined in Table 1. We consider that half of the IoT devices connect with NB-IoT in view of the data privacy and related security requirements; these represent Group A. The remaining devices connect to the eNB through the WiFi gateway, hence over two wireless hops, and represent Group B. Consequently, there are six possible fixed scenarios that may be formed by selecting the processing location of each group of devices; these are listed in Table 6. A total of 100 iterations is conducted and, in each, random battery levels are allocated to each of the devices.

We compare the results obtained with our method to the six listed scenarios in terms of five different parameters: *energy*, *cost*, *dissatisfaction*, *number of out of budget devices*, and *joint penalty*. First, *energy* represents the end-to-end energy consumption caused from both connection and data processing. Second, *cost* is the overall monetary cost incurred by the use of the data processing locations, such as fog and cloud. Third, *dissatisfaction* is a measure of the total number of device requirements that are not satisfied. Fourth, *number of out of budget devices* reflects the count of devices that exceed their available monetary budgets during performing their tasks. Finally, *the joint penalty* indicates the cumulative combination of previous four parameters (*energy, cost, dissatisfaction,* and *number of out of budget devices*).

The results in terms of gain (positive values) and loss (negative values) are shown in Figure 5. Note that the values for parameters *energy*, *cost*, *dissatisfaction*, and *joint penalty* are obtained as follows:

$$g(x) = \frac{p_s - p_q}{p_q} \times 100, \tag{7}$$

where p_s and p_q are the values from Table 5 for Scenarios A-F and Q-learning, respectively.

On the other hand, the gain/loss values for the parameter of *number of out of budget devices* in Figure 5 is calculated using the function given as

$$o(x) = \frac{\#Out\ of\ Budget\ Devices}{N_G} \times 100. \tag{8}$$

It is worth noting that the results provided in Figure 5 are evaluated using the average values given in Table 5 along with 95% confidence intervals. Moreover, the joint cost parameter in Table 5 is calculated by summing them. However, before the summation, other four parameters (energy consumption,

Data: Context-aware constraints, available computational capacity in gateway and eNB, budget
Result: Combination of connectivity route and processing venue
initialization;
for *all IoT devices* **do**
  Determine the current state using Table 3;
  Evaluate all the actions;
  Calculate the penalty using Table 3;
  Select the best action;
  Jump to the next state;
  Update the Q-table;
  if *the selected action includes fog(gateway) or cloud (eNB) processing* **then**
    go to Algorithm 2
  end
end

Algorithm 1: First stage learning.

Data: Action selected by the first stage, available computational capacity in gateway and eNB, budget
Result: Share of data to be offloaded
initialization;
for *all IoT devices* **do**
  Determine the current state using Table 4;
  Evaluate all the actions;
  Calculate the penalty using Table 4;
  Select the best action;
  Jump to the next state;
  Update the Q-table;
end

Algorithm 2: Second stage learning.

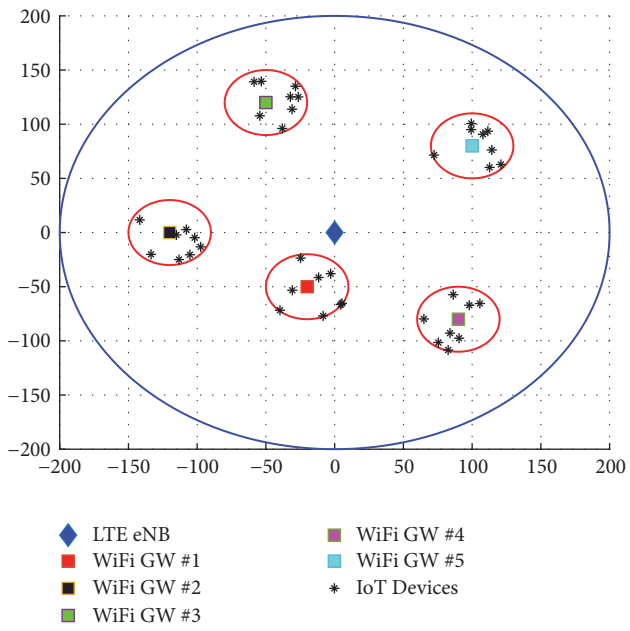


Figure 4: Sample snapshot of the simulation environment. IoT devices are located randomly, while positions of the gateways are fixed.

cost, dissatisfaction, and number of out of budget devices) are feature scaled into the range of [0, 1] using the function in (5) in order to keep their impacts in the same scale.

Our method outperforms any fixed combination when examining the joint or holistic gain, with values ranging from 95.9% to 283.54%. Similarly, the reinforcement learning technique results in better matching between the context-aware constraint and the availability of the IoT network compare to any other scenario, with gains varying from 183.33% to 344.44%. Although the processing cost of our proposed method is higher than that of Scenario A, the resulting gain in energy saving is even more important as well as the context-aware constraint compliance. The closest contender to reinforcement learning, with respect to the generated results, is Scenario C, in which the processing of Group A IoT devices is locally conducted while that of Group B occurs in the gateway. Nonetheless, the reinforcement learning allows for a device-driven context-aware connectivity that improves the compliance criteria by more than two times while saving 43.22% of energy, resulting in a holistic gain of 58.52%. Scenario D manages to reduce the energy consumption more than our proposed approach at the same total cost; however, 30.3% of the devices are out of budget resulting in incomplete or interrupted computational tasks.

Table 5: Results on various metrics for Q-learning and the scenarios.

	Energy Consumption (mJ)	Cost	Dissatisfaction	#Out of Budget Devices	Joint Cost
Q-Learning	5.69 ± 0.322	96.77 ± 4.01	1.8 ± 0.291	0 ± 0	0.7822
Scenario A	14.88 ± 0.385	$0.24 \pm 6.15e^{-3}$	5.1 ± 0.28	0 ± 0	1.5323
Scenario B	7.55 ± 0.24	118.57 ± 4.49	5.29 ± 0.181	3.03 ± 0.217	2.0679
Scenario C	8.16 ± 0.284	12.07 ± 0.383	5.81 ± 0.208	0 ± 0	1.2399
Scenario D	0.83 ± 0.025	130.41 ± 4.54	6 ± 0	3.03 ± 0.217	1.7756
Scenario E	7.48 ± 0.281	119.68 ± 3.83	7.81 ± 0.208	2.97 ± 0.213	2.4643
Scenario F	$0.15 \pm 4.59e^{-3}$	238.02 ± 6.16	8 ± 0	6 ± 0.339	3.0000

Table 6: List of fixed scenarios with connection types and locations of data processing.

Scenario	Group A	Group B
A	Device	Device
B	Cloud	Device
C	Device	Fog
D	Cloud	Fog
E	Device	Cloud
F	Cloud	Cloud

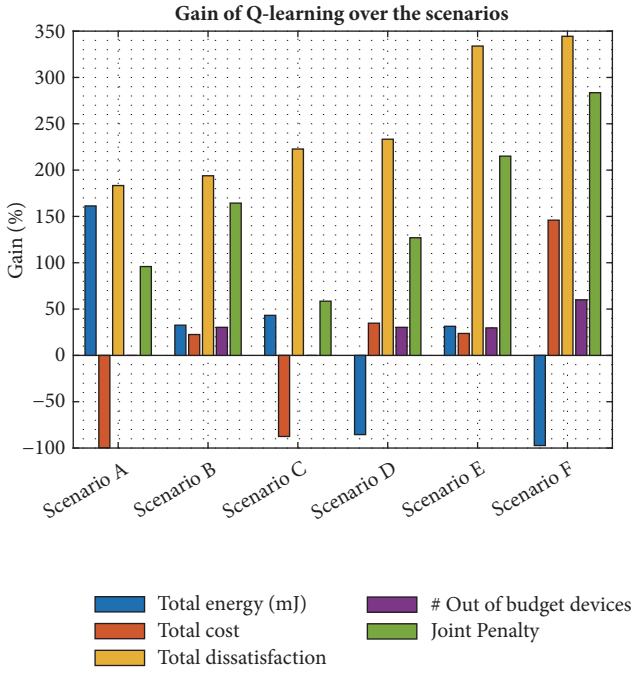


Figure 5: Summary of results for $\varsigma = 0.1$. Positive and negative values reflect gain and loss, respectively. Gain/loss occurs when the Q-learning/scenarios is better than the scenarios/Q-learning.

Moreover, in this scenario, connected devices are more than two times more likely to be dissatisfied with one or more of the context-aware requirements.

Next, we examine the impact of the battery priority factor, ς, on the energy efficiency. As shown in Figure 6, low values of ς result in almost neglecting the battery life of the device in the optimisation process until it drops below 10%. Very high

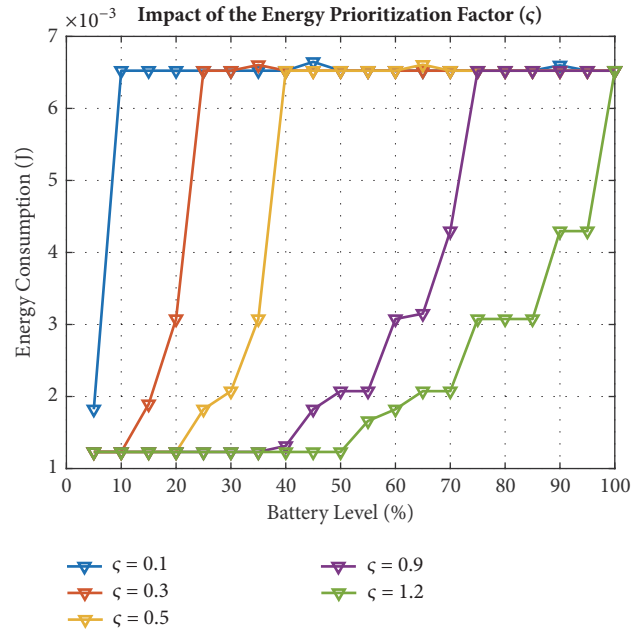


Figure 6: Impact of energy prioritisation factor ς.

values of ς prioritise the reduction of energy consumption for all devices except those that have higher than 70% battery life. To this end, it is possible to tune this parameter depending on the scenario at hand and in a device-specific manner. For instance, some devices may be part of a moving vehicle with the possibility of agile and low cost battery replenishment. Such devices may benefit from low settings of ς to allow more flexibility in meeting the remaining constraints. Other devices may be in hard-to-reach places and would require skilled force, special equipment, and hence high cost to replace the dead battery. In this case, higher settings of ς are more suitable and would result in better cost to quality ratio.

The simulation results achieved in this work are very promising, as they indicate a large margin for improvement that is not possible in fixed connection schemes. The proposed reinforcement learning method relies on centralised intelligence, which has access to all the constraints and requirements of all devices, gateways, and connections. Hence, the Q-learning-based method selects the best action (connection type/processing location pair in the first stage, and amount of data to be transmitted in the second stage) after the convergence. We appreciate that such a deployment

is not realistic and propose to explore the feasibility and corresponding gains of multiagent and distributed reinforcement learning, as adopted in [24], in our future work. Nonetheless, this work is undoubtedly the first to highlight the importance of context-aware connectivity in the IoT context that addresses jointly security, energy, and computational power as well as cost. We present a new application, Smart Ports, and quantify the potential margin for improvement by employing the novel scheme and highlight its effects on the application.

6. Conclusion

In this work, we have presented novel approach for energy-aware and context-aware IoT connectivity that jointly optimises the energy, security, computational power, and response time of the connection. The proposed scheme employs reinforcement learning and manages to achieve a holistic gain of up to 283.54% compared to deterministic routes. Although some deterministic scenarios may result in lower computational cost or lower energy consumption, none is able to meet the holistic context-aware performance target. In addition, we presented an analysis of the impact of the energy prioritisation factor in which we demonstrated the importance of tuning this parameter in a device-centric manner in order to achieve better optimisation of the whole system.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was partly funded by EPSRC Global Challenges Research Fund—the DARE Project—EP/P028764/1. The first author was supported by the Republic of Turkey Ministry of National Education (MoNE-1416/YLSY).

References

[1] S. Andreev, O. Galinina, A. Pyattaev et al., "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 32–40, 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] N. Kouzayha, M. Jaber, and Z. Dawy, "Measurement-based signaling management strategies for cellular IoT," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1434–1444, 2017.

[4] Y. Yang, M. Zhong, H. Yao, F. Yu, X. Fu, and O. Postolache, "Internet of things for smart ports: technologies and challenges," *IEEE Instrumentation Measurement Magazine*, vol. 21, no. 1, pp. 34–43, 2018.

[5] GSMA, "3GPP low power wide area technologies," GSMA, White paper, Oct 2016.

[6] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE coverage enhancements," 3GPP Thechnical Report 36, Jun 2012.

[7] Technologies Keysight, "The menu at the IoT cafe: a guide to IoT wireless technologies," *Application Note*, 2017.

[8] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in *Proceedings of the 2017 Eleventh International Conference on Sensing Technology (ICST)*, pp. 1–5, December 2017.

[9] S. Tayade, P. Rost, A. Maeder, and H. D. Schotten, "Device-centric energy optimization for edge cloud offloading," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pp. 1–7, Singapore, December 2017.

[10] F. Renna, J. Doyle, V. Giotsas, and Y. Andreopoulos, "Query processing for the internet-of-things: coupling of device energy consumption and cloud infrastructure billing," in *Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 83–94, Berlin, Germany, April 2016.

[11] S. Persia, C. Carciofi, and M. Faccioli, "NB-IoT and LoRA connectivity analysis for M2M/IoT smart grids applications," in *Proceedings of the 2017 AEIT International Annual Conference*, pp. 1–6, Cagliari, September 2017.

[12] A. Mihovska and M. Sarkar, "Smart connectivity for internet of things (IoT) applications," in *New Advances in the Internet of Things*, vol. 715 of *Studies in Computational Intelligence*, pp. 105–118, Springer International Publishing, Cham, 2018.

[13] N. Kouzayha, M. Jaber, and Z. Dawy, "M2M data aggregation over cellular networks: signaling-delay trade-offs," in *Proceedings of the 2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 1155–1160, December 2014.

[14] J. Xu, L. Chen, and P. Zhou, "Joint service caching and task offloading for mobile edge computing in dense networks," ArXiv e-prints 1801.05868, Jan 2018.

[15] O. Y. Bursalioglu, Z. Li, C. Wang, and H. Papadopoulos, "Efficient C-RAN random access for IoT devices: learning links via recommendation systems," ArXiv e-prints 1801.04001, Jan 2018.

[16] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[17] E. Oyekanlu, "Predictive edge computing for time series of industrial IoT and large scale critical infrastructure based on open-source software analytic of big data," in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, pp. 1663–1669, Boston, MA, USA, December 2017.

[18] S. Barbarossa, S. Sardellitti, E. Ceci, and M. Merluzzi, "The edge cloud: a holistic view of communication, computation and caching," ArXiv e-prints 1802.00700, Feb 2018.

[19] T. X. Vu, S. Chatzinotas, and B. Ottersten, "Edge-caching wireless networks: performance analysis and optimization," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2827–2839, 2018.

[20] ITU-R, "Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems and radio local area networks in the frequency range 300 MHz to 100 GHz," *International Telecommunication Union—Radiocommunication Sector, Geneva*, 2017, Recommendation ITU-R P.1411-9.

[21] L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: a survey," *Journal of Artificial Intelligence Research*, vol. 4, pp. 237–285, 1996.

[22] E. M. Russek, I. Momennejad, M. M. Botvinick, S. J. Gershman, and N. D. Daw, "Predictive representations can link model-based reinforcement learning to model-free mechanisms," *PLoS Computational Biology*, vol. 13, no. 9, Article ID e1005768, 2017.

[23] E. Even-Dar and Y. Mansour, "Convergence of optimistic and incremental q-learning," in *Advances in Neural Information Processing Systems*, pp. 1499–1506, 2002.

[24] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, "A distributed SON-based user-centric backhaul provisioning scheme," *IEEE Access*, vol. 4, pp. 2314–2330, 2016.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6319378, 14 pages
https://doi.org/10.1155/2018/6319378

Research Article

Robust and Low-Complexity Cooperative Spectrum Sensing via Low-Rank Matrix Recovery in Cognitive Vehicular Networks

Xia Liu, Zhimin Zeng, and Caili Guo

Beijing Laboratory of Advanced Information Networks, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China

Correspondence should be addressed to Xia Liu; liuxiabupt@bupt.edu.cn

Received 7 February 2018; Revised 16 April 2018; Accepted 15 May 2018; Published 26 June 2018

Academic Editor: Mahdi Ben Ghorbel

In cognitive vehicular networks (CVNs), many envisioned applications related to safety require highly reliable connectivity. This paper investigates the issue of robust and efficient cooperative spectrum sensing in CVNs. We propose robust cooperative spectrum sensing via low-rank matrix recovery (LRMR-RCSS) in cognitive vehicular networks to address the uncertainty of the quality of potentially corrupted sensing data by utilizing the real spectrum occupancy matrix and corrupted data matrix, which have a simultaneously low-rank and joint-sparse structure. Considering that the sensing data from crowd cognitive vehicles would be vast, we extend our robust cooperative spectrum sensing algorithm to dense cognitive vehicular networks via weighted low-rank matrix recovery (WLRMR-RCSS) to reduce the complexity of cooperative spectrum sensing. In the WLRMR-RCSS algorithm, we propose a correlation-aware selection and weight assignment scheme to take advantage of secondary user (SU) diversity and reduce the cooperation overhead. Extensive simulation results demonstrate that the proposed LRMR-RCSS and WLRMR-RCSS algorithms have good performance in resisting malicious SU behavior. Moreover, the simulations demonstrate that the proposed WLRMR-RCSS algorithm could be successfully applied to a dense traffic environment.

1. Introduction

Social problems of road accidents, traffic congestion, and air pollution are becoming increasingly severe with the increasing number of vehicles worldwide. According to a report published by the World Health Organization (WHO), approximately 1.25 million people die each year because of road traffic collisions [1]. Vehicular networks are envisioned to revolutionize the lifestyle of human beings within the next few years, with the aim of reducing the number of traffic collisions and providing entertainment services. According to the current standard for Wireless Access in Vehicular Environments (WAVE) [2, 3], multiple channels with one control channel (CCH) and six service channels (SCHs) for data exchange are permitted to support safety-related services (e.g., lane change assistance, and intersection collision warning) and non-safety-related services (e.g., commercial infotainment, multimedia downloads).

However, both theoretical analysis and simulation results indicate that the currently allocated bandwidth is not sufficient to provide reliable safety-related services under certain heavy traffic conditions [4–7]. The generation rate of a typical basic safety message (BSM) is from 2 to 10 messages per second to support many safety-related applications [6]. The high probability of an increased BSM generation rate in a heavy traffic environment will lead to the CCH becoming congested due to an increased number of packet collisions. This congestion will decrease the reliability of vehicular communication. Moreover, certain studies have demonstrated that non-safety-related services of the allocated band might also have to be severely restricted in high-density traffic. Reference [7] proved that a large share of non-safety-related services only appropriates in low or moderate traffic conditions. Additionally, only 10% of the bandwidth would remain for non-safety-related applications in order to guarantee 95% of the reliability of transmissions for safety-related applications in a high traffic environment.

Cognitive radio (CR) technology is a feasible measure that has been used to solve the spectrum scarcity problems in vehicular networks (see, e.g., the recent overviews in [8, 9]).

In cognitive vehicular networks (CVNs), as unlicensed users, the vehicles equipped with CR can detect and use other idle licensed spectrums when the primary user (PU) is absent. Cooperative spectrum sensing (CSS) has been extensively investigated in efforts to improve the detection performance via the diversity gain of cooperative secondary users (SUs) in CVNs [10–14]. These papers have shown that CSS can achieve spatial diversity gains under the assumption that the collaborative SUs are proactive. However, none of these studies have considered that SU sensing data may be unreliable due to either certain malicious behaviors or unexpected equipment failures. Many envisioned applications in vehicular networks that are related to safety would need high reliable connectivity. Therefore, some preliminary work in [15–20] has focused on increasing the robustness of cooperative spectrum sensing in cognitive vehicular networks. However, it is hard to implement these methods in practical CVNs environment due to their complexity, especially under heavy traffic conditions. While moving on the road, it is difficult to detect a malicious vehicle that may be transmitting untrustworthy spectrum sensing data during a sensing period. One challenge in CSS is the uncertainty of the sensing data quality, which may be corrupted by unreliable vehicles. This uncertainty motivated us to investigate the issue of efficient and robust CSS in CVNs. We formulate an optimization problem as a low-rank and sparse recovery by utilizing the real spectrum occupancy matrix and corrupted data matrix, which have a simultaneously low-rank and joint-sparse structure. In our previous work [21], our model simply assumed that cognitive vehicles carried out low-speed and single movement on a highway. But this assumption, apparently, is not always conformed with the real case, considering that, in CVNs, vehicle density reveals sparse and dense fluctuations with the space and time. As there are few users participating in cooperative sensing with sparse traffic flows, it is impossible to improve the detection probability of cooperative spectrum sensing. When the vehicles are dense, it has a large number of cooperative users, which makes the algorithm more expensive. In view of the above problems, this study is focused on establishing different algorithms for actual nondense and dense traffic environment. Firstly, LRMR-RCSS algorithm in this paper is established to recover the real data from noisy and corrupted data for improving the spectrum sensing data quality and CSS performance, which is applicable to low traffic density environments. The low-rank matrix $\mathbf{X}$ is directly recovered by the ALM algorithm. At the same time, we extend our robust cooperative spectrum sensing algorithm WLRMR-RCSS algorithm into dense cognitive vehicular networks by considering the reliability of cooperative cognitive vehicles. Different from [21], this study concentrates on the adaptability of the WLRMR-RCSS algorithm with the change of traffic density. In this paper, we analyze the improvement of algorithm performance in traffic density from the sparse to dense state and the changes in the number of selected cooperative users under different traffic density. In the simulation process, VISSIM, the software of traffic flow, is used to generate the traffic flow in this article. We demonstrate that our proposed LRMR-RCSS and WLRMR-RCSS algorithms are secure and more efficient in CVNs, and the WLRMR-RCSS algorithm is particularly robust against traffic density changes.

1.1. Related Work. In traditional CSS, many defense methods have been proposed in the literature in order to mitigate the negative effect of false spectrum sensing data. These methods could be classified into SU weighting schemes and SU filtering schemes. In SU weighting schemes, all the spectrum sensing data take part in the cooperation and smaller weights are assigned to the data of lower quality. In SU filtering schemes, it is to take out the "detected malicious SUs," and only utilize the remaining spectrum sensing data from the "detected honest SUs" for cooperation.

In the context of SU weighting schemes in CVNs, paper [15] proposed to apply Belief Propagation (BP) in order to establish the belief on the existence of primary users to its neighbors. In this paper, the spatial correlation between neighboring vehicles is exploited by message passing. In [16], an entropy-based voting algorithm was proposed to decide whether a channel is available with its one-hop neighbor vehicles. In [10], a weighting function based on the distance between the vehicle and its neighbor is established for the sake of evaluating neighbors' credibility with reference to the aggregated spectrum sensing decisions. In fact, the distance may not actually be in accordance with the neighbors' credibility. Due to fading of the communication links, environmental obstacles, or transmission errors, each neighbor's credibility can potentially be distinct based on the vehicular environment. In addition, many security threats have been raised as a result of the openness of low-layer protocol stacks in cognitive vehicular networks [17]. The malicious cognitive vehicles can introduce false data to confuse the cooperated vehicles. At this point, CSS would be distorted by malicious cognitive vehicles. For example, when the false data is introduced, the CSS result might conclude in the presence of PU, on the contrary. By doing so, these malicious cognitive vehicles can use the PU channels selfishly. References [18, 19] introduced CSS with trust assistance to solve the security issue that was introduced by a spectrum sensing data falsification (SSDF) attack in CVNs. Despite few SU filtering schemes in CVNs, data recovery algorithm provides a new approach. In [20], in order to mitigate the influence of abnormal data on the performance of CSS, a robust cooperative spectrum sensing has been studied for a wireless sensor networks environment. Nuclear norm minimization is adopted to recover the real spectrum sensing data in this paper.

The aforementioned methods [15–19] have played a vital role in fostering new strategies for robust spectrum sensing in CVNs. However, many of the methods in these papers are trust-based, which utilize historical information on malicious vehicles' behavior. Responsible reputation information is not invariably available because well-established historical statistics would be too expensive or even unrealistic in fast changing CVNs. In addition, as [22] notes, intelligent malicious users can send random false values that are close to the real values. In this case, it is more of a challenge to recognize the malicious users than the types that always send very high or very low values. The aforementioned low-rank matrix

recovery-based CSS method [20] focuses on improving sensing data quality without considering high data transmission cost in CSS networks. These above methods are complex to implement in practical CVNs due to their complexity or hardware facility. In CVNs, the network topology changes quickly with diverse vehicles taking part in the cooperation at different times. The cost of transmission from cognitive vehicles to the fusion center (FC) is high as all the collected cognitive vehicles' spectrum sensing data are transmitted to an FC, which is inefficient or even unaffordable. Therefore, a robust cooperative spectrum detection algorithm with low complexity in CVNs is strongly needed but challenging to achieve.

1.2. Our Contribution. In this paper, our contribution comprises three parts.

(i) We develop a robust cooperative spectrum sensing algorithm LRMR-RCSS in CVNs, with a view to guaranteeing sensing data quality. We recover the real spectrum sensing data from the noisy and abnormal data to improve the quality of the sensing data by taking advantage of the real spectrum occupancy matrix, and the corrupted data matrix has a simultaneously low-rank and joint-sparse structure.

(ii) By extending our LRMR-RCSS algorithm to dense CVNs, we propose a WLRMR-RCSS algorithm. In the WLRMR-RCSS algorithm, we establish a correlation-aware selection and weight assignment scheme for cooperative SUs in heavy traffic environments. A certain number of cognitive vehicles are chosen by considering the correlation between the SUs. Based on this scheme, our WLRMR-RCSS algorithm obtains cooperative SU diversity and reduces cooperative overhead. The complexity of the cooperative spectrum sensing in the CVNs is reduced.

(iii) The simulations demonstrate that the LRMR-RCSS and WLRMR-RCSS algorithms can effectively mitigate the adverse effects of corrupted data introduced by the malicious behaviors of SUs. Moreover, the proposed WLRMR-RCSS algorithm can be successfully applied in a dense traffic environment.

The remainder of this paper is organized as follows. In Section 2, we construct the system model and problem formulation. In Section 3, we provide details of our proposed LRMR-RCSS and WLRMR-RCSS algorithms. In Section 4, we present the simulation results and demonstrate the correctness of the theoretical analysis and make comparisons with other algorithms under low and high traffic density environments. Finally, we provide our conclusions in Section 5. Table 1 shows the notations.

Table 1: Notations.

Variables	Explanation
PU	Primary user
SU	Secondary user
CVNs	Cognitive vehicular networks
CSS	Cooperative spectrum sensing
FC	Fusion center
ED	Energy detection
SSDF	spectrum sensing data falsification
EGC	Equal Gain Combining
ADMM	The proximal alternating direction method of multipliers
P_d	The detection probability
P_f	The false alarm probability
r_m	the received signal at the mth SU in one subband
Th	The preset threshold at the FC
y_m	The detected energy at the mth SU
Y_n	The detected energy calculated by EGC
$\sigma_{s,m}^2$	The received primary signal power at the mth SU
σ_n^2	The noise power
h_m	The channel response
d_{corr}	The decorrelation function
$R(\cdot,\cdot)$	The correlation function between two nodes
d_{ij}	The distance between the node i and j
Ω	The set of vehicles
N	The number of subband
N_{sam}	The number of samples in each subband
λ	The tradeoff parameter
μ	A constant (> 0)
M	The number of cooperative vehicles
ρ	A constant (> 1)
$s_t(\cdot)$	The shrinkage operator
$\mathbf{Y}$	The sensing data matrix at the FC
$\mathbf{R}$	The energy matrix
$\mathbf{O}$	The real occupancy state matrix
$\mathbf{A}$	The energy detector output matrix
$\mathbf{V}$	The noise matrix
$\mathbf{A}$	The corrupted data matrix
$\mathbf{W}$	The weighting matrix
$\mathbf{U}$	The unitary matrix
$\mathbf{\Sigma}$	The positive semi-definite diagonal matrix
$\mathbf{Q}$	The unitary matrix
$\mathbf{G}$	The Lagrangian multiplier matrix

2. System Model and Problem Formulation

2.1. System Model. A typical cognitive vehicular network communications scenario is shown in Figure 1. For simplicity, we consider a cognitive vehicular network scenario of a road that consists of a primary network and a secondary network that is colocated in a geographical area. The PU owns several licensed wideband channels that are divided into N subbands. According to the existing spectrum measurements in [24–26], the licensed subbands are underutilized; namely, the spectrum occupancy rate of these N subbands is relatively low. The secondary network is an infrastructure-based network that contains several SUs and a fusion center.

There are many vehicles traveling along the road, and they are equipped with spectrum sensing-enabled terminals and Global Positioning System (GPS) devices. M SUs participate in the cooperative sensing process. Furthermore, the SUs are supposed to be randomly distributed along the road. Each SU first performs energy detection (ED) to detect the presence of a PU in each subband, either concurrently [27] or sequentially [28], and then reports the measurement results to the FC at the end of the sensing period. In the case of sequential sensing, each SU has to report the measurements to the FC which should collect the measurements from all SUs. This process may take time, especially under high traffic environment. By the time the FC took the decision, the SU might have a different observation. Therefore, we adopt the pattern of [27] in this paper. After fusing the collected sensing data, the FC makes a decision regarding the occupancy state of the N subbands as either present (H_1) or absent (H_0). It is further noticed that some of the Sus would send corrupted values to the FC, such as SU_1, SU_4, and SU_M, as labeled in Figure 1. Because some SUs may experience deep fading or shadowing in CVNs, they may always send very low power values to the FC regardless of the spectrum occupancies. On the other hand, some SUs may show malicious behaviors in order to use the PU channels selfishly. These malicious vehicles appear randomly to corrupt a random number of channels at random locations.

Assume that the PU state remains unchanged during each spectrum sensing period. We adopt ED; then, the received signal r_m at the mth SU in one subband under the two hypotheses is expressed as

$$r_m(k) = \begin{cases} n_m(k), & H_0 \\ h_m s_m(k) + n_m(k), & H_1, \end{cases} \quad k = 0, 1, \ldots, N_{sam} - 1 \tag{1}$$

where N_{sam} is the number of samples in each subband, n_m is additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2, h_m is the channel response related to the location of the SU, and s_m denotes the transmitted signal of the PU. The detected energy y_m at the mth SU is

$$y_m = \frac{1}{N_{sam}} \sum_{k=0}^{N_{sam}-1} |r_m(k)|^2 \tag{2}$$

According to the Central Limit Theorem, y_m can approximate the Gaussian distribution as

$$y_m \sim \begin{cases} N\left(\sigma_n^2, \dfrac{2\sigma_n^4}{N_{sam}}\right) & H_0 \\ N\left(\left(\sigma_n^2 + \sigma_{s,m}^2\right), \dfrac{2\left(\sigma_n^2 + \sigma_{s,m}^2\right)^2}{N_{sam}}\right) & H_1 \end{cases} \tag{3}$$

where $\sigma_{s,m}^2$ is the received primary signal power and σ_n^2 is the noise power.

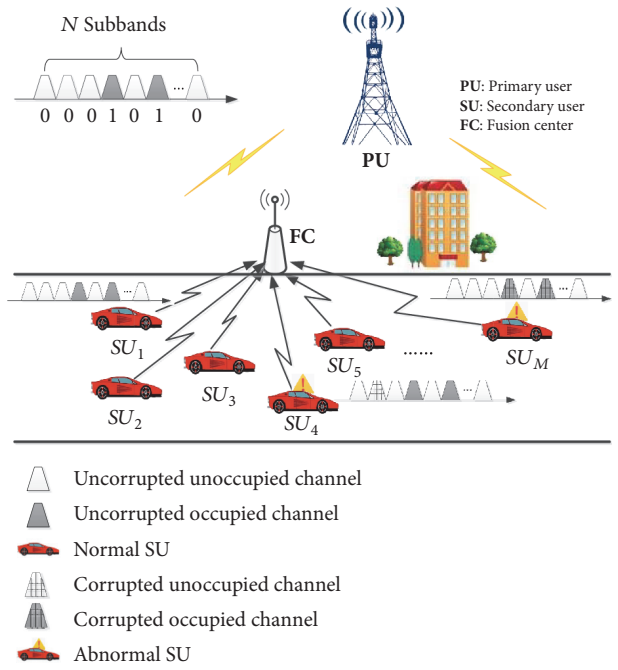


Figure 1: Network model of cooperative spectrum sensing in CVNs with malicious users.

After performing local spectrum sensing, SUs send their local ED results directly to the FC. For the soft-decision schemes [29] considered in this paper, the FC employs the equal gain combining (EGC) rule and calculates the ED results Y_w. According to (2) and (3), Y_w obeys the distribution

$$Y_w \sim \begin{cases} N\left(M\sigma_n^2, \dfrac{2M\sigma_n^4}{N_{sam}}\right) & H_0 \\ N\left(\sum_{m=1}^{M}\left(\sigma_n^2 + \sigma_{s,m}^2\right), \sum_{m=1}^{M}\dfrac{2\left(\sigma_n^2 + \sigma_{s,m}^2\right)^2}{N_{sam}}\right) & H_1 \end{cases} \tag{4}$$

Then, the detection probability P_d and false alarm probability P_f can be expressed as

$$P_d = P\left(Y_w > Th \mid H_1\right) = Q\left(\frac{Th - \sum_{m=1}^{M}\left(\sigma_n^2 + \sigma_{s,m}^2\right)}{\sqrt{\sum_{m=1}^{M}\left(2\left(\sigma_n^2 + \sigma_{s,m}^2\right)^2 / N_{sam}\right)}}\right) \tag{5}$$

$$P_f = P\left(Y_w > Th \mid H_0\right) = Q\left(\frac{Th - \sigma_n^2}{\sqrt{2\sigma_n^4 / N_{sam}}}\right) \tag{6}$$

where $Q(x)$ is the complementary distribution function, and $Q(x) = (1/\sqrt{2\pi}) \int_x^{+\infty} \exp(-x^2/2)dx$. Th represents the preset threshold in the FC,

$$Th = \sqrt{\frac{2\sigma_n^4}{N_{sam}}} Q^{-1}\left(P_f\right) + \sigma_n^2 \tag{7}$$

where $Q^{-1}(\cdot)$ is the inverse Q-function.

Note that the distance between SUs and a PU is a crucial parameter for spectrum sensing in CVNs because the distance determines whether a PU is inside the sensing range of SUs or not. Because cognitive vehicle is mobile, the PU may fall within or outside the sensing range of the cognitive vehicle after a certain time. Whether or how long the PU in CVNs can fall within the SUs' sensing range is determined by the speed and direction of the cognitive vehicle. Different from other mobile ad hoc networks, cognitive vehicles in CVNs move in same direction or opposite directions based on the road structure. It has demonstrated that whether a PU is inside the sensing range of SUs would be related to velocity of SUs, sensing range of SU, and transmission range of PU [30, 31].

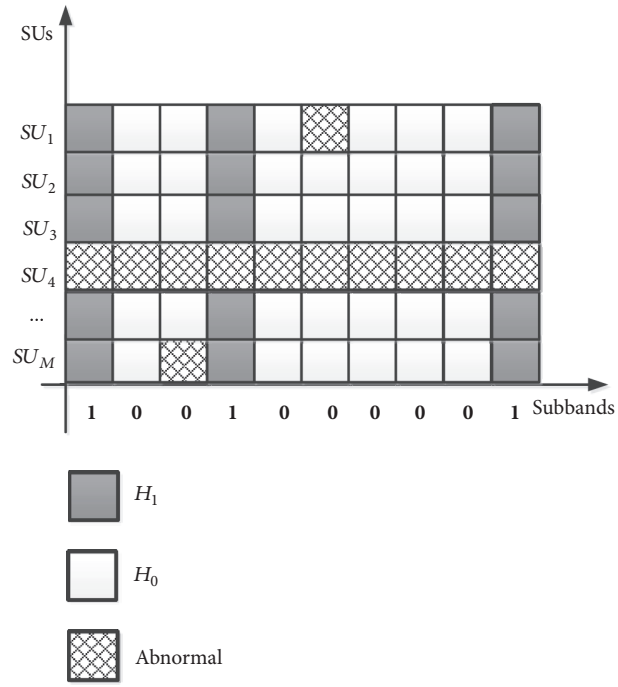


Figure 2: Example of a corrupted data distribution [21].

2.2. Problem Formulation. Although cooperation can significantly exploit the spectrum sensing in CVNs, it also introduces a security hole for various malicious attackers. Some studies have recently considered an attack model known as SSDF [32–34], which is a fatal threat to CSS. There are several typical attack patterns under the SSDF model, which are known as always opposite (AO), always busy (AB), always free (AF), and random disguising. In these attack models, AO attacks always send opposite decisions. AB attacks always report that the PU is present, whereas AF attacks always declare that the PU is absent. The random disguising attack may not always transmit false spectrum sensing data.

Notably, all of these attack patterns introduce corrupted spectrum sensing data for CSS. Figure 2 shows an example of a corrupted data distribution in CVNs. Some vehicles may nonrandomly transmit fake spectrum sensing data as SU_4 (which always exhibit malicious behavior). Some vehicles may sporadically send unreliable data, such as SU_1 and SU_M. As in the above discussion, both nonrandom and random abnormal data have an adverse influence on the certainty of the spectrum sensing result. These events occur only occasionally in practice. In other words, the abnormal data are randomly and sparsely distributed. The matrix constructed by the received signals exhibits a low-rank property, as indicated in [35–37].

In this paper, we consider the case that every cognitive vehicle could sporadically and randomly contribute with abnormal data, due to either accidental equipment failures or random malicious behaviors, which makes the cooperative spectrum sensing inaccurate. Let $\mathbf{O}_{N\times N} \coloneqq [O_{n,n}]$, $\mathbf{Y}_{M\times N} \coloneqq [y_{m,n}]$, $\mathbf{R}_{M\times N} \coloneqq [r_{m,n}]$, $\mathbf{V}_{M\times N} \coloneqq [v_{m,n}]$, and $\mathbf{A}_{M\times N} \coloneqq [a_{m,n}]$ denote the real occupancy state matrix, the sensing data matrix at the FC, the energy matrix for M Sus, the noise matrix, and the corrupted data matrix, respectively. The sensing data matrix $\mathbf{Y}$ at the FC can be expressed as

$$\mathbf{Y}_{M\times N} = \mathbf{R}_{M\times N}\mathbf{O}_{N\times N} + \mathbf{V}_{M\times N} + \mathbf{A}_{M\times N} \tag{8}$$

Diagonal matrix $\mathbf{O}$ satisfies $\text{rank}(\mathbf{O}) < N$ due to the underutilization of licensed bands. Therefore, matrix $\mathbf{O}$ is low-rank. Considering the random malicious behaviors in CVNs, nonzero entries in the matrix $\mathbf{A}$ are supposed to be randomly and sparsely distributed. So the matrix $\mathbf{A}$ has sparsity property. Our goal is to recover the real spectrum occupancy state matrix $\mathbf{O}$ from the noisy and corrupted observations $\mathbf{Y}$ by taking advantage of the low-rank property of $\mathbf{O}$ and the sparsity property of $\mathbf{A}$.

In static environment, malicious SUs would have dominated the location reliability for the fixed Region. However, in CVNs, the malicious cognitive vehicles distributed across all the road over time. On the other hand, mobile honest cognitive vehicles help to train location reliability of each road segment. As a result, the reports generated from a road segment at different times are from different vehicles. As malicious users are full of sparse characteristics, spectrum sensing data polluted in the report should also possess sparse features.

3. Proposed Algorithms

3.1. Robust Cooperative Spectrum Sensing via Low-Rank Matrix Recovery in CVNs (LRMR-RCSS). Here, we introduce a matrix $\mathbf{X}_{M\times N} \coloneqq \mathbf{R}_{M\times N}\mathbf{O}_{N\times N}$ that represents the energy detector output matrix. Matrix $\mathbf{X}$ is also low-rank because $\text{rank}(\mathbf{X}) \leq \min(\text{rank}(\mathbf{R}), \text{rank}(\mathbf{O}))$. In such a CSS network, we must reconstruct the real energy matrix from the sensing

data matrix at the FC by a low-rank matrix recovery technique [38–41]. The goal of recovering the spectrum occupancy state matrix $\mathbf{O}$ translates into approximately recovering matrix $\mathbf{X}$ because it is difficult to recover $\mathbf{O}$ directly.

According to the current low-rank matrix recovery theory, to recover the low-rank matrix $\mathbf{X}$ from the sensing data matrix $\mathbf{Y}$, it can be formulated as

$$\begin{aligned} \min_{\mathbf{X},\mathbf{A}} \quad & \operatorname{rank}(\mathbf{X}) + \lambda \|\mathbf{A}\|_0 \\ \text{s.t.} \quad & \mathbf{Y} = \mathbf{X} + \mathbf{A} + \mathbf{V} \end{aligned} \tag{9}$$

where $\operatorname{rank}(\cdot)$ is the rank of the matrix, and $\|\cdot\|_0$ is the number of nonzero entries in the matrix. λ is a positive rank-sparsity controlling parameter which represents a tradeoff parameter to balance matrix $\mathbf{X}$ and matrix $\mathbf{A}$.

According to previous research [39–41], we introduce a matrix $\mathbf{G}$ of the Lagrangian multiplier; then, model (9) could be transferred to minimizing the following augmented Lagrangian function $\mathscr{L}$:

$$\begin{aligned} \mathscr{L}(\mathbf{X}, \mathbf{A}, \mathbf{G}, \mu) = {} & \|\mathbf{X}\|_* + \lambda \|\mathbf{A}\|_1 + \langle \mathbf{G}, \mathbf{Y} - \mathbf{X} - \mathbf{A} \rangle \\ & + \frac{\mu}{2} \|\mathbf{Y} - \mathbf{X} - \mathbf{A}\|_F^2 \end{aligned} \tag{10}$$

where $\|\cdot\|_*$ is the sum of the singular values and represents the nuclear norm of a matrix, $\|\cdot\|_1$ is the l_1-norm which denotes the sum of the absolute values of matrix entries, $\|\cdot\|_F$ is the Frobenius norm $\|\mathbf{A}\|_F = \sqrt{tr\mathrm{AA}^T}$, $\langle \mathbf{A}, \mathbf{B} \rangle \equiv \operatorname{tr}(\mathbf{A}^{\mathrm{T}}\mathbf{B})$. Then, the optimal solution to the original problem can be obtained by iterating the following two steps until convergence for some $\rho > 1$:

$$\begin{aligned} (\mathbf{X}_{k+1}, \mathbf{A}_{k+1}) &\longleftarrow \min_{\mathbf{X},\mathbf{A}} \mathscr{L}(\mathbf{X}, \mathbf{A}, \mathbf{G}_k, \mu_k) \\ \mu_{k+1} &\longleftarrow \rho \mu_k \\ \mathbf{G}_{k+1} &\longleftarrow \mathbf{G}_k + \mu_k (\mathbf{Y} - \mathbf{X}_{k+1} - \mathbf{A}_{k+1}) \end{aligned} \tag{11}$$

where $\mu > 0$ denotes the penalty for infeasible points. According to [38], update the $\mathbf{X}$ and $\mathbf{A}$ in order to search for the optimal $\mathbf{X}$ and $\mathbf{A}$ alternately and iteratively as follows:

$$\begin{aligned} \mathbf{X}_{k+1} &= \arg_{\mathbf{X}} \min (\mathbf{X}_k, \mathbf{A}_k, \mathbf{G}_k, \mu) \\ &= \arg_{\mathbf{X}} \min \|\mathbf{X}\|_* + \frac{\mu_k}{2} \|\mathbf{Y} - \mathbf{X} - \mathbf{A}\|_F^2 \\ &\quad - Tr\left((\mathbf{G}_k)^T \mathbf{X}\right) \end{aligned} \tag{12}$$

$$\begin{aligned} \mathbf{A}_{k+1} &= \arg_{\mathbf{A}} \min \lambda \|\mathbf{A}\|_* + \frac{\mu_k}{2} \|\mathbf{Y} - \mathbf{X}_{k+1} - \mathbf{A}\|_F^2 \\ &\quad - Tr\left((\mathbf{G}_k)^T \mathbf{A}\right) \end{aligned} \tag{13}$$

Then the optimization problems in (11) can be solved as follows [41]:

$$\begin{aligned} \mathbf{X}_{k+1} &\longleftarrow \mathbf{U}_k s_{\mu_k^{-1}}[\mathbf{\Sigma}_k] \mathbf{Q}_k^{\mathrm{T}} \\ \mathbf{A}_{k+1} &\longleftarrow s_{\lambda\mu_k^{-1}}\left[\mathbf{Y} - \mathbf{X}_{k+1} + \mu_k^{-1}\mathbf{G}_k\right] \\ \mathbf{G}_{k+1} &\longleftarrow \mathbf{G}_k + \mu_k\left[\mathbf{Y} - \mathbf{X}_{k+1} - \mathbf{A}_{k+1}\right] \end{aligned} \tag{14}$$

Initialization: $\mathbf{G}_1 = 0$, $\mathbf{A}_1 = 0$, $\mu_1 = 0.1$, $\rho = 1.1$, $k = 1$, $\lambda > 0$
Output: $\mathbf{X}$, $\mathbf{A}$, Y_n
Given $\mathbf{X} \coloneqq [x_{m,n}]$;
while not converged **do**
$(\mathbf{U}_k, \mathbf{\Sigma}_k, \mathbf{V}_k) \leftarrow svd(\mathbf{Y} - \mathbf{A}_k + \mu_k^{-1}\mathbf{G}_k)$;
  update $\mathbf{X}_{k+1} \leftarrow \mathbf{U}_k s_{\mu_k^{-1}}[\mathbf{\Sigma}_k]\mathbf{V}_k^{\mathrm{T}}$;
  update $\mathbf{A}_{k+1} \leftarrow s_{\lambda\mu_k^{-1}}[\mathbf{Y} - \mathbf{X}_{k+1} + \mu_k^{-1}\mathbf{G}_k]$;
  update $\mathbf{G}_{k+1} \leftarrow \mathbf{G}_k + \mu_k[\mathbf{Y} - \mathbf{X}_{k+1} - \mathbf{A}_{k+1}]$;
  update $\mu_{k+1} \leftarrow \rho\mu_k$;
  $k = k + 1$;
end while
for $n = 1, \ldots N$, $\mathbf{X}_{M\times N} \coloneqq [x_{m,n}]$ **do**
$Y_n = \sum_{m=1}^{M} x_{m,n} \gtrless Th$;
end for
Return $\mathbf{X}$, $\mathbf{A}$, Y_n;

Algorithm 1: Robust cooperative spectrum sensing via low rank matrix recovery in CVNs (LRMR-RCSS).

where $s_t(\cdot)$ is shrinkage operator, which is defined as $s_t(x) = \operatorname{sign}(x) \cdot \max(|x| - t, 0)$, and $(\mathbf{U}_k, \mathbf{\Sigma}_k, \mathbf{Q}_k) \equiv svd(\mathbf{Y} - \mathbf{A}_k + \mu_k^{-1}\mathbf{G}_k)$. We obtain the real sensing data $\mathbf{X}$ based on these steps. Next, we perform spectrum sensing by data fusion. The main steps of our proposed LRMR-RCSS are outlined in Algorithm 1.

Computational Complexity Analysis. The primary computational cost of the LRMR-RCSS algorithm is the singular value decomposition (SVD) of an $M \times N$ matrix in the process of updating $\mathbf{X}$ when using the augmented Lagrangian multiplier (ALM) approach. Its computational complexity is $O(MN \min(M, N))$. On the other hand, the number of iterations taken by the LRMR-RCSS algorithm to optimality is less vulnerable to changes in dimension, which has a worst-case complexity result of $O(k^{-2})$.

3.2. Extension to Robust Cooperative Spectrum Sensing via Weighted Low-Rank Matrix Recovery in Dense CVNs (WLRMR-RCSS). In general, the calculation to solve the low-rank model is very large when faced with a large matrix problem. Reference [40] proposed an algorithm to reduce the complexity, but this algorithm must dynamically predict the value of the rank. Therefore, it suffers from high computational cost when M is large during dense traffic in vehicular networks. In this part, we focus on solving the problem of robust CSS in a dense vehicular network environment. Cognitive vehicles experience different environmental conditions and contribute to spatial diversity based on their distribution. The sensing data could be combined based on the reliability factor of an SU, which is considered its weight. Therefore, we propose a novel weighted low-rank matrix recovery model for spectrum sensing as follows:

$$\begin{aligned} \min_{\mathbf{X},\mathbf{A}} \quad & \operatorname{rank}(\mathbf{X}) + \lambda \|\mathbf{A}\|_0 \\ \text{s.t.} \quad & \mathbf{W} \circ \mathbf{Y} = \mathbf{W} \circ \mathbf{X} + \mathbf{V} + \mathbf{A} \end{aligned} \tag{15}$$

Initialization: $S = \phi$, $\psi = \phi$, $\mathbf{G}_1 = 0$, $\mathbf{A}_1 = 0$, $\mu_1 = 0.1$, $\rho = 1.1$, $k = 1$, $\lambda > 0$, $\mathbf{X} \coloneqq [x_{m,n}]$;
Output: $\mathbf{W}$, $\mathbf{X}$, $\mathbf{A}$, Y_n;
Randomly select s_k, **do**
$S \leftarrow \{s_k\}$, $\varphi \leftarrow \Omega - \{s_k\}$, $choosed \leftarrow s_k$;
while $\psi = \phi$ **do**
  for $s_q \in \varphi$ **do**
    if $R\{choosed, s_q\} < \tau$ **then**
      $\varphi \longleftarrow \varphi - \{s_q\}$;
    end if
  end for
find $s_q \in \varphi$, $R(s_q, choosed) = \max R(s_q, choosed)$
  $S \leftarrow s_q$, $\varphi \leftarrow \Omega - \{s_q\}$ **then**
  $choosed \longleftarrow s_q$;
end while
  for each SU, $s_i, s_j, s_p \in S$ **do**
    $$\omega_i = 1 - \frac{\sum_{s_i \in S} R(s_i, s_j)}{\sum_{s_p \in S} \sum_{s_j \in S} R(s_p, s_j)}$$
  end for
  for $R_{\max} = \max\{R(s_i, s_j), \ \forall s_i, s_j \in S\}$ **do**
    choose $s_p = \arg\max \omega_i \ \forall s_i \in S$;
    $S = S - \{s_p\}$;
  end for
  for s_j **do**
    $$\omega_j = \omega_j \cdot \left(1 - \frac{R(s_p, s_j)}{R_{\max}}\right);$$
  end for until $S = \phi$
  for each SU **do**
    $$\omega_j = \frac{\omega_j}{\sum_{s_i \in S} \omega_i};$$
  end for
while not converged **do**
$(\mathbf{U}_k, \mathbf{\Sigma}_k, \mathbf{V}_k) \leftarrow svd(\mathbf{W} \circ \mathbf{Y} - \mathbf{A}_k + \mu_k^{-1}\mathbf{G}_k)$;
  update $\mathbf{X}_{k+1} \leftarrow \mathbf{U}_k s_{\mu_k^{-1}}[\mathbf{\Sigma}_k]\mathbf{V}_k^{\mathrm{T}}$;
  update $\mathbf{A}_{k+1} \leftarrow s_{\lambda\mu_k^{-1}}[\mathbf{W} \circ (\mathbf{Y} - \mathbf{X}_{k+1}) + \mu_k^{-1}\mathbf{G}_k]$;
  update $\mathbf{G}_{k+1} \leftarrow \mathbf{G}_k + \mu_k[\mathbf{W} \circ (\mathbf{Y} - \mathbf{X}_{k+1}) - \mathbf{A}_{k+1}]$;
  update $\mu_{k+1} \leftarrow \rho\mu_k$;
  $k = k + 1$;
end while
for $n = 1, \ldots N$, $\mathbf{X}_{M \times N} \coloneqq [x_{m,n}]$ **do**
    $$Y_n = \sum_{m=1}^{M} x_{m,n} \gtrless Th;$$
end for
Return $\mathbf{W}$, $\mathbf{X}$, $\mathbf{A}$, Y_n;

Algorithm 2: Robust cooperative spectrum sensing via weighted low rank matrix recovery in CVNs (WLRMR-RCSS).

where $\circ$ denotes the element-wise multiplication of two matrices and $\mathbf{W}$ is the weighting matrix which we will introduce in the following section. To address the aforementioned issues, the problem could typically be relaxed by tractable convex optimization, and it can be efficiently solved by the proximal alternating direction method of multipliers (ADMM) [38]. rank$(\cdot)$ and l_0-norm are typically convex relaxed by the nuclear norm and l_1-norm.

$$\begin{aligned} \min_{\mathbf{X},\mathbf{A}} \quad & \|\mathbf{X}\|_* + \lambda \|\mathbf{A}\|_1 \\ \text{s.t.} \quad & \mathbf{W} \circ \mathbf{Y} = \mathbf{W} \circ \mathbf{X} + \mathbf{V} + \mathbf{A} \end{aligned} \tag{16}$$

Our model extends the classic matrix recovery model by considering the reliability of cooperative cognitive vehicles. Next we describe our proposed algorithm WLRMR-RCSS whose main steps are outlined in Algorithm 2.

3.2.1. The Weighted Matrix $\boldsymbol{W}$ Establishment

Step I (correlation-aware SU selection). First, we define the set Ω as all the vehicles in the road segment. We randomly selected s_k among the set of vehicles Ω. The set φ is defined as the set of the remaining vehicles $\Omega - \{s_k\}$. According to [36],

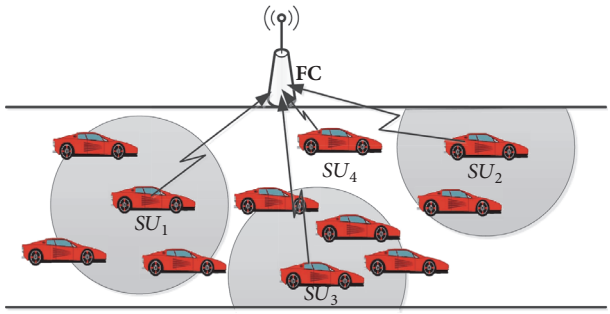


Figure 3: Example Scenario for Choosing Cooperative SUs (figure adapted from [21].).

we calculate the correlation function between s_k and the other vehicles in set φ:

$$R\left(s_k, s_q\right) = e^{-(d_{kq}/d_{corr})\cdot \ln 2} \tag{17}$$

where d_{kq} is the distance between the samples s_k and s_q and d_{corr} is the decorrelation function. We set the decorrelation function to 20 m for urban environments as in [37]. We choose vehicle s_q, which satisfies $R(s_k, s_q)$, as the maximum among the vehicles in set φ. The vehicles with a correlation function smaller than a certain threshold τ are removed from set φ. Then, s_q performs the steps presented above. This scheme is repeated until $\varphi \in \phi$. This correlation-aware SU selection scheme discards the correlated SU and selects the uncorrelated SUs among the remaining users. Finally, we denote the set of uncorrelated SUs with S. An example is shown in Figure 3. The subset S which contains SU_1, SU_2, SU_3, and SU_4 is established.

Step II (weight assignment). First, we calculate the weight ω_i of s_i in set S.

$$\omega_i = 1 - \frac{\sum_{s_i \in S} R\left(s_i, s_j\right)}{\sum_{s_p \in S} \sum_{s_j \in S} R\left(s_p, s_j\right)} \tag{18}$$

We choose s_p to satisfy $s_p = \arg\max \omega_i$. Then, we recalculate the weight of the remaining SUs using the equation $\omega_j' = \omega_j \cdot (1 - R(s_p, s_j)/R_{\max})$, where $R_{\max} = \max R(s_i, s_j)$. These steps are repeated for all s_j in the set S. Finally, we normalize the weight $\omega_j = \omega_j / \sum_{s_i \in S} \omega_i$. Now, all of the cooperative SUs are assigned weights. To establish the weighting matrix $\mathbf{W}$ of cooperative SUs, we employ location to characterize the correlation function between the SUs and then establish a weight assignment scheme to transfer to a weighting matrix $\mathbf{W}$. We divide this step into two phases to construct the weighting matrix; the weighted matrix $\mathbf{W}$ could be expressed as

$$\mathbf{W} = \begin{bmatrix} \omega_1 & \cdots & \omega_N \\ \vdots & \ldots & \vdots \\ \omega_1 & \cdots & \omega_N \end{bmatrix}_{M \times N} \tag{19}$$

3.2.2. Robust Spectrum Sensing via Weighted Low-Rank Matrix Recovery. The authors of [20] proposed robust CSS with a crowd of low-end personal spectrum sensors. This paper assumed that all sensing data (both the normal data and the nonabnormal data) would be exploited for spectrum sensing to gain full diversity. As expressed in (15), our model extends the WLRMR-CSS to dense cognitive vehicular networks by taking the effect of correlation on aggregating the samples of SUs into consideration. The weighting matrix $\mathbf{W}$ assigns smaller weights to the corrupted data matrix in the sensing data matrix $\mathbf{Y}$; the l_1-norm of the corresponding vectors in the recovered sparse matrix $\mathbf{A}$ is inclined to be small. Thus, recovering the low-rank matrix $\mathbf{X}$ from $\mathbf{Y}$ can be highlighted more effectively.

Then, we focus on recovering the low-rank matrix $\mathbf{X}$ from $\mathbf{Y}$. According to previous research [39–41], we introduce a matrix $\mathbf{G}$ of the Lagrangian multiplier; then, the solver of model (16) could instead be

$$\begin{aligned} \mathscr{L}\left(\mathbf{X}, \mathbf{A}, \mathbf{G}, \mu\right) = {} & \|\mathbf{X}\|_* + \lambda \|\mathbf{A}\|_1 \\ & + \langle \mathbf{G}, \mathbf{W} \circ (\mathbf{Y} - \mathbf{X}) - \mathbf{A} \rangle \\ & + \frac{\mu}{2} \|\mathbf{W} \circ (\mathbf{Y} - \mathbf{X}) - \mathbf{A}\|_F^2 \end{aligned} \tag{20}$$

Then, we can get the solutions as follows:

$$\begin{aligned} \mathbf{X}_{k+1} &\longleftarrow \mathbf{U}_k \mathrm{s}_{\mu_k^{-1}} \left[\mathbf{\Sigma}_k\right] \mathbf{Q}_k^{\mathrm{T}} \\ \mathbf{A}_{k+1} &\longleftarrow s_{\lambda\mu_k^{-1}} \left[\mathbf{W} \circ \left(\mathbf{Y} - \mathbf{X}_{k+1}\right) + \mu_k^{-1} \mathbf{G}_k\right] \\ \mathbf{G}_{k+1} &\longleftarrow \mathbf{G}_k + \mu_k \left[\mathbf{W} \circ \left(\mathbf{Y} - \mathbf{X}_{k+1}\right) - \mathbf{A}_{k+1}\right] \end{aligned} \tag{21}$$

where $(\mathbf{U}_k, \mathbf{\Sigma}_k, \mathbf{Q}_k) \equiv svd(\mathbf{W} \circ \mathbf{Y} - \mathbf{A}_k + \mu_k^{-1} \mathbf{G}_k)$. We obtain the real sensing data $\mathbf{X}$ based on these steps. Next, we perform spectrum sensing by data fusion.

Remark 1. The set Ω is not fixed a priori but changes with the current vehicles within the road segment. The number of selected cognitive vehicles in the WLRMR-RCSS is able to adapt different traffic densities and different network topologies.

Remark 2. The proposed WLRMR-RCSS algorithm is centralized, and the FC handles the selection. This mechanism in the WLRMR-RCSS does not require explicit coordination communications among the SUs, thus limiting the communication overhead. During the selection process, the cognitive vehicles in Ω are all equipped with GPS devices. The FC could readily collect their location information.

Remark 3. The nonzero abnormal data might be generated by either accidental equipment failure or malicious behavior. The style of malicious behaviors could contain AO, AB, AF, or random disguising as previously discussed. The sparsity of these abnormal data is random during the process of spectrum sensing.

Remark 4. To recover all sensing data (both the normal data and the nonabnormal data) is time-consuming and

complicated. In our Algorithm 2, both the normal sensing data and the nonabnormal sensing data of cooperated SUs will be separated. Meanwhile, the diversity of SUs is exploited for spectrum sensing.

Computational Complexity Analysis. The proposed WLRMR-RCSS algorithm chooses M noncorrelated vehicles with lower correlation coefficients and higher sensing reliability out of the total SUs. In this part, it needs $O(M^2)$ computational complexity. On the other hand, the reporting overhead will decline vastly without an obvious loss of performance with the SUs selection. For the part of robust spectrum sensing via weighted low-rank matrix recovery, its computational complexity is $O(MN\min(M,N))$. On the other hand, the WLRMR-RCSS algorithm has a worst-case complexity result of $O(k^{-2})$, as is the case in LRMR-RCSS algorithm. The computational cost of the WLRMR-RCSS algorithm is not as high as [20] after the correlation-aware SUs selection step in our algorithm. Thus, our algorithm is efficient. BP-CSS in [15] must calculate the k iterations of the exchange of information between vehicles, and its computational cost is $O(M^k)$. The overhead of the Blind-CSS [42] is mainly from the transmissions made by all vehicles performing sensing of spectrum availability to all nearby RSUs. In ADMM-CSS [20], matrix $\mathbf{Y}$ is all of the spectrum sensing data of the SUs. As such, its computational complexity is more than that of our WLRMR-RCSS algorithm.

4. Performance Evaluation

Considering the actual vehicular environment, we analyze our algorithm in low and high traffic density environment scenarios. Our proposed algorithm simulation environment is shown in Figure 4. All of the mobility models in our simulations are generated using the software VISSIM [43]. We now evaluate our proposed schemes by comparing the ADMM-CSS algorithm [20], the BP-CSS algorithms in [15] (suitable for low traffic density), and the Blind-CSS algorithm [42] (suitable for high traffic density), as these schemes are all designed for robust cooperative spectrum sensing.

4.1. Performance Analysis and Comparison

Case I (low traffic density environment). To investigate our algorithm in a low traffic density environment, we consider a cognitive vehicular network on a highway, as shown in Figure 5. Detailed parameters are given in Table 2. We simulated 1000 m of a freeway. A primary transmitter is assumed in the middle, and crowd vehicles are randomly distributed. The Propagation Model computes the power received as in [10]. The rate of SUs that contribute abnormal data in all cooperated SUs is defined as R_{mal}. The ρ_{vel} is the traffic density, which means the number of vehicles per meter per lane (veh/m/l).

Figure 6 focuses on the influence of R_{mal}. A higher value of R_{mal} indicates a higher scale of corrupted data. In this figure, although the sensing performance worsens with an increasing fraction of SUs that introduce corrupted data, our proposed LRMR-RCSS algorithm could achieve satisfactory performance in the case of a high number of malicious SUs.

As shown in Figure 7, to evaluate the performance of the proposed algorithm, we plot the complementary receiver operating characteristic (ROC) curve when $R_{mal} = 0.1$. The simulation results in Figure 7(a) show that our proposed LRMR-RCSS algorithm has good performance in sparse traffic flow ($\rho_{vel} = 0.05$). We find that LRMR-RCSS and WLRMR-RCSS algorithms both outperform the trust based among neighboring vehicles in BP-CSS, whether in a sparse

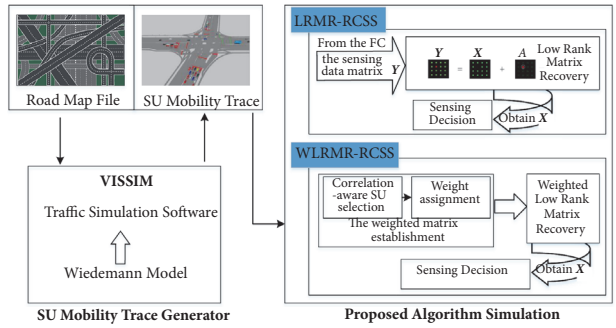


Figure 4: Our proposed algorithm simulation environment.

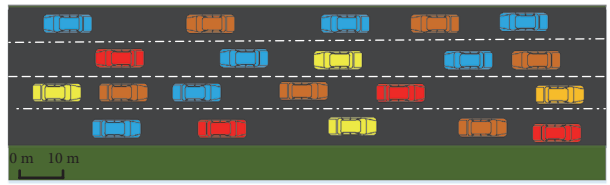


Figure 5: A cognitive vehicular network on a highway.

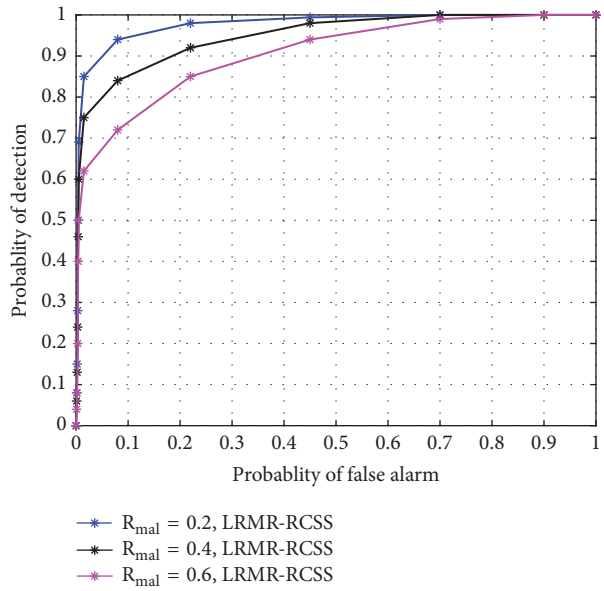


Figure 6: Sensing performance of various schemes under various abnormal data rates R_{mal} for LRMR-RCSS [21].

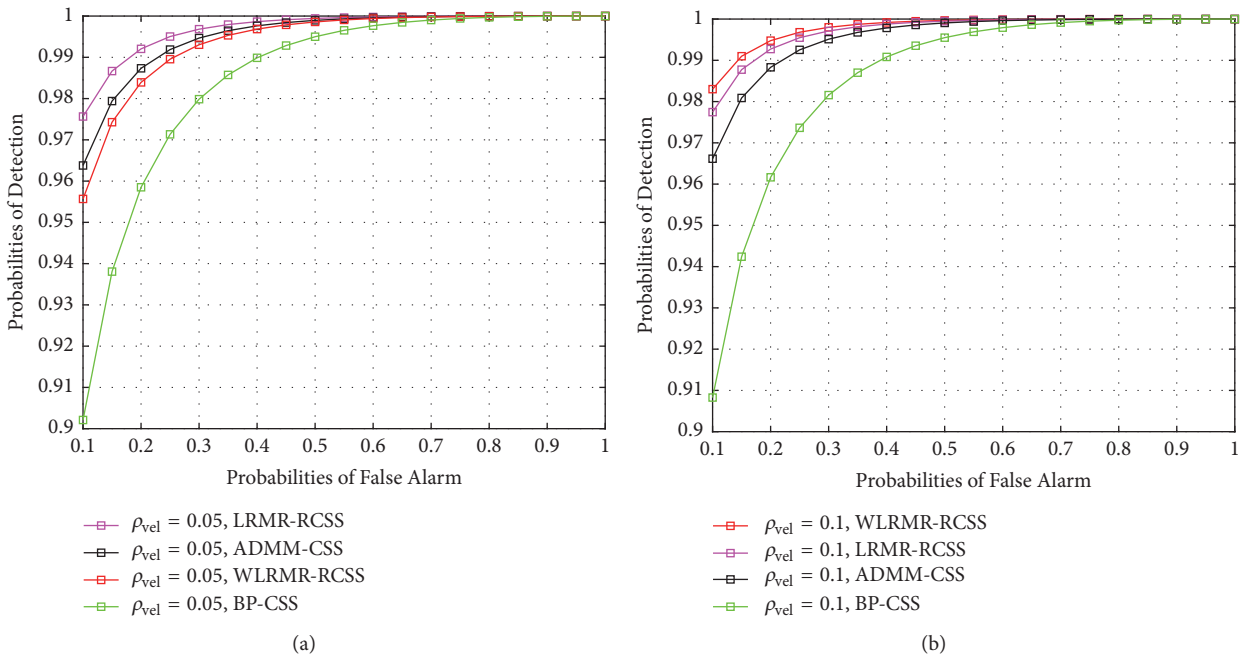


Figure 7: Comparison of the proposed LRMR-RCSS and WLRMR-RCSS algorithms with BP-CSS and ADMM-CSS algorithms at different traffic densities ρ_{vel}.

Table 2: Simulation parameters.

Parameter	Value
Road length (Highway)	1000 m
Road length	W-E: 1000 m
(Road intersection in Urban)	N-S: 800 m
Lanes (Highway)	4-lanes
Lanes (Road intersection in Urban)	4-lanes
Traffic light timing	cycle = 100 s
(Road intersection in Urban)	red = 50 s, green = 50 s
Traffic flow (Highway)	0-3000 veh/h
Traffic flow	NS-SS: 0-1800 veh/h
(Road intersection in Urban)	ES-WS: 0-2700 veh/h
Speed limit (Highway)	50 m/s (180 km/h)
Speed limit (Urban)	20 m/s (72 km/h)
SU mobility model	Wiedemann model [23]
Number of subbands N	20
Bandwidth of each subband BW	200 kHz
Single/noise power	27dBm/-110dBm
N_{sam}	100
Sample time	0.1ms
The path-loss exponent	2-6
shadowing dB-spread	2-20 dB
Simulation step for VISSIM	0.1s

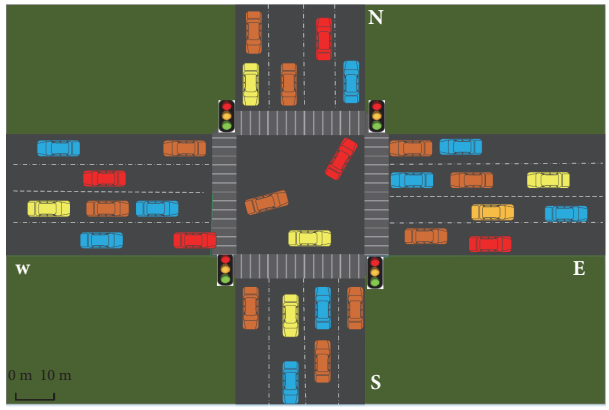


Figure 8: A cognitive vehicular network at a road intersection in an urban environment.

or a moderate traffic flow environment. The traditional trust based cooperative spectrum sensing in cognitive vehicular networks is unable to determine the style of malicious SU behavior. For example, the malicious SUs may be considered trustworthy when PU appears as if its form is AB attack. The inaccuracy due to inaccurate spectrum sensing data introduced by malicious SUs reduces the precision in BP-CSS. From sparse to moderate, with an increase in the number of cooperative SUs, the performances of the three algorithms all increase due to the diversity effect of the cooperative SUs. The simulation results in Figure 7(b) show that our proposed WLRMR-RCSS algorithm could effectively eliminate the unreliable data component from the corrupted sensing data in moderate traffic densities.

Case II (high traffic density environment). To investigate our algorithm in a high traffic density environment, we consider a cognitive vehicular network at a road intersection with traffic lights in an urban area, as described in Figure 8. All vehicles

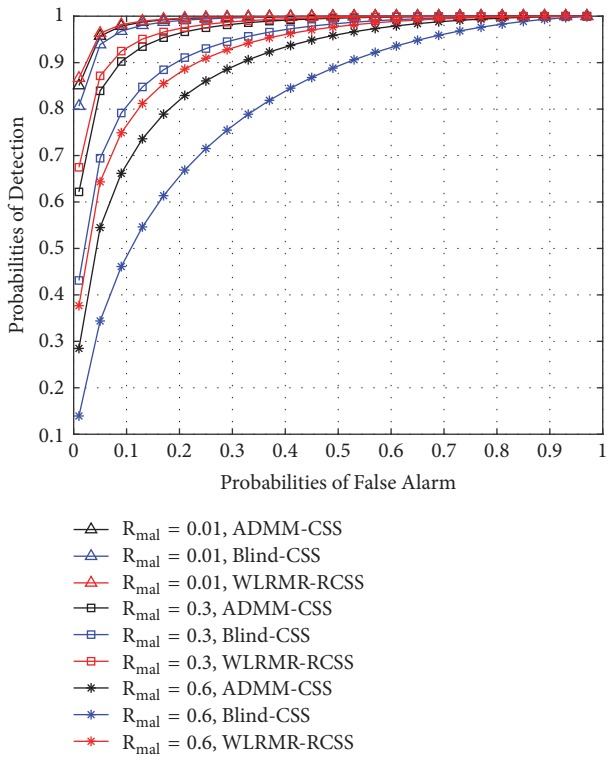


Figure 9: Comparison of the proposed WLRMR-RCSS algorithm with Blind-CSS and ADMM-CSS algorithms with different R_{mal} values.

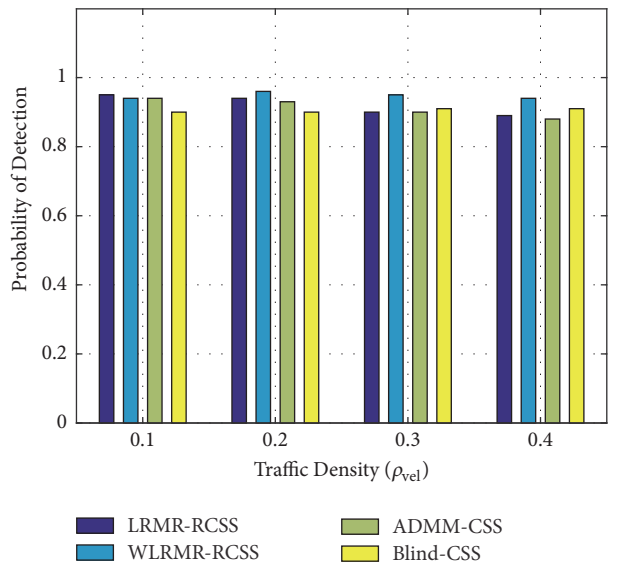


Figure 10: Comparison of the proposed LRMR-RCSS and WLRMR-RCSS algorithms with Blind-CSS and ADMM-CSS algorithms at different traffic densities.

could repeatedly move from one end to the other three ends. For example, among the vehicles departing from the left end, vehicles in the middle lane will turn left (toward the top end) at the intersection and vehicles in the right lane will go straight (toward the right end) at the intersection. The dense vehicle traffic at the road intersection in the urban area obeys the Wiedemann model generated by VISSIM.

As shown in Figure 9, our proposed WLRMR-RCSS algorithm has high performance in accordance with the ADMM-CSS algorithm when the value R_{mal} is small. The Blind-CSS algorithm for vehicular networks is to be used for sharing with the surrounding vehicles. The choice of vehicles to perform the sensing operation is determined by vehicle speed. The Blind-CSS algorithm also has good performance because the SUs received few abnormal data. With the increase of the rate of abnormal data in all cooperating SUs sensing data, our algorithm is better than the ADMM-CSS algorithm because the weighting matrix in our algorithm assigns smaller weights to the corrupted data matrix in the sensing data matrix; then the corresponding vectors in the recovered real data matrix are inclined to be small. Our recovery of the real data matrix from the corrupted data matrix becomes more effective. The experimental results show that our WLRMR-RCSS algorithm is effective along with an increase in R_{mal}. The performance of the traditional blind cooperative sensing scheme as in Blind-CSS in CVNs would be influenced significantly.

Figure 10 presents the performances of the four spectrum sensing algorithms as a function of the vehicle density at a road intersection in an urban environment. The traffic density is set to 0.1, 0.2, 0.3, and 0.4 veh/m/l, denoting moderate, high, very high, and severe congestion traffic conditions, respectively. After a period of observation, it shows that the performance of our proposed WLRMR-RCSS algorithm remains stable under different traffic conditions. Our proposed WLRMR-RCSS algorithm outperforms the algorithms Blind-CSS and ADMM-CSS in the dense traffic environment. It is observed that our proposed LRMR-RCSS algorithm is more suitable for sparse or even moderate traffic conditions. The performance of our proposed WLRMR-RCSS algorithm increases slightly from moderate traffic conditions to high traffic conditions. The improved SU diversity introduces this slight increase because of the increased number of cooperative vehicles. Of course, the diversity would not continually increase. This fact has been verified under the senior traffic condition, as the detection probability is not higher. When traffic is congested, our proposed algorithm is not affected. In such a scenario, the detection performance of ADMM-CSS algorithms would be reduced due to the increase of SUs. This indicates that our proposed WLRMR-RCSS algorithm is appropriate for dense vehicular environments.

According to Figure 11, we record the number of the selected cooperative SUs for WLRMR-RCSS at different traffic densities during our simulation process. We find that the number varies. This indicates that the proposed WLRMR-RCSS algorithm can adapt to various traffic densities as the number of cooperative users in the dense vehicular environment is not fixed but rather is altered according to the spatial distribution of vehicles. The number of selected cooperative SUs is not high in the high

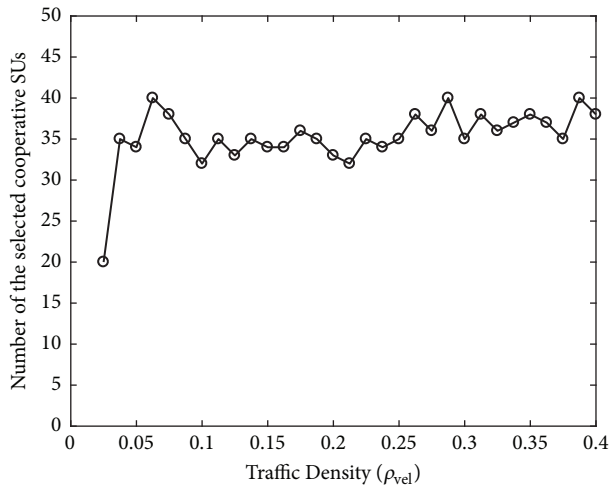


Figure 11: Number of the selected cooperative SUs for WLRMR-RCSS at different traffic densities.

traffic density environment. That means that the selection of cooperative SUs in the WLRMR-RCSS algorithm could reduce the overhead in dense cognitive vehicular networks.

5. Conclusions

This work investigates the issue of robust and effective cooperative spectrum sensing in cognitive vehicular networks. We establish a robust spectrum sensing algorithm, LRMR-RCSS, to eliminate the negative impact of corrupted sensing data. In addition, we extend our robust cooperative spectrum sensing algorithm WLRMR-RCSS while utilizing cooperative diversity into dense CVNs. In the WLRMR-RCSS algorithm, we introduce a correlation-aware SU selection and weight assignment scheme to reduce the overhead of cooperative vehicles. The WLRMR-RCSS algorithm has realized cooperative SU diversity, and the historical information on vehicle reputation is not needed. Simulation results demonstrate that the proposed robust sensing WLRMR-RCSS algorithm can achieve stable and competitive performance. The complexity of WLRMR-RCSS is not high. In practice, the cognitive vehicles are often caught in traffic jams due to road accidents or morning and evening peak traffic times. Our proposed WLRMR-RCSS algorithm could specifically be applied to dense traffic environments. These algorithms are performed by the vehicles which allows to discover white channels accurately. As a consequence, a greater number of vehicles are allowed to communicate safety and nonsafety information, which can prove diversified applications in areas that normally experience heavy traffic.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

This paper was presented in part at the IEEE/CIC International Conference on Communications in China, Qingdao, China, Oct. 22-24, 2017. This is an extended version.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Chinese National Nature Science Foundation under Grants 61571062 and 61271177.

References

[1] World Health Statistics, World Health Organizaton, 2016.

[2] "IEEE standard for wireless access in vehicular environments (WAVE)—multi-channel operation," *IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2010)*, pp. 1–206, 2016.

[3] C. Campolo and A. Molinaro, "Multichannel communications in vehicular Ad Hoc networks: a survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 158–169, 2013.

[4] X. Yin, X. Ma, K. S. Trivedi, and A. Vinel, "Performance and reliability evaluation of BSM broadcasting in DSRC with multi-channel schemes," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 63, no. 12, pp. 3101–3113, 2014.

[5] K. Xiong, X. Chen, L. Rao, X. Liu, and Y. Yao, "Solving the performance puzzle of DSRC multi-channel operations," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 3843–3848, June 2015.

[6] X. Ma, J. Zhang, X. Yin, and K. S. Trivedi, "Design and analysis of a robust broadcast scheme for VANET safety-related services," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 46–61, 2012.

[7] Z. Wang and M. Hassan, "How much of dsrc is available for non-safety use?" in *Proceedings of the 5th ACM International Workshop on VehiculAr Inter-NETworking (VANET '08)*, pp. 23–29, ACM, New York, NY, USA, September 2008.

[8] S. Mumtaz, K. M. S. Huq, M. I. Ashraf, J. Rodriguez, V. Monteiro, and C. Politis, "Cognitive vehicular communication for 5G," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 109–116, 2015.

[9] K. D. Singh, P. Rawat, and J.-M. Bonnin, "Cognitive radio for vehicular ad hoc networks (CR-VANETs): approaches and challenges," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, article 49, 2014.

[10] M. di Felice, K. R. Chowdhury, and L. Bononi, "Cooperative spectrum management in cognitive vehicular Ad Hoc networks," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '11)*, pp. 47–54, November 2011.

[11] A. J. Ghandour, K. Fawaz, H. Artail, M. Di Felice, and L. Bononi, "Improving vehicular safety message delivery through the implementation of a cognitive vehicular network," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2408–2422, 2013.

[12] X. Y. Wang and P.-H. Ho, "A novel sensing coordination framework for CR-VANETs," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1936–1948, 2010.

[13] H. Kremo, O. Altintas, H. Tanaka, M. Kitamura, K. Inage, and T. Fujii, "Cooperative spectrum sensing in the vehicular environment: an experimental evaluation," in *Proceedings of the 2014 IEEE Vehicular Technology Conference (VTC 2014-Spring)*, pp. 1–5, Seoul, South Korea, May 2014.

[14] M. Di Felice, A. J. Ghandhour, H. Artail, and L. Bononi, "Integrating spectrum database and cooperative sensing for cognitive vehicular networks," in *Proceedings of the 2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, pp. 1–7, Las Vegas, NV, USA, September 2013.

[15] H. Li and D. K. Irick, "Collaborative spectrum sensing in cognitive radio vehicular ad hoc networks: belief propagation on highway," in *Proceedings of the IEEE 71st Vehicular Technology Conference (VTC '10)*, pp. 1–5, Taipei, Taiwan, May 2010.

[16] B. Aygun and A. M. Wyglinski, "A voting-based distributed cooperative spectrum sensing strategy for connected vehicles," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5109–5121, 2017.

[17] C. Chembe, R. M. Noor, I. Ahmedy, M. Oche, D. Kunda, and C. H. Liu, "Spectrum sensing in cognitive vehicular network: State-of-Art, challenges and open issues," *Computer Communications*, vol. 97, pp. 15–30, 2017.

[18] Z. Wei, F. R. Yu, and A. Boukerche, "Cooperative spectrum sensing with trust assistance for cognitive radio vehicular ad hoc networks," in *Proceedings of the 5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, DIVANet 2015*, pp. 27–33, November 2015.

[19] Z. Wei, F. R. Yu, H. Tang, C. Liang, and Q. Yan, "Securing cognitive radio vehicular Ad hoc networks with trusted lightweight cloud computing," in *Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 450–456, Philadelphia, PA, USA, October 2016.

[20] G. Ding, J. Wang, Q. Wu et al., "Robust spectrum sensing with crowd sensors," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3129–3143, 2014.

[21] X. Liu, Z. Zeng, and C. Guo, "Robust cooperative spectrum sensing in dense cognitive vehicular networks," in *Proceedings of the 2017 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–6, October 2017.

[22] Y. Al-Mathehaji, S. Boussakta, M. Johnston, and H. Fakhrey, "Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks," *IEEE Sensors Letters*, vol. 1, no. 4, pp. 1–4, 2017.

[23] P. T. Fishburn, J. Golkar, and K. M. Taaffe, "Simulation of transportation systems," in *Proceedings of the 1995 Winter Simulation Conference, WSC'95*, pp. 51–54, December 1995.

[24] M. Lpezbenłtez and F. Casadevall, "Spectrum usage models for the analysis, design and simulation of cognitive radio networks," *Lecture Notes in Computer Science*, vol. 62, no. 5, pp. 2091–2104, 2012.

[25] R. k Lindquist, "FCC spectrum policy task force reports on progress, initiatives," in *Proceedings of the QST*, vol. 76, p. 76, 2004.

[26] S. Pagadarai, A. M. Wyglinski, and R. Vuyyuru, "Characterization of vacant UHF TV channels for vehicular dynamic spectrum access," in *Proceedings of the 2009 IEEE Vehicular Networking Conference, VNC 2009*, October 2009.

[27] W. Lee and D. Cho, "Concurrent spectrum sensing and data transmission scheme in a CR system," in *Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1326–1330, Paris, France, April 2012.

[28] Y. Pei, Y. Liang, K. C. Teh, and K. H. Li, "Energy-efficient design of sequential channel sensing in cognitive radio networks: optimal sensing strategy, power allocation, and sensing order," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 8, pp. 1648–1659, 2011.

[29] S. Chaudhari, J. Lunden, V. Koivunen, and H. V. Poor, "Cooperative sensing with imperfect reporting channels: hard decisions or soft decisions?" *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 18–28, 2012.

[30] X. Liu, Z. Zeng, C. Guo, and S. Zhu, "Performance analysis of spatial-temporal spectrum sensing for cognitive vehicular network," in *Proceedings of the the 3rd ACM Workshop*, pp. 1–6, Paderborn, Germany, July 2016.

[31] Y. Zhao, P. Paul, C. Xin, and M. Song, "Performance analysis of spectrum sensing with mobile SUs in cognitive radio networks," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 2761–2766, aus, June 2014.

[32] L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending against byzantine attack in cooperative spectrum sensing: defense reference and performance analysis," *IEEE Access*, vol. 4, pp. 4011–4024, 2016.

[33] A. Vosoughi, J. R. Cavallaro, and A. Marshall, "Trust-aware consensus-inspired distributed cooperative spectrum sensing for cognitive radio Ad Hoc networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 1, pp. 24–37, 2016.

[34] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[35] Z. Tian and G. B. Giannakis, "Compressed sensing for wideband cognitive radios," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '07)*, pp. IV1357–IV1360, Honolulu, Hawaii, USA, April 2007.

[36] Y. Wang, Z. Tian, and C. Feng, "Collecting detection diversity and complexity gains in cooperative spectrum sensing," *IEEE Transactions on Wireless Communications*, vol. 11, no. 8, pp. 2876–2883, 2012.

[37] Z. Qin, Y. Gao, and M. D. Plumbley, "Malicious user detection based on low-rank matrix completion in wideband spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 66, no. 1, pp. 5–17, 2018.

[38] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends in Machine Learning*, vol. 3, no. 1, pp. 1–122, 2010.

[39] Z. Zhang, A. Ganesh, X. Liang, and Y. Ma, "TILT: transform invariant low-rank textures," *International Journal of Computer Vision*, vol. 99, no. 1, pp. 1–24, 2012.

[40] X. Ren and Z. Lin, "Linearized alternating direction method with adaptive penalty and warm starts for fast solving transform invariant low-rank textures," *International Journal of Computer Vision*, vol. 104, no. 1, pp. 1–14, 2013.

[41] C. Tang, P. Wang, C. Zhang, and W. Li, "Salient object detection via weighted low rank matrix recovery," *IEEE Signal Processing Letters*, vol. 24, no. 4, pp. 1–5, 2017.

[42] K. Baraka, L. Safatly, H. Artail, A. Ghandour, and A. El-Hajj, "An infrastructure-aided cooperative spectrum sensing scheme for vehicular ad hoc networks," *Ad Hoc Networks*, vol. 25, pp. 197–212, 2015.

[43] VISSIM, http://vision-traffic.ptvgroup.com/en-us/products/ptv-vissim/.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8509693, 16 pages
https://doi.org/10.1155/2018/8509693

Research Article

Performance Analysis of RF-Powered Cognitive Radio Networks with Integrated Ambient Backscatter Communications

Longteng Xu,[1] **Kun Zhu**,[1] **Ran Wang**,[1] **and Shimin Gong**[2]

[1]*Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[2]*Shenzhen Institutes of Advanced Technology, Shenzhen, China*

Correspondence should be addressed to Kun Zhu; zhukun@nuaa.edu.cn

Received 24 November 2017; Accepted 11 February 2018; Published 2 April 2018

Academic Editor: Hina Tabassum

Integrating ambient backscatter communications into RF-powered cognitive radio networks has been shown to be a promising method for achieving energy and spectrum efficient communications, which is very attractive for low-power or no-power communications. In such scenarios, a secondary user (SU) can operate in either transmission mode or backscatter mode. Specifically, an SU can directly transmit data if sufficient energy has been harvested (i.e., transmission mode). Or an SU can backscatter ambient signals to transmit data (i.e., backscatter mode). In this paper, we investigate the performance of such systems. Specifically, channel inversion power control and an energy store-and-reuse mechanism for secondary users are adopted for efficient use of harvested energy. We apply stochastic geometry to analyze coverage probability and achievable rates for both primary and secondary users considering both communication modes. Analytical tractable expressions are obtained. Extensive simulations are performed and the numerical results show the validity of our analysis. Furthermore, the results indicate that the performance of secondary systems can be improved with the integration of both communication modes with only limited impact on the performance of primary systems.

1. Introduction

In recent years, the demand for smart systems (e.g., on-body sensing for e-Healthy) is growing fast. For such systems, the deployed sensors usually need to work continuously and transmit collected data for upper layer applications. Since most sensors have limited battery and limited spectrum resources, energy-efficient and spectrum efficient wireless communications are required.

Several techniques have been developed for achieving low-power or even no-power communications in a spectrum efficient manner, among which ambient backscatter communications and radio-frequency (RF) powered cognitive communications are two remarkable ones. In [1], authors investigate practical backscatter for on-body sensors by using the signals from Wi-Fi or Bluetooth. Such a backscatter system based on Wi-Fi is referred to as Wi-Fi backscatter [2]. Be different from RF identification (RFID) which needs a dedicated signal emitter (RFID reader) [3], Wi-Fi backscatter does not need dedicated reader. However, it does not perform well in outdoor environment. While ambient backscatter communication [4] is also a type of passive communication which utilizes ambient RF signals (e.g., TV signals) to transmit data, no dedicated signal source is required, which makes no-power wireless communications possible. However, the communications are vulnerable since backscattered signals are usually weak and volatile.

Another technique, harvesting energy from ambient RF signals, has been proposed to support energy-efficient communications [5–7]. Besides, RF-powered cognitive radio network (CRN) offers a method to utilize primary transmitter (PTs) signals as the energy source for secondary transmitters (STs). A main problem is that the transmission opportunities of RF-powered STs are limited by the harvested energy and channel availability.

In this work, we consider the integration of ambient backscatter communications into RF-powered cognitive radio networks in a similar way to [8]. In this case, these two techniques could complement each other to jointly achieve the

advantages while overcoming the individual shortcomings. Specifically, in such scenarios, the secondary transmitters can operate in two modes, that is, transmission mode and backscatter mode. In transmission mode, an ST can directly transmit data to its receiver if sufficient energy has been harvested and the channel is available. When the channel is busy, an ST can switch to backscatter mode which backscatters the ambient signals to transmit its own data.

In other words, in our cognitive radio network, the transmission of secondary transmitters falls into interweave paradigm to utilize white spaces of specific channels [9], and the needed energy is harvested from existing signals. As for backscatter communication, in some extent it falls into overlay paradigm since the backscattered signals from secondary transmitters to primary receivers can be ignored which will be stated in more detail in the following [9–11]. As for the primary user activity model, which has a vital influence on cognitive users' performance, that is, directly determining spectrum access time of cognitive users, in this paper follows a simplified ON/OFF model [12] wherein total active (ON) duration and inactive (OFF) duration of a primary user are fixed. Besides, the details of spectrum sensing are omitted in this paper. Other complex and widely used primary user activity models and spectrum analysis can be found in [12–15].

Note that several existing works have been done for the integration of backscatter communications with cognitive radio networks or cellular networks. In [16], authors give an overview of backscatter assisted wireless powered communications and introduce a multiple access scheme in cognitive radio networks. The tradeoff analysis in RF-powered backscatter CRNs is provided in [17]. However, only one single cell is considered and no performance analysis is provided. In [18], the integration of backscatter communications with heterogeneous cellular networks is proposed and analyzed. In [19], a backscatter network is analyzed by using stochastic geometry, but dedicated power beacons are deployed to support the communication, while, in [20, 21], a single hybrid transmitter harvests energy from multiple ambient transmitters, transmits its own signal, or backscatters existing signals to a hybrid receiver, and its performance is analyzed.

In this paper, we investigate the performance of ambient backscatter communications in RF-powered cognitive radio network. Specifically, we propose an analytical framework based on stochastic geometry [22–24], with which the tractable expressions for coverage probability and achievable rates for both primary and secondary users considering both communication modes are obtained. We perform extensive simulations and the numerical results demonstrate the validity of the theoretical analysis. Also, the results indicate that secondary systems can achieve improved performance while having only limited impact on the primary systems, which show the effectiveness of integration.

The rest of the paper is organized as follows: Section 2 presents the comprehensive system model. Section 3 presents channel inversion power control and energy storage and reusing. Analytical expressions are given in Section 4. In Section 5, numerical results from analysis and simulations are described. Finally, Section 6 draws the conclusions.

2. System Model

2.1. Network Model. We consider a cognitive cellular network in which macro base stations (MBSs, i.e., PTs, Y) serve primary cellular users (PRs, U) in the downlink while overlaid by cognitive secondary users. Each PR will connect to the nearest MBS. Besides, there are secondary transmitters (STs, X) equipped with energy storage and secondary receivers (SRs, Z). An ST can communicate with an SR by either backscattering signals or emitting its own signals. Since backscattered signal is weak, the distance from backscattering node (i.e., ST) to receiving node (i.e., SR) is limited. It is shown in [4] that, for achieving 1 kbps information rate in outdoor environment, 2.5 feet is the maximum distance. Therefore, in this paper, for ease of analysis, we assume that an SR is at a constant small distance d to its associated ST in an isotropic direction [19].

MBSs and PRs are modeled by homogeneous Poisson point processes (HPPP) Φ and $\widetilde{\Phi}_U$ with intensities λ and $\widetilde{\lambda}_U$, respectively. STs are uniformly distributed in annular regions with radii R_m and R_M centered at each MBS. Each ST can be loosely seen as a result of random and independent displacement of the MBS. In each annular region, the number of STs is $N_{\mathrm{ST}} \sim \pi(\Lambda)$, where $\pi(\Lambda)$ is the Poisson distribution with parameter Λ. The distribution model of STs then is similar to a Matern cluster process where Φ is the parent process [25]. An inner radius $R_m > 0$ of the annular region is considered for avoiding singularity of integral in the derivation process and the outer radius R_M is related to *circuit power constraint* described in the following part.

We assume each PR is associated with its nearest MBS. The probability density function (pdf) of distance r from a PR to its nearest MBS is [23]

$$f(r) = 2\pi\lambda r e^{-\pi\lambda r^2}. \tag{1}$$

If a point is uniformly distributed within a circle with radius R and r is the distance to the center, the pdf of r is $f_o(r) = 2r/R^2$ [26]. By using conditional probability, we can get the pdf of distance r from an ST to its MBS as

$$\begin{aligned} F\left(R \mid r \geq R_m\right) &= \frac{P\left(R_m \leq r \leq R\right)}{P\left(r \geq R_m\right)} = \frac{R^2 - R_m^2}{R_M^2 - R_m^2}, \\ f_{\geq R_m}(r) &\triangleq f\left(r \mid r \geq R_m\right) = \frac{\mathrm{d}F\left(R \mid r \geq R_m^2\right)}{\mathrm{d}r} \\ &= \frac{2r}{R_M^2 - R_m^2}. \end{aligned} \tag{2}$$

Without loss of generality, according to Slivnyak's theorem [27], we analyze a typical PR (U_0) and a typical SR (Z_0) located at the origin. The typical SR's corresponding ST and MBS are also similarly typical ST (X_0) and typical MBS (Y_0), respectively. Figure 1 illustrates randomly generated positions of MBSs, PRs, and STs. Figure 2 shows the system model.

2.2. Channel Model. All MBSs share the same available channel set $\mathbf{C} = \{c_1, c_2, \ldots, c_{|\mathbf{C}|}\}$, where $|\mathbf{C}| = N_{\mathrm{ch}}$ is the number of channels. We assume $\widetilde{\lambda}_U \gg \lambda$ and there is one and only

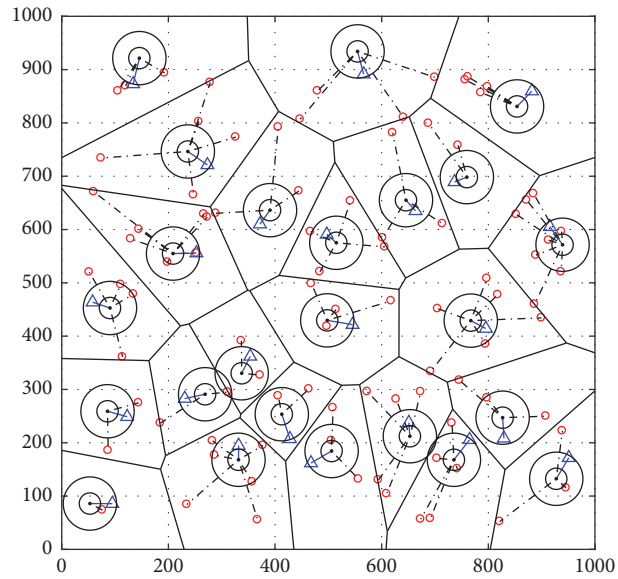


FIGURE 1: Network composition illustration. Centers of dual-circles (annular regions), red dots, and blue triangles represent MBSs, primary receivers, and secondary transmitters, respectively. To ensure visibility, only one ST is showed in an annular region and all SRs are omitted. (Radii of annular regions in the illustration are enlarged.)

one active PR in each channel of a cell, so active PRs in a generic channel form an HPPP Φ_U with intensity $\lambda_U = \lambda$ by independent thinning.

We also assume that STs in each cell have equal probabilities to access a channel when it is idle, and no two STs share the same channel. However, STs in different cells may not have equal probabilities since numbers of STs in different cells may differ from each other. This means the thinned processes are not HPPPs. But for ease of analysis, in this paper, similar to the assumptions in [6, 28–30], we assume STs in different cells in a generic channel constitute an HPPP by random displacement and thinning.

Besides, if there are N_{ST} STs in one annular region, the probability that a channel in $\mathbf{C}$ is used by an ST is $N_{\mathrm{ST}}/N_{\mathrm{ch}}$, while if $N_{\mathrm{ST}} > N_{\mathrm{ch}}$, the probability is 1. Since $N_{\mathrm{ST}} \sim \pi(\Lambda)$, the probability that a channel is used averaged over N_{ST} is

$$p_{\mathrm{ch}} = \sum_{k=0}^{N_{\mathrm{ch}}} \mathbb{P}\left[N_{\mathrm{ST}} = k\right] \frac{k}{N_{\mathrm{ch}}} + \sum_{k=N_{\mathrm{ch}}+1}^{\infty} \mathbb{P}\left[N_{\mathrm{ST}} = k\right] \cdot 1 = 1 + \frac{(\Lambda - N_{\mathrm{ch}})\,\Gamma\left(N_{\mathrm{ch}}, \Lambda\right) - e^{-\Lambda}\Lambda^{N_{\mathrm{ch}}}}{\Gamma\left(1 + N_{\mathrm{ch}}\right)}, \tag{3}$$

where $\Gamma(z) = \int_0^{\infty} t^{z-1}e^{-t}\mathrm{d}t$ is the Gamma function and $\Gamma(z,a) = \int_a^{\infty} t^{z-1}e^{-t}\mathrm{d}t$ is the upper incomplete Gamma function. So STs in a generic channel form an HPPP Φ_{ST} with intensity $\lambda_{\mathrm{ST}} = p_{\mathrm{ch}}\lambda$ by independent thinning and random displacement. And p_{ch} is termed *channel in use probability*.

An extreme case is that Λ is high enough and $p_{\mathrm{ch}} = 1$ holds. This equals the setting that only one channel is considered in the network and channels of all cells are used. In this case, besides p_{ch}, other details of the network remain unchanged, so does the analysis.

We assume that each channel experiences a constant noise power W and exponential path-loss $\ell(r) = r^{-\alpha}$ (or $\ell(X-Y) = \|X-Y\|^{-\alpha}$) with a uniform exponent $\alpha > 2$, where r is a distance, $X, Y \in \mathbb{R}$ are two points, and $\|\cdot\|$ is the Euclidean norm. Independent Rayleigh fading is considered which remains constant within one time slot. The fading from a PR/ST to its corresponding MBS is $h \sim \exp(\mu_h)$, fading from an ST to its SR is $q \sim \exp(\mu_q)$, and interference fading from an MBS/PR/ST to a PR/SR is $g \sim \exp(\mu_g)$. Moreover, for convenience we set a time slot duration to be a unit time.

2.3. Communication Model. When an MBS serves a PR, it may turn into busy or idle mode during each time slot. We further divide each time slot into M minislots [19] and all minislots are synchronized among MBSs. In addition, we assume that each MBS randomly and independently turns into idle mode in one of the minislots. With such assumptions, when the MBS is transmitting, we consider that an ST performs energy harvesting (EH) and ambient backscatter communication (BC) in D_E and D_B minislots, respectively, and we have $D_E + D_B + 1 = M$. Minislots for EH and BC of each ST are also randomly and independently selected with equal probability. Besides, the ST performs traditional information transmission (IT) using the harvested energy when the MBS is idle. In the following, these two communication modes are termed BC mode and IT mode, respectively. An example of minislots assignment and selection when $M = 7$ is given in Figure 3.

In a generic minislot, STs performing energy harvesting form an HPPP Φ_{eh} with intensity $\lambda_{\mathrm{eh}} = (D_E/M)\lambda_{\mathrm{ST}}$, which can be seen as the thinning of Φ_{ST} since each ST may work in EH mode within a minislot with probability D_E/M. Similarly, STs in BC mode and IT mode form HPPPs Φ_{bc} and $\widetilde{\Phi}_{\mathrm{it}}$ with intensities $\lambda_{\mathrm{bc}} = (D_B/M)\lambda_{\mathrm{ST}}$ and $\widetilde{\lambda}_{\mathrm{it}} = \lambda_{\mathrm{ST}}/M$, respectively. Moreover, MBSs in busy mode also form an HPPP Φ_{bs} with intensity $\lambda_{\mathrm{bs}} = (1 - 1/M)\lambda$.

We further assume that the SR knows about its ST's work mode so as to perform corresponding decoding. Saturation condition is also assumed where a data packet is always ready for transmission.

Besides, we assume that when an ST performs BC, a portion β of the received power is used for BC, and the backscatter efficiency is η_b. So the backscatter power of a generic ST is

$$P_{\mathrm{bc}} = \beta\eta_b \|X - Y\|^{-\alpha} h, \tag{4}$$

where $\|X - Y\|$ is the distance from the MBS to the ST, while the remaining portion $1-\beta$ is stored as energy [19] along with received power in EH mode. And the conversion efficiency is η. In this case, the harvested energy within a time slot is

$$E_H = \eta\left(\frac{D_E}{M} + (1-\beta)\frac{D_B}{M}\right) r^{-\alpha} h = \frac{D_{\mathrm{eb}} h}{M r^{\alpha}}, \tag{5}$$

where $D_{\mathrm{eb}} = \eta(D_E + (1-\beta)D_B)$.

In order to perform IT, an ST must satisfy the circuit power constraint that E_H is more than that consumed E_C by

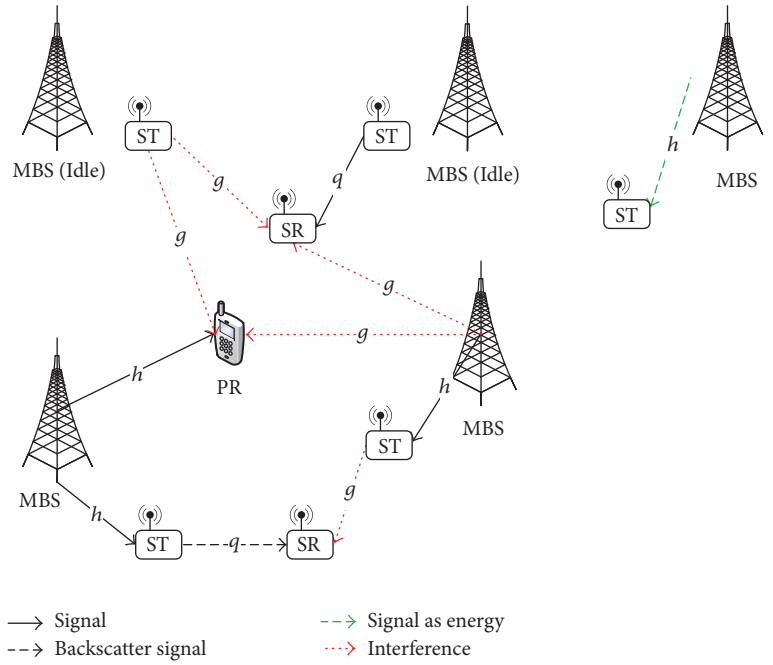


Figure 2: System model of our network. h, g, q refer to three types of fading described in Section 2.2.

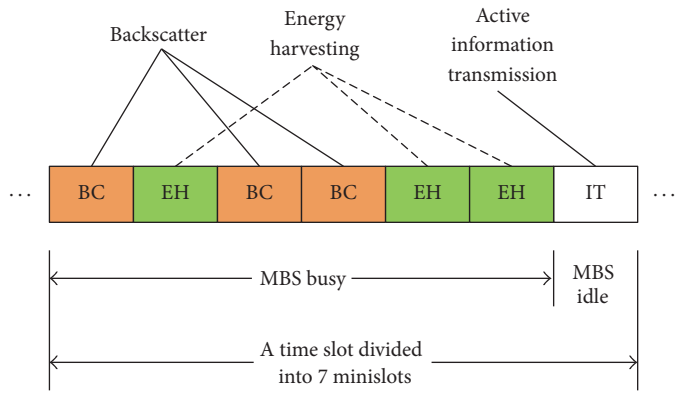


Figure 3: An example of minislots assignment and selection for different mode when number of minislots is 7.

the circuit, while the remaining power $E_H - E_C$ is used for data transmission. Since a time slot lasts a unit time, we will also describe E_H and E_C as the power. The average harvested energy can be obtained as

$$\mathbf{E}_h\left[E_H\right] = \int_0^\infty \mu_h e^{-\mu_h h} \frac{D_{\text{eb}} h}{M r^\alpha} \mathrm{d}h = \frac{D_{\text{eb}}}{\mu_h M r^\alpha}, \tag{6}$$

and the limitation of distance r from an ST to an MBS, that is, R_M, can be derived as

$$\mathbf{E}_h\left[E_H\right] - E_C > 0 \Longleftrightarrow r < R_M \triangleq \left(\frac{D_{\text{eb}}}{\mu_h M E_C}\right)^{1/\alpha}, \tag{7}$$

where R_M is based on the setting that STs distributed in the annular region should satisfy the circuit power constraint. When fading is considered, the probability that harvested energy E_H is above demand is

$$\begin{aligned} G(x) &\triangleq \mathbb{P}\left[E_H > x\right] = \mathbb{P}\left[\frac{D_{\text{eb}} h}{M r^\alpha} > x\right] \\ &= \int_{R_m}^{R_M} \int_{M r^\alpha x / D_{\text{eb}}}^{\infty} f_{\geq R_m}(r) \cdot f(h)\, \mathrm{d}h\, \mathrm{d}r \\ &= \frac{2\left(H(x, R_m) - H(x, R_M)\right)}{\alpha\left(R_M^2 - R_m^2\right)}, \end{aligned} \tag{8}$$

where x is a parameter representing energy demand, r is the distance from an ST to its MBS, $f_{\geq R_m}(r)$ is the pdf given in (2), h is the fading, and

$$H(x,y) = y^2 E\left(\frac{\alpha-2}{\alpha}, J(x)\, y^{\alpha}\right),$$
$$J(x) = \frac{x\mu_h M}{D_{\text{eb}}}, \tag{9}$$
$$E(n,z) = \int_1^{\infty} e^{-zt} t^{-n} \mathrm{d}t \ \ (\text{exponential integral}),$$

where α, μ_h, M, and D_{eb} have been presented. Therefore, the constraint satisfaction probability p_{sat} of an ST is

$$p_{\text{sat}} \triangleq \mathbb{P}\left[E_H - E_C > 0\right] = G\left(E_C\right). \tag{10}$$

In the following, p_{sat} will also be termed *power satisfaction probability*. Taking this probability into account, STs in IT mode that have enough energy form an HPPP Φ_{it} with intensity $\lambda_{\text{it}} = p_{\text{sat}}\widetilde{\lambda}_{\text{it}} = p_{\text{sat}}\lambda_{\text{ST}}/M$. In the following, these STs are called *working STs*.

When performing IT, the available energy is $E_H - E_C$, but for ease of analysis, in this paper we adopt the setting that a portion ξ of the harvested energy E_H can be used for active information transmission [31] and energy not used is ignored in different time slots. So the transmit power of a generic ST is

$$P_{\text{it}} = \frac{\xi E_H}{1/M} = \xi D_{\text{eb}} \|X - Y\|^{-\alpha} h, \tag{11}$$

where $\|X - Y\|$ is the distance from the MBS to the ST.

2.4. Interference Model. In [32], authors mentioned *interference regeneration* that a backscatter node reflects all incident signals which leads to a square number of interference components for each SR. One effective solution is to adopt spread spectrum techniques. In this paper, we simplify this problem and assume that an ST backscatters only the signal from its corresponding MBS.

2.4.1. Backscattered Signal to an SR in IT Mode. Backscattered signal from an ST to an SR in IT mode is considered as an extra path. We assume an SR in IT mode has the ability to eliminate multipath effect like PRs [4], so such interference is ignored.

2.4.2. Transmitted Signal to an SR in BC Mode. Since an SR in BC mode senses and decodes backscattered signal by sensing changes in the signal caused by backscattering [4], we also ignore such interference.

2.4.3. Backscattered Interference to an SR in BC Mode. Such interference comes from other STs (X_i) in BC mode whose corresponding MBSs (Y_i) are in busy mode. Interfering STs come from $\Phi_{\text{bc}} \setminus \{X_0\}$. Such interference is firstly transmitted from an MBS to its ST, encountering path-loss $\ell(X_i - Y_i)$ and Rayleigh fading $h \sim \exp(\mu_h)$, then it is backscattered from an ST to the typical SR, encountering path-loss $\ell(X_i - Z_0)$ and Rayleigh fading $g \sim \exp(\mu_g)$. The interference is denoted as

$$I_{\text{bc}} = \sum_{X_i \in \Phi_{\text{bc}} \setminus \{X_0\}} P_{\text{bc}_i} \left\|X_i - Z_0\right\|^{-\alpha} g_i, \tag{12}$$

where P_{bc_i} is the backscatter power of an ST in BC mode given in (4).

2.4.4. Transmitted Interference to an SR in IT Mode. Such interference comes from other MBSs in busy mode and other STs in IT mode whose corresponding MBSs are in idle mode. Interfering MBSs come from $\Phi_{\text{bs}} \setminus \{Y_0\}$. Such interference is transmitted from an MBS to the typical SR, encountering path-loss $\ell(Y_i - Z_0)$ and Rayleigh fading $g \sim \exp(\mu_g)$. Interfering STs come from $\Phi_{\text{it}} \setminus \{X_0\}$. Such interference is firstly transmitted from an MBS to its ST, encountering path-loss $\ell(X_i - Y_i)$ and Rayleigh fading $h \sim \exp(\mu_h)$, then it is backscattered from the ST to the SR, encountering path-loss $\ell(X_i - Z_0)$ and Rayleigh fading $g \sim \exp(\mu_g)$. The interference is denoted as

$$\begin{aligned} I_{\text{sum}} &= I_{\text{it}} + I_{\text{bs}} \\ &= \sum_{X_i \in \Phi_{\text{it}} \setminus \{X_0\}} P_{\text{it}_i} \left\|X_i - Z_0\right\|^{-\alpha} g_i \\ &\quad + \sum_{Y_i \in \Phi_{\text{bs}} \setminus \{Y_0\}} \left\|Y_i - Z_0\right\|^{-\alpha} g_i, \end{aligned} \tag{13}$$

where I_{it}, I_{bs} represent two interference components, respectively, and P_{it_i} is the transmit power of an ST in IT mode given in (11).

2.4.5. Transmitted Interference to a PR. All interference to a PR is identical to the interference to an SR in IT mode. We will analyze performance of a PR located at the origin encountering no interference from STs to make a comparison to reveal the effect on PRs.

2.5. Rate Model for Backscatter Link. In [4], the bit rate (alternating sequence of ones and zeros) of the ambient backscatter prototype is related to the setting of circuit elements. Similar settings are also used in [8, 17, 18] and will be used in this paper, too. Besides, we assume if the signal-to-interference-plus-noise-ratio (SINR) of backscatter communication is above a threshold, the predesigned rate can be achieved [20].

Notations used in this paper are listed in the Notations.

3. Channel Inversion Power Control and Energy Storage and Reusing

Since energy is precious for secondary users, the harvested energy should be used more efficiently. So in this section we apply channel inversion power control to ST's active information transmission to avoid poor signal transmitted from STs. Moreover, since power control is applied, there is a higher probability that secondary users do not use up its energy. Therefore, we also propose a simple energy storage and reusing mechanism, to improve the utilization of harvested energy.

3.1. Channel Inversion Power Control. In this part, we use channel inversion power control to let STs make less interference to primary users and conserve energy, while keeping

their active transmission reliable. To be specific, an ST in IT mode will not use up its energy but transmit at a power to invert the path-loss to make sure that the average received power at its SR is equal to an SR's sensitivity ρ in IT mode [33]. Specifically, if the available energy is enough to support channel inversion power control, the ST will transmit at power ρd^{α}, where d is the distance between a secondary pair. So ρ will highly impact the performance of STs in IT mode. Besides, if the available energy cannot support the power control to achieve the SR's sensitivity, the ST will not transmit. So an ST's transmit power using channel inversion power control is

$$P_{\rho} = \begin{cases} \rho d^{\alpha}, & \dfrac{E_H - E_C}{1/M} > \rho d^{\alpha}, \\ 0, & \dfrac{E_H - E_C}{1/M} \leq \rho d^{\alpha}, \end{cases} \tag{14}$$

which can be rewritten as

$$P_{\rho} = \begin{cases} \rho d^{\alpha}, & E_H > \dfrac{\rho d^{\alpha}}{M} + E_C, \\ 0, & E_H \leq \dfrac{\rho d^{\alpha}}{M} + E_C. \end{cases} \tag{15}$$

The probability that an ST transmits at power P_{ρ}, which takes circuit power constraint into account, is

$$p_{\rho} = \mathbb{P}\left[E_H \geq \frac{\rho d^{\alpha}}{M} + E_C\right] = G\left(\frac{\rho d^{\alpha}}{M} + E_C\right), \tag{16}$$

where $G(\cdot)$ is given in (8). For convenience, $E_H > \rho d^{\alpha}/M + E_C$ is termed *power constraint with sensitivity* and p_{ρ} is termed *sensitivity satisfaction probability*. Since STs are independent from each other, working STs in IT mode adopting the power control form an HPPP Φ_{ρ} with intensity $\lambda_{\rho} = p_{\rho}\widetilde{\lambda}_{\text{it}} = p_{\rho}\lambda_{\text{ST}}/M$. Any working ST will transmit at power P_{ρ} and the remaining energy is ignored.

In the following, for convenience, when we analyze STs and PRs under power control, we still use notations which exist in normal settings, but with a slight difference when the notations involve STs in IT mode. For example, I_{it} under power control equals $\sum_{X_i \in \Phi_{\rho} \setminus \{X_0\}} P_{\rho} \| X_i - Z_0 \|^{-\alpha} g_i$.

3.2. Energy Storage and Reusing. As described above, an ST has a probability to get enough energy for transmitting in IT mode. If it does not get enough, in our previous settings, the unused energy is ignored and cannot be used in other time slots. Here we consider the setting that the energy can be stored, for a potential reusing. And we assume an ST has an energy storage component with capacity E_M. Besides, energy storage follows channel inversion power control, and the remaining energy when an ST can perform active transmission is also stored.

If the energy demand for active transmission is E_D, herein $E_D = \rho d^{\alpha}/M + E_C$, where E_C is the circuit power consumption, the stored energy in a time slot is

$$E_S = \begin{cases} E_H - E_D, & E_H > E_D, \\ E_H, & E_H \leq E_D. \end{cases} \tag{17}$$

Note that we assume an ST can detect whether the harvested energy is enough for active transmission before trying to transmit. If not enough, the ST will not work and cost no energy. Besides, the energy consumption for detection is ignored, so the harvest energy is E_H and we do not consider the case that $E_H < E_C$. From (8) we know the sensitivity satisfaction probability is $G(E_D)$; hence the expectation of stored energy is

$$\begin{aligned} \overline{E}_S &= \mathbf{E}\left[E_S\right] \\ &= G\left(E_D\right) \cdot \left(\mathbf{E}\left[E_H\right] - E_D\right) + \left(1 - G\left(E_D\right)\right) \cdot \mathbf{E}\left[E_H\right] \\ &= \mathbf{E}\left[E_H\right] - G\left(E_D\right) \cdot E_D. \end{aligned} \tag{18}$$

For ease of analysis, we assume once an ST has stored enough energy for active transmission before a time slot, it will use that energy in the slot. But the unused part and harvested energy in that slot are ignored. Therefore, the expectation of stored energy after $N_S = \lceil E_D/\overline{E}_S \rceil$ time slots is enough for another active transmission. So in the next time slot, an ST certainly has enough energy for active transmission, and the sensitivity satisfaction probability of the $N_S + 1$ slots increases to $(N_S G(E_D) + 1)/(N_S + 1)$. For simplicity we consider only the next time slot, so the increase of sensitivity satisfaction probability is

$$\begin{aligned} p_{\rho}^{\Delta} &= \left(\frac{N_S G\left(E_D\right) + 1}{N_S + 1} - G\left(E_D\right)\right)\left(1 - G\left(E_D\right)\right) \\ &= \frac{\left(G\left(E_D\right) - 1\right)^2}{N_S + 1}, \end{aligned} \tag{19}$$

where $1 - G(E_D)$ is the dissatisfaction probability, and this part means the improvement works only when harvested energy is not enough.

Although the reusing mechanism of stored energy is rough, it provides a view of reusing stored energy and increases the chance of active transmission.

Some point processes (p.p.) described in the paper, along with their descriptions, intensities (inten.), and values are listed in Table 1 to provide a clear view.

4. Coverage Probability and Achievable Rate

We analyze the coverage probabilities and average achievable rates of an SR in different communication modes and a PR, by using Shannon formula. The average rate is

$$\mathbf{E}\left[\log_2\left(1 + \text{SINR}\right)\right] = \mathbf{E}\frac{\left[\ln\left(1 + \text{SINR}\right)\right]}{\ln\left(2\right)}. \tag{20}$$

Besides, since SINR ≥ 0, it is easy to derive

$$\mathbf{E}\left[\ln\left(1 + \text{SINR}\right)\right] = \int_0^{\infty} \frac{1}{1+T} \mathbb{P}\left[\text{SINR} > T\right] \mathrm{d}T, \tag{21}$$

where T is the SINR threshold. So in the following, we will derive the coverage probability of the typical SR or PR in form

$$\mathbb{P}\left[\text{SINR} > T\right] = \mathbb{P}\left[\frac{S}{I + W} > T\right], \tag{22}$$

Table 1: Some point processes and their descriptions.

p.p.	Description	Inten.	Value
Φ_U	Primary users in a generic channel	λ_U	λ
Φ_{ST}	STs in a generic channel	λ_{ST}	$p_{\text{ch}}\lambda$
Φ_{eh}	STs in EH mode	λ_{eh}	$(D_E/M)\lambda_{\text{ST}}$
Φ_{bc}	STs in BC mode	λ_{bc}	$(D_B/M)\lambda_{\text{ST}}$
Φ_{bs}	Busy MBSs	λ_{bs}	$(1-1/M)\lambda$
$\widetilde{\Phi}_{\text{it}}$	STs in IT mode	$\widetilde{\lambda}_{\text{it}}$	λ_{ST}/M
Φ_{it}	Working STs in IT mode	λ_{it}	$p_{\text{sat}}\widetilde{\lambda}_{\text{it}}$
Φ_ρ	Working STs (power control)	λ_ρ	$p_\rho\widetilde{\lambda}_{\text{it}}$

where S is the desired signal, I is the interference, and W is the noise. After deriving the coverage probabilities, average rates can be easily obtained.

Firstly, we show some properties of the derivation processes which will be used for the following analysis and theorems.

Property 1. If the pdf of distance r from an MBS to an ST is $f_{\geq R_m}(r)$ in (2), the following expectation of r can be derived easily:

$$\mathbf{E}\left[r^{-2}\right] = \int_{r\geq R_m}^{R_M} r^{-2}\frac{2r}{R_M^2 - R_m^2}\mathrm{d}r = \frac{2\ln\left(R_M/R_m\right)}{R_M^2 - R_m^2}. \quad (23)$$

Property 2. If fading $h \sim \exp(\mu_h)$, the following expectation of h can be derived easily:

$$\mathbf{E}\left[h^{2/\alpha}\right] = \int_0^\infty \mu_h e^{-\mu_h h} h^{2/\alpha}\mathrm{d}h = \mu_h^{-2/\alpha}\Gamma\left(\frac{2}{\alpha}+1\right), \quad (24)$$

where α is the path-loss exponent and $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\mathrm{d}t$ is the Gamma function.

Property 3. If y is a random variable, the following integral of y can be represented in nonintegral form:

$$K(\alpha) = \int_0^\infty \frac{y}{1+y^\alpha}\mathrm{d}y = \frac{\pi}{\alpha\sin\left(2\pi/\alpha\right)}, \quad (25)$$

where α is the path-loss exponent. Be similar to [26], we denoted the result in (25) as $K(\alpha)$ with some differences.

Property 4. Given the Laplace transform $\mathscr{L}_X(s)$ of a continuous random variable X, the pdf $f_X(x)$ of X can be recovered by inverse Laplace transform as [21]

$$f_X(x) = \mathscr{L}^{-1}\left\{\mathscr{L}_X(s)\right\}(x). \quad (26)$$

Note that, in this paper, we focus on a generic channel, a typical primary receiver, and a typical secondary receiver. Unless otherwise stated, the following analyzed coverage probabilities and average rates are analyzed under the setting that the receivers exist already.

4.1. Coverage Probability of an SR in BC Mode. Here we analyze the coverage probability of the typical secondary receiver working in backscatter mode; that is, its secondary transmitter backscatters signals for data transmission. The desired signal power is given in (4) and the interference is analyzed in Section 2.4.

Theorem 5. *The coverage probability of an SR in BC mode located at the origin is*

$$p_c^{bc} = \int_{r\geq R_m}^{R_M}\int_{q>0}^{\infty}\mu_q\exp\left(A_{bc} - B_{bc}C\right)\mathrm{d}q f_{\geq R_m}(r)\,\mathrm{d}r, \quad (27)$$

where

$$\begin{aligned} A_{bc} &= -\mu_q q - \frac{\mu_h}{\beta\eta_b q}TWd^\alpha r^\alpha, \\ B_{bc} &= \lambda_{bc}\left(\frac{\mu_h T}{\mu_g q}\right)^{2/\alpha} d^2, \\ C &= 2\pi r^2\mathbf{E}\left[R^{-2}\right]\mathbf{E}\left[h^{2/\alpha}\right]K(\alpha), \end{aligned} \quad (28)$$

and $\mathbf{E}[R^{-2}]$, $\mathbf{E}[h^{2/\alpha}]$, *and* $K(\alpha)$ *are given in (23), (24), and (25), respectively, where R is the distance from a generic interfering ST to its MBS having the same pdf given in (2).*

Proof. See Appendix. □

4.2. Coverage Probability of an SR in IT Mode. Here we analyze the coverage probability of the typical secondary receiver working in information transmission mode, that is, receiving signals transmitted by its secondary transmitter. The desired signal power is given in (11) and the interference is analyzed in Section 2.4.

Note that the typical ST in IT mode also has a probability of satisfying circuit power constraint, so the average coverage probability of the typical SR is

$$\overline{p}_c^{\text{it}} = \begin{cases} \mathbb{P}\left[\text{SINR}_{\text{it}} > T\right], & E_H \geq E_C, \\ 0, & E_H < E_C, \end{cases} \quad (29)$$

which can be further written as

$$\overline{p}_c^{\text{it}} = p_{\text{sat}}\mathbb{P}\left[\text{SINR}_{\text{it}} > T\right]. \quad (30)$$

Since p_{sat} has been analyzed, in the following, we mainly derive $p_c^{\text{it}} = \mathbb{P}[\text{SINR}_{\text{it}} > T]$ under the assumption that the typical ST satisfies the circuit power constraint, and *coverage probability* refers to p_c^{it} for convenience.

Theorem 6. *The coverage probability of an SR in IT mode located at the origin is*

$$p_c^{\mathrm{it}} = \int_{r\geq R_m}^{R_M} \int_{q>0}^{\infty} \mu_q \exp\left(A_{\mathrm{it}} - B_{\mathrm{it}}C - D_{\mathrm{it}}\right) \mathrm{d}q f_{\geq R_m}(r)\,\mathrm{d}r, \tag{31}$$

where

$$\begin{aligned} A_{\mathrm{it}} &= -\mu_q q - \frac{\mu_h TW}{\xi D_{\mathrm{eb}} q} d^{\alpha} r^{\alpha}, \\ B_{\mathrm{it}} &= \lambda_{\mathrm{it}} \left(\frac{\mu_h T}{\mu_g q}\right)^{2/\alpha} d^2, \\ D_{\mathrm{it}} &= 2\pi\lambda_{\mathrm{bs}} \left(\frac{\mu_h T}{\mu_g \xi D_{\mathrm{eb}} q}\right)^{2/\alpha} d^2 r^2 K(\alpha), \end{aligned} \tag{32}$$

and C is given in (28).

Proof. See Appendix. □

4.3. Coverage Probability of a PR. Here we analyze the coverage probability of the typical primary receiver with regard to interference from STs in IT mode. The desired signal comes from its MBS, and the interference is analyzed in Section 2.4.

Theorem 7. *The coverage probability of a PR located at the origin is*

$$p_c^{pr} = \int_{r>0}^{\infty} \exp\left(A_{pr} - B_{pr}C - D_{pr}\right) f(r)\,\mathrm{d}r, \tag{33}$$

where

$$\begin{aligned} A_{pr} &= -\mu_h TW r^{\alpha}, \\ B_{pr} &= \lambda_{it} \left(\frac{\xi D_{eb} \mu_h T}{\mu_g}\right)^{2/\alpha}, \\ D_{pr} &= 2\pi\lambda_{bs} \left(\frac{\mu_h T}{\mu_g}\right)^{2/\alpha} r^2 \int_{(\mu_g/(\mu_h T))^{1/\alpha}}^{\infty} \frac{y}{1+y^{\alpha}} \mathrm{d}y, \end{aligned} \tag{34}$$

and C is given in (28).

Proof. See Appendix. □

4.4. Coverage Probability of a PR without Interference from STs. Here we analyze the coverage probability of the typical primary receiver without interference from STs in IT mode. The desired signal still comes from the MBS and the primary receiver suffers only interference from other MBSs.

Theorem 8. *The coverage probability of a PR considering no interference from STs is*

$$p_c^{pr'} = \int_{r>0}^{\infty} \exp\left(A_{pr} - D_{pr}\right) f(r)\,\mathrm{d}r, \tag{35}$$

where A_{pr} and D_{pr} are given in (34).

Proof. See Appendix. □

4.5. Coverage Probability of an SR in IT Mode under Power Control. Here we analyze the coverage probability of the typical secondary receiver working in information transmission mode and adopting power control. The main differences are the transmit power of STs and their constraint satisfaction probability from p_{sat} to p_ρ.

Similarly to Section 4.2, coverage probability averaged over constraint satisfaction probability is

$$\overline{p}_{c,\rho}^{\mathrm{it}} = p_\rho \mathbb{P}\left[\mathrm{SINR}_{\mathrm{it}}^{\rho} > T\right], \tag{36}$$

and in the following, *coverage probability* refers to $p_{c,\rho}^{\mathrm{it}} = \mathbb{P}[\mathrm{SINR}_{\mathrm{it}}^{\rho} > T]$ under the assumption that the typical ST satisfies the power constraint with sensitivity.

Theorem 9. *The coverage probability of an SR in IT mode under power control is*

$$p_{c,\rho}^{it} = \exp\left(A_{it}^{\rho} - \lambda_\rho D_{it}^{\rho} - \lambda_{bs} P_\rho^{-2/\alpha} D_{it}^{\rho}\right), \tag{37}$$

where

$$\begin{aligned} A_{it}^{\rho} &= -\frac{\mu_q TW}{P_\rho} d^{\alpha}, \\ D_{it}^{\rho} &= 2\pi \left(\frac{\mu_q T}{\mu_g}\right)^{2/\alpha} d^2 K(\alpha). \end{aligned} \tag{38}$$

Proof. See Appendix. □

4.6. Coverage Probability of a PR under Power Control

Theorem 10. *The coverage probability of a PR suffering interference from STs in IT mode under power control is*

$$p_{c,\rho}^{pr} = \int_{r>0}^{\infty} \exp\left(A_{pr} - B_{pr}^{\rho} - D_{pr}\right) f(r)\,\mathrm{d}r, \tag{39}$$

where A_{pr}, D_{pr} are given in (34), and

$$B_{pr}^{\rho} = 2\pi\lambda_\rho \left(\frac{\mu_h T}{\mu_g}\right)^{2/\alpha} r^2 P_\rho^{2/\alpha} K(\alpha). \tag{40}$$

Proof. See Appendix. □

5. Numerical Results

We evaluate our analytical results by simulations. The simulation region is a square with side length of 10 km. The simulation results are obtained by averaging over 1000 runs. Unless otherwise stated, parameter values are listed in Table 2. To generate uniformly distributed points in an annular region, we use a native method of generating a random point within a circle with radius R_M, and if the random value is smaller than the inner radius R_m, the point will be generated repeatedly until it is in the annular region. A mathematical method is to use *inverse transform sampling*.

Table 2: Parameter value list.

Parameter	Value
Inner radius of annular regions R_m	5
Constant distance from an SR to its ST d	10
MBS density λ	5/km^2
Poisson distribution parameter Λ	3
Number of channels N_{ch}	4
Minislot number M	7
BC minislot number D_B	3 (i.e., $D_E = 3$)
Path-loss exponent α	4
Fading parameters μ_h, μ_g, μ_q	1
Noise W	−90 dBm
EH efficiency η	0.6
BC portion β	0.3
BC efficiency η_b	0.6
IT portion ξ	0.5
Circuit energy consumption E_C	−30 dBm
SR's sensitivity in IT mode	−60 dBm

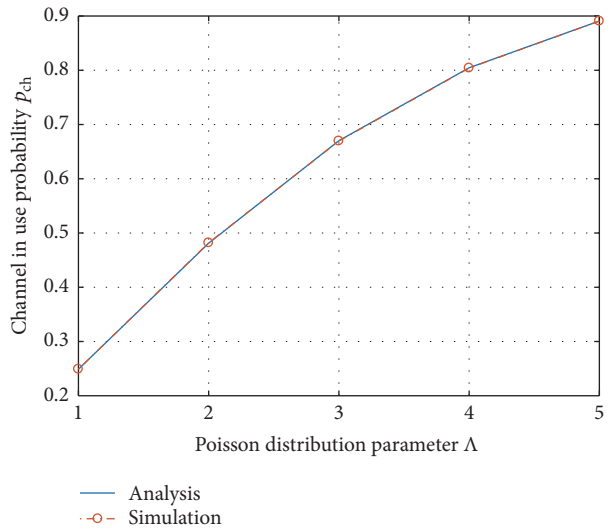


Figure 4: Channel in use probability versus Poisson distribution parameter (i.e., average number of STs clusters around an MBS).

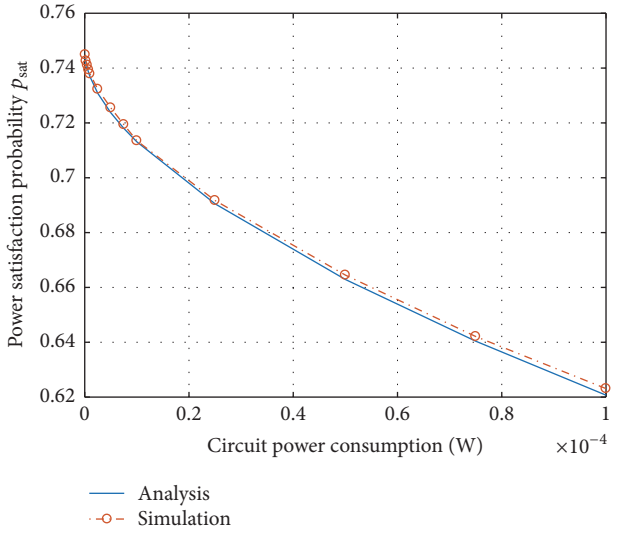


Figure 5: Power satisfaction probability of an ST.

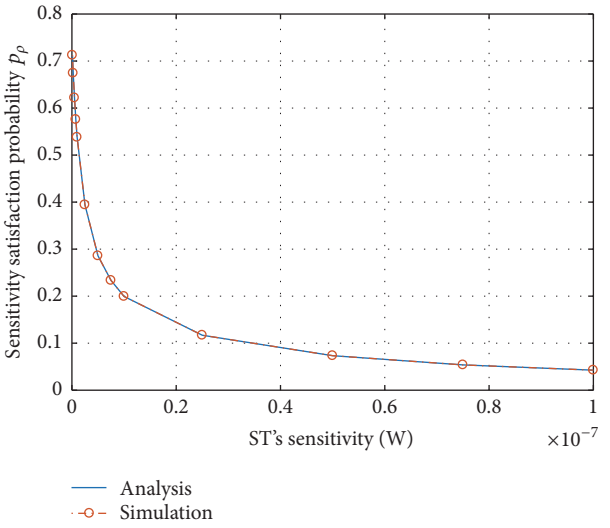


Figure 6: Sensitivity satisfaction probabilities of an ST under power control.

5.1. Channel in Use Probability. Figure 4 shows the channel in use probability p_{ch} given in (3). The simulation of channel selection is performed by random selection from all possible combinations. STs clustering around an MBS select idle channels using the method in Section 2.2; that is, they randomly select idle channels. We focus on the typical channel (numbered 1) and count how many typical channels are selected by STs clustering around all MBSs. The analytical and simulation curves overlap since the channel selection is simple, and the results are almost identical.

5.2. Power Satisfaction Probability and Sensitivity Satisfaction Probability. Figure 5 shows the power satisfaction probability p_{sat} given in (10), of an ST. As circuit power consumption E_C increases from −40 dBm (0.1 μW) to −10 dBm (0.1 mW), the probability decreases, but not much. The reason is that a larger E_C makes STs closer to MBSs, and STs then can harvest more energy to support a high satisfaction probability.

Figure 6 shows the sensitivity satisfaction probability p_ρ given in (16), of an ST under power control. As SRs' sensitivity ρ increases from −70 dBm to −50 dBm, p_ρ decreases sharply. The reason is that ρ does not change R_M, but requires more energy. And when ρ decreases further, the probability is already very low, so the change of satisfaction probability is small. The difference between these two figures also reveals the importance of R_M. Moreover, p_ρ is affected by circuit power constraint as well, which further affects the energy demand to transmit at P_ρ.

5.3. Coverage Probabilities. Figure 7 shows the analytical and simulated coverage probabilities of an ST in BC mode, IT

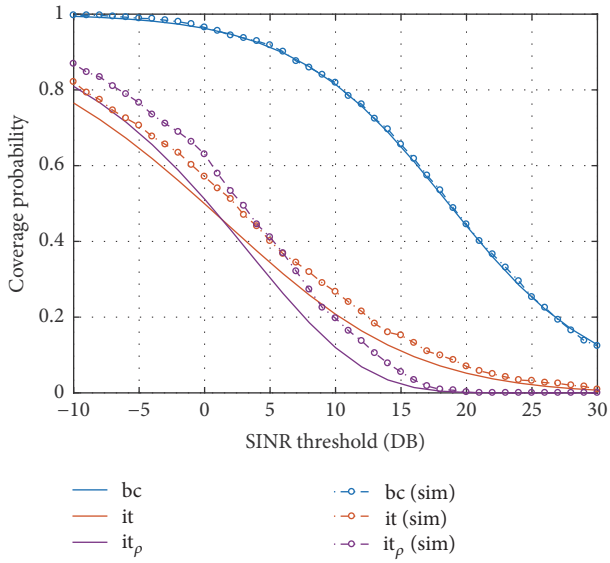


FIGURE 7: Analytical coverage probability of an ST in BC mode (bc), IT mode (it), and IT mode under power control (it$_\rho$).

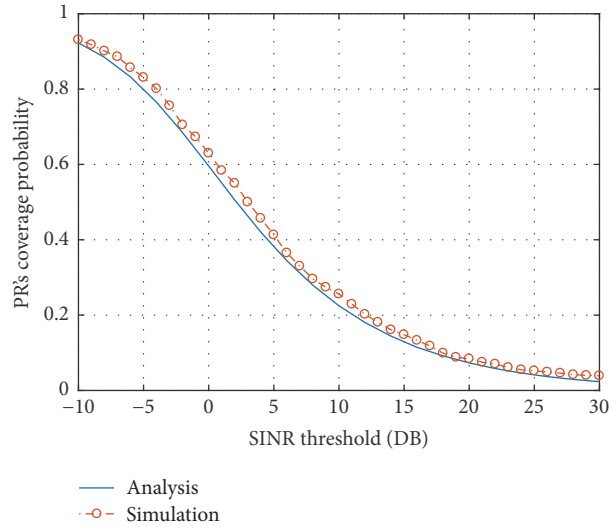


FIGURE 8: Analytical and simulated coverage probabilities of a PR.

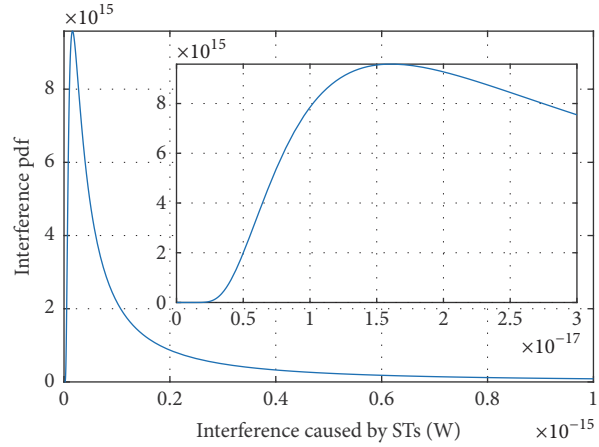


FIGURE 9: Analytical distribution of interference caused by STs in IT mode.

mode, and IT mode under power control. Since distance from an ST to its MBS and distance from an SR to its ST are both very short, signals decay not much. Besides, as described in Section 2.4, transmitted signals from MBSs and STs in IT mode make no interference to an SR in BC mode, so coverage probability of BC mode is much higher, while coverage probability of IT mode (under power control) is lower. Moreover, there is an intersection of curves of probabilities of IT mode and IT mode under power control. This happens since an SR in normal IT mode receives varied-power signals related to the ST's harvested energy. This means an ST may transmit at a high power, resulting in a high SINR, and may transmit at a low power, resulting in a low SINR. So the SINRs of SRs in normal IT mode range widely. On the other hand, an SR in IT mode under power control always receives constant-power (equals its sensitivity) signals from its ST, if fading is not considered. This means, there are few SRs having (extremely) low SINRs or high SINRs, which makes the curve shrink horizontally.

Note that these probabilities are not averaged over p_{sat} or p_ρ; that is, we assume the typical ST has already satisfied the constraints.

Figure 8 shows the analytical and simulated coverage probabilities of a PR. The probabilities of a PR interfered or not by STs in IT mode change too little to be observed, so the figure shows that only two curves represent analytical and simulated results. Since an ST transmits by using harvested energy, the transmit power is relatively lower to the power of MBSs. Besides, only STs whose MBSs are idle can transmit, and the idle ratio is low (1/7 in our settings), so the number of interfering STs to a PR is small. These are the two main reasons why STs' interference to a PR is so low. As for an SR in IT mode, since it is very close to its ST, it still gets high SINR even when the ST transmits at low power.

5.4. Distributions of Interference Caused by STs in IT Mode and under Power Control. As interference caused by STs in IT mode (and under power control) to a PR has quite limited effect on the PR's SINR, here we give the distributions of interference caused by STs. Following (26) in Property 4, (B.3) in Appendix, and (E.3) in Appendix, the analytical interference distributions caused by STs in IT mode and STs under power control are drawn in Figures 9 and 10, respectively.

5.5. Effect of Minislots Assignment on Coverage Probabilities. The different assignments of minislots, that is, different D_B and D_E, result into different numbers of STs in backscatter mode and energy harvesting mode, that is, intensities λ_{bc} and λ_{eh} of Φ_{bc} and Φ_{eh}, respectively. The intensity λ_{bc} does not affect backscatter power of an ST, because backscattering is instantaneous. But λ_{bc} affects interference power since it changes number of STs in backscatter mode. However, as described in previous subsection, SINR of an SR in BC mode is much higher, which means change of interference power

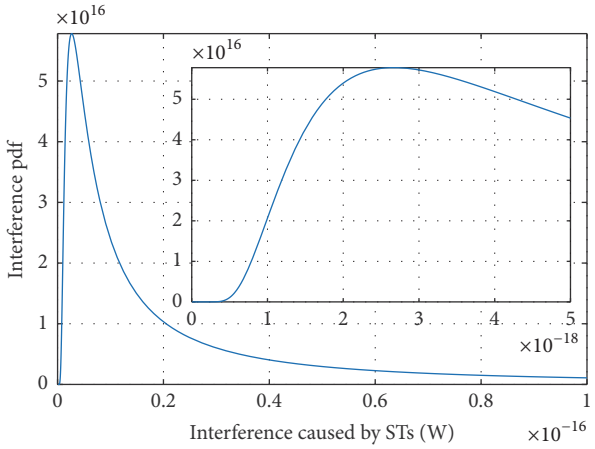


Figure 10: Analytical distribution of interference caused by STs in IT mode (under power control).

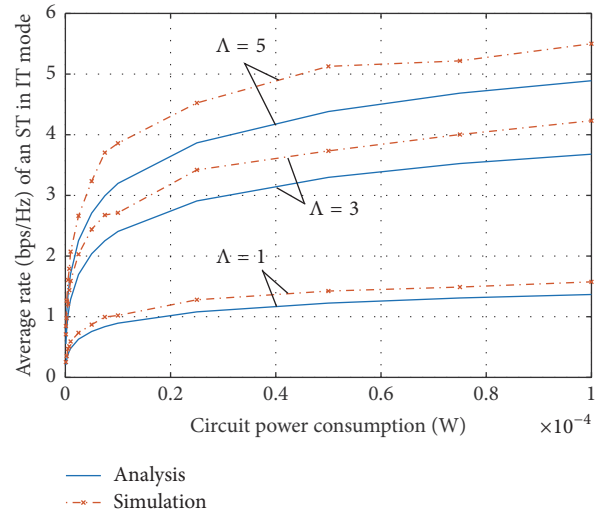


Figure 11: Average rates of an ST in IT mode versus circuit power consumption.

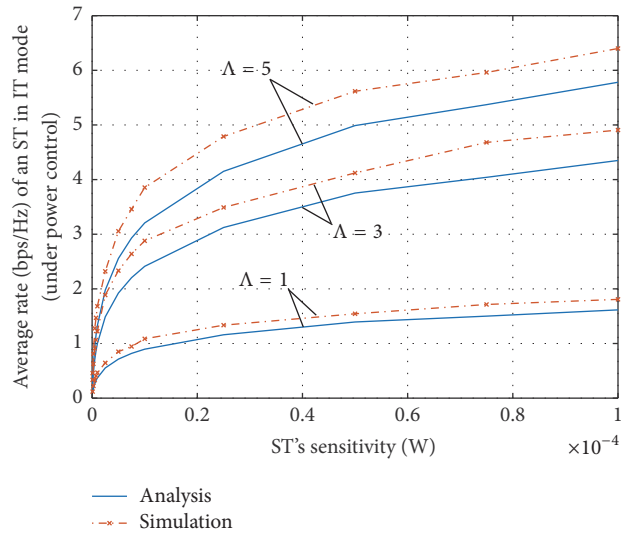


Figure 12: Average rates of an ST in IT mode under power control versus sensitivity.

makes little effect on the SINR, where noise W affects. So in both analytical and simulated results, when D_B changes from 1 to 5, p_c^{bc} varies quite little (less than 3%) when 5 dB is selected as the SINR threshold.

As for coverage probabilities of an SR in other modes, they change quite little, too (less than 1% and 4% in analytical and simulated results, resp.). The reason is that when D_B decreases, all STs harvest more energy (on average), so their transmit powers increase together. On the other hand, since we assume each MBS turns into idle in only one minislot, the minislots assignment does not affect number of STs in IT mode. Therefore, D_B makes little change on their SINRs. As for PR, since STs' impact of it is very limited as shown in the previous subsection, its SINR changes little (less than 1% and 3% in analytical and simulated results, resp.) when D_B varies.

5.6. Coverage Probabilities When Channels Are Fully Used. When considering special case *fully used channels*, $p_{\text{ch}} = 1$ holds and other settings remained. The analytical and simulated results of coverage probabilities in this case are very close to the above probabilities under normal settings. The analytical average changes over different SINR thresholds are 0.11%, 0.01%, 0.01%, 0%, 0%, and 0.01% corresponding to BC mode, IT mode, IT mode under power control, a PR, a PR without STs, and a PR (STs under power control), respectively. And the simulated average changes are 0.90%, 1.81%, 0.83%, 0.83%, 0.47%, and 0.83%, respectively. So when $N_{\text{ch}} = 4$ and Λ changes from 3 to a high enough value, the coverage probabilities change little.

5.7. Average Rates of STs in IT Mode. Figure 11 shows average rates of an ST in IT mode versus circuit power consumption E_C, with different Λ. As E_C increases, the rate becomes higher, too. This reason is that E_C affects R_M given in (7). A smaller E_C means a smaller R_M since STs have to be distributed closer to MBSs to get enough energy. However, since we assume a portion of the harvested energy can be used to perform information transmission, the power of the desired signal increases as well, resulting in a higher rate. Figure 12 shows average rates of an ST in IT mode under power control versus SRs' sensitivity ρ, with different Λ. As ρ increases, an SR receives a higher SINR because the desired signal is stronger, and there are less interfering STs.

Note that the rates are averaged over p_{ch} which represents the utility ratio of a channel by STs. Besides, since it is observed that STs in IT mode have limited interference to PRs, rates of a PR are omitted.

5.8. Average Stored Energy and Reusing. A larger circuit power consumption E_C or SRs' sensitivity ρ makes energy demand E_D higher, $G(E_D)$ lower, R_M smaller, and E_H higher. So the impact on average stored energy in a time slot $\overline{E}_S$ cannot be observed directly from (18). Figures 13 and 14 show

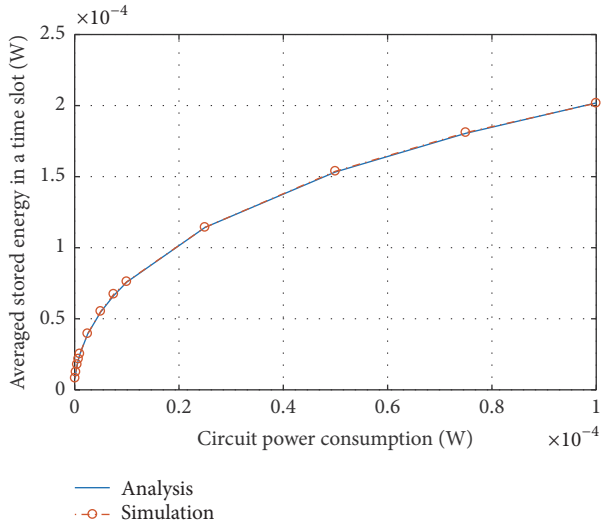


Figure 13: Average stored energy of an ST versus circuit power consumption.

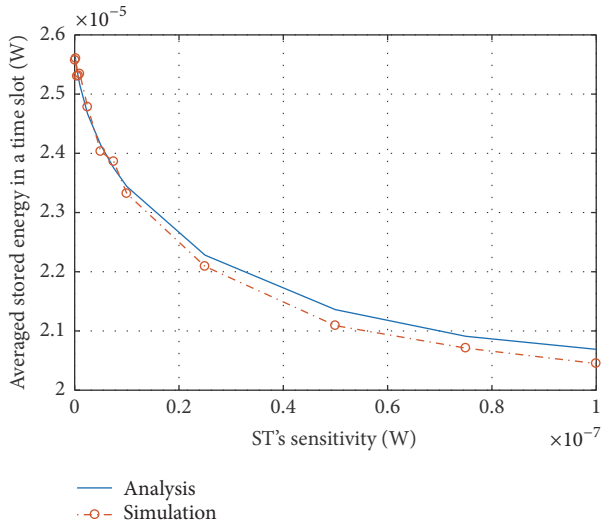


Figure 14: Average stored energy of an ST versus sensitivity.

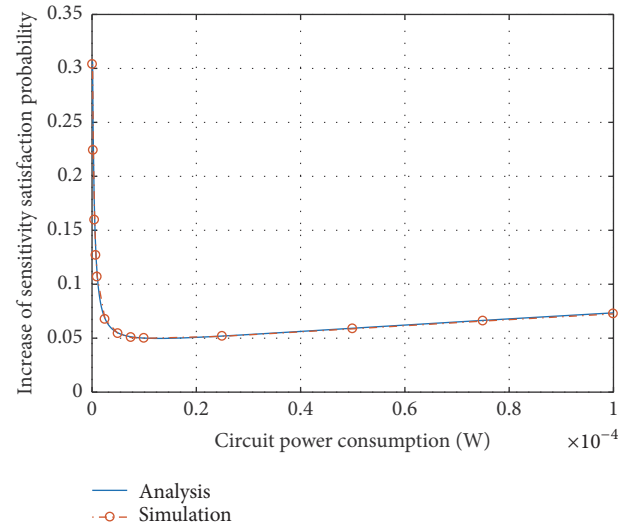


Figure 15: Average stored energy of an ST versus circuit power consumption.

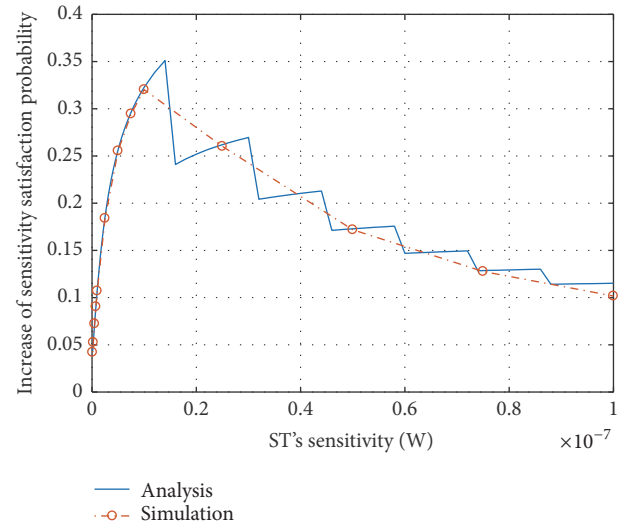


Figure 16: Average stored energy of an ST versus sensitivity.

the analytical and simulated results of $\overline{E}_S$ versus E_C and ρ, respectively.

Figures 15 and 16 show the sensitivity satisfaction probability increase p_ρ^Δ given in (19). These results are computed using (19), and the simulation data needed are obtained from simulations. Besides, analytical results are computed in small granularity (about 100 data points in both figures), while a spot of simulated data points is drawn in circles. Under our parameter settings, when E_C increases, p_ρ^Δ decreases sharply with a slow increase after that. But when ρ increases, p_ρ^Δ varies like a staircase function and decreases overall after the beginning increase. The staircase follows N_S which contains a ceiling function. Once the energy demand is large enough or averaged stored energy is less enough, N_S increases by 1, and the satisfaction probability drops down.

6. Conclusions

In this work, we have analyzed the performance of ambient backscatter communications in RF-powered cognitive radio networks based on stochastic geometry. Besides, we have applied channel inversion power control to active information of secondary users. After that, a simple energy storage and reusing mechanism has been designed and analyzed to improve utilization of harvested energy. Analytical results for constraint satisfaction probabilities and coverage probabilities of secondary users and of primary users considering both communication modes of secondary users have been obtained. Besides, average rates of secondary users have been obtained based on coverage probability. As for energy reusing, we have analyzed average stored energy during a time slot and the increase of constraint satisfaction

probability when power control is applied. The numerical results validate our theoretical analysis. Also, the results show performance improvement of secondary systems with only limited impact on the performance of primary systems. The analytical results and simulations demonstrate that integrating ambient backscatter communications into RF-powered cognitive radio network is a promising way to achieve energy and spectrum efficient wireless communications, which is suitable for certain Internet of things (IoT) applications.

Appendix

A. Proof of Theorem 5

By definition of coverage probability with SINR threshold T, we can start as

$$\begin{aligned} p_c^{\mathrm{bc}} &\triangleq \mathbb{P}\left[\mathrm{SINR}_{\mathrm{bc}} > T\right] = \mathbb{P}\left[\frac{P_{\mathrm{bc}} d^{-\alpha} q}{I_{\mathrm{bc}} + W} > T\right] \\ &= \mathbb{P}\left[\frac{\beta\eta_b r^{-\alpha} h d^{-\alpha} q}{I_{\mathrm{bc}} + W} > T\right] = \int_{r\geq R_m}^{R_M} \int_{q>0}^{\infty} \mu_q e^{-\mu_q q} \\ &\cdot \mathbb{P}\left[h > \frac{1}{\beta\eta_b q} T\left(I_{\mathrm{bc}} + W\right) d^{\alpha} r^{\alpha}\right] \mathrm{d}q \\ &\cdot f_{\geq R_m}(r)\, \mathrm{d}r, \end{aligned} \tag{A.1}$$

where P_{bc} is the backscatter power of the typical ST given in (4), r is the distance from the typical MBS to the typical ST, and d is the constant distance from the typical ST to the typical SR. The inner probability can be derived as

$$\begin{aligned} &\mathbb{P}\left[h > \frac{1}{\beta\eta_b q} T\left(I_{\mathrm{bc}} + W\right) d^{\alpha} r^{\alpha}\right] \\ &= \int_{i>0}^{\infty} \mathbb{P}\left[h > \frac{1}{\beta\eta_b q} T\left(I_{\mathrm{bc}} + W\right) d^{\alpha} r^{\alpha}\right] f_I(i)\, \mathrm{d}i \\ &= \exp\left(-\frac{\mu_h}{\beta\eta_b q} T W d^{\alpha} r^{\alpha}\right) \mathscr{L}_I\left(\frac{\mu_h}{\beta\eta_b q} T d^{\alpha} r^{\alpha}\right) \\ &= \exp(-sW)\, \mathscr{L}_{I_{\mathrm{bc}}}(s), \end{aligned} \tag{A.2}$$

where $s = (\mu_h/(\beta\eta_b q)) T d^{\alpha} r^{\alpha}$ and $\mathscr{L}_{I_{\mathrm{bc}}}(s)$ is the Laplace transform of I_{bc} and can be derived as

$$\begin{aligned} \mathscr{L}_{I_{\mathrm{bc}}}(s) &= \mathbf{E}\left[\exp\left(-sI_{\mathrm{bc}}\right)\right] \\ &= \mathbf{E}_{\Phi_{\mathrm{bc}}} \mathbf{E}_{P_{\mathrm{bc}_i}} \mathbf{E}_{g_i}\left[\exp\left(-s \sum_{X_i \in \Phi_{\mathrm{bc}} \setminus \{X_0\}} P_{\mathrm{bc}_i} \left\|X_i - Z_0\right\|^{-\alpha} g_i\right)\right] \\ &= \mathbf{E}_{\Phi_{\mathrm{bc}}} \prod_{X_i \in \Phi_{\mathrm{bc}} \setminus \{X_0\}} \mathbf{E}_{P_{\mathrm{bc}_i}} \mathbf{E}_{g_i}\left[\exp\left(-sP_{\mathrm{bc}_i} \left\|X_i - Z_0\right\|^{-\alpha} g_i\right)\right] \\ &= \exp\left(-2\pi\lambda_{\mathrm{bc}} \int_0^{\infty} \left(1 - \mathbf{E}_{P_{\mathrm{bc}}} \mathbf{E}_g\left[\exp\left(-sP_{\mathrm{bc}} x^{-\alpha} g\right)\right]\right) x\, \mathrm{d}x\right), \end{aligned} \tag{A.3}$$

where the last step follows from the probability generating functional of PPP [23]. The lower limit 0 follows from the fact that ST's positions are independent from each other, and SRs are in isotropic directions, so it could happen that another ST is close enough to an SR.

The inner expectation of g is

$$\begin{aligned} &\mathbf{E}_g\left[\exp\left(-sP_{\mathrm{bc}} x^{-\alpha} g\right)\right] \\ &= \int_0^{\infty} \mu_g e^{-\mu_g g} \exp\left(-sP_{\mathrm{bc}} x^{-\alpha} g\right) \mathrm{d}g \\ &= \int_0^{\infty} \mu_g \exp\left(-\left(\mu_g + sP_{\mathrm{bc}} x^{-\alpha}\right) g\right) \mathrm{d}g \\ &= \frac{1}{1 + \mu_g^{-1} sP_{\mathrm{bc}} x^{-\alpha}}. \end{aligned} \tag{A.4}$$

Plugging (A.4) into (A.3) gives

$$\begin{aligned} &\mathscr{L}_{I_{\mathrm{bc}}}(s) \\ &= \exp\left(-2\pi\lambda_{\mathrm{bc}} \int_0^{\infty} \mathbf{E}_{P_{\mathrm{bc}}}\left[\frac{1}{1 + 1/\left(\mu_g^{-1} sP_{\mathrm{bc}} x^{-\alpha}\right)}\right] \right. \\ &\left. \cdot x\, \mathrm{d}x\right). \end{aligned} \tag{A.5}$$

By changing the variable $x = (\mu_g^{-1} sP_{\mathrm{bc}})^{1/\alpha} y$, $\mathscr{L}_{I_{\mathrm{bc}}}(s)$ is further simplified as

$$\begin{aligned} &\mathscr{L}_{I_{\mathrm{bc}}}(s) \\ &= \exp\left(-2\pi\lambda_{\mathrm{bc}} \left(\mu_g^{-1} s\right)^{2/\alpha} \mathbf{E}\left[P_{\mathrm{bs}}^{2/\alpha}\right] \int_0^{\infty} \frac{y}{1 + y^{\alpha}} \mathrm{d}y\right), \end{aligned} \tag{A.6}$$

where

$$\mathbf{E}\left[P_{\mathrm{bs}}^{2/\alpha}\right] = (\beta\eta_b)^{2/\alpha} \mathbf{E}\left[R^{-2}\right] \mathbf{E}\left[h^{2/\alpha}\right], \tag{A.7}$$

where R is the distance from an interfering ST to its corresponding MBS with pdf $f_{\geq R_m}(R)$, which means $\mathbf{E}[R^{-2}]$ can be derived as (23). Besides, plugging s, $\mathbf{E}[P_{\mathrm{bs}}^{2/\alpha}]$, and (25) into $\mathscr{L}_{I_{\mathrm{bc}}}(s)$ gives

$$\begin{aligned} &\mathscr{L}_{I_{\mathrm{bc}}}(s) \\ &= \exp\left(-2\pi\lambda_{\mathrm{bc}} \left(\frac{\mu_h T}{\mu_g q}\right)^{2/\alpha} d^2 r^2 \mathbf{E}\left[R^{-2}\right] \mathbf{E}\left[h^{2/\alpha}\right] K(\alpha)\right). \end{aligned} \tag{A.8}$$

And plugging intermediate results into former equations will complete the proof.

Note that s here has no specific physical meaning, so for convenience, in other proofs, we still use the notation s with different values when we derive Laplace transforms.

B. Proof of Theorem 6

Here we show parts of the proof since it is similar to Appendix.

By definition of coverage probability,

$$p_c^{\mathrm{it}} \triangleq \mathbb{P}\left[\mathrm{SINR}_{\mathrm{it}} > T\right] = \mathbb{P}\left[\frac{P_{\mathrm{it}} d^{-\alpha} q}{I_{\mathrm{sum}} + W} > T\right]$$
$$= \mathbb{P}\left[\frac{\xi D_{\mathrm{eb}} r^{-\alpha} h d^{-\alpha} q}{I_{\mathrm{sum}} + W} > T\right] = \int_{r \geq R_m}^{R_M} \int_{q>0}^{\infty} \mu_q e^{-\mu_q q} \quad \text{(B.1)}$$
$$\cdot \mathbb{P}\left[h > \frac{T\left(I_{\mathrm{sum}} + W\right) d^{\alpha} r^{\alpha}}{\xi D_{\mathrm{eb}} q}\right] \mathrm{d}q f_{\geq R_m}(r)\, \mathrm{d}r,$$

where P_{it} is the transmit power of the typical ST in (11) and r and d are given in (A.1). By using the method in Appendix, it is easy to derive the inner probability as

$$\mathbb{P}\left[h > \frac{T\left(I_{\mathrm{sum}} + W\right) d^{\alpha} r^{\alpha}}{\xi D_{\mathrm{eb}} q}\right] = \exp\left(-sW\right) \mathscr{L}_{I_{\mathrm{sum}}}(s), \quad \text{(B.2)}$$

where $s = \mu_h T d^{\alpha} r^{\alpha} / (\xi D_{\mathrm{eb}} q)$. Since $I_{\mathrm{sum}} = I_{\mathrm{it}} + I_{\mathrm{bs}}$, we can get $\mathscr{L}_{I_{\mathrm{sum}}}(s) = \mathscr{L}_{I_{\mathrm{it}}}(s) \cdot \mathscr{L}_{I_{\mathrm{bs}}}(s)$. Continually following the steps in Appendix, we can derive the two Laplace transform components as

$$\mathscr{L}_{I_{\mathrm{it}}}(s)$$
$$= \mathbf{E}_{\Phi_{\mathrm{it}}} \mathbf{E}_{P_{\mathrm{it}_i}} \mathbf{E}_{g_i}\left[\exp\left(-s \sum_{X_i \in \Phi_{\mathrm{it}} \setminus \{X_0\}} P_{\mathrm{it}_i} \left\|X_i - Z_0\right\|^{-\alpha} g_i\right)\right] \quad \text{(B.3)}$$
$$= \exp\left(-2\pi\lambda_{\mathrm{it}} \left(\mu_g^{-1} s\right)^{2/\alpha} \mathbf{E}\left[P_{\mathrm{it}}^{2/\alpha}\right] K(\alpha)\right),$$

where

$$\mathbf{E}\left[P_{\mathrm{it}}^{2/\alpha}\right] = \left(\xi D_{\mathrm{eb}}\right)^{2/\alpha} \mathbf{E}\left[R^{-2}\right] \mathbf{E}\left[h^{2/\alpha}\right], \quad \text{(B.4)}$$

$$\mathscr{L}_{I_{\mathrm{bs}}}(s)$$
$$= \mathbf{E}_{\Phi_{\mathrm{bs}}} \mathbf{E}_{g_i}\left[\exp\left(-s \sum_{Y_i \in \Phi_{\mathrm{bs}} \setminus \{Y_0\}} \left\|Y_i - Z_0\right\|^{-\alpha} g_i\right)\right] \quad \text{(B.5)}$$
$$= \exp\left(-2\pi\lambda_{\mathrm{bs}} \left(\mu_g^{-1} s\right)^{2/\alpha} K(\alpha)\right).$$

Note that MBSs transmit at unit power, so there is no power notation before $\|Y_i - Z_0\|$. Finally, we can get the desired result by substituting intermediate results.

C. Proof of Theorem 7

Here we also give parts of the proof starting from definition of coverage probability:

$$p_c^{\mathrm{pr}} \triangleq \mathbb{P}\left[\mathrm{SINR}_{\mathrm{pr}} > T\right] = \mathbb{P}\left[\frac{r^{-\alpha} h}{I_{\mathrm{sum}} + W} > T\right]$$
$$= \int_{r>0}^{\infty} \mathbb{P}\left[h > T\left(\mathrm{I}_{\mathrm{sum}} + W\right) r^{\alpha}\right] f(r)\, \mathrm{d}r, \quad \text{(C.1)}$$

where r is the distance from the typical MBS to the typical PR, $f(r)$ is given in (1), and I_{sum} is given in (13). The inner probability is

$$\mathbb{P}\left[h > T\left(I_{\mathrm{sum}} + W\right) r^{\alpha}\right] = \exp\left(-sW\right) \mathscr{L}_{I_{\mathrm{sum}}}(s), \quad \text{(C.2)}$$

where $s = \mu_h T r^{\alpha}$. The first component of the Laplace transform $\mathscr{L}_{I_{\mathrm{it}}}(s)$ is the same as (B.3) except the specific value of s. The second component can be derived as

$$\mathscr{L}_{I_{\mathrm{bs}}}(s)$$
$$= \mathbf{E}_{\Phi_{\mathrm{bs}}} \mathbf{E}_{g_i}\left[\exp\left(-s \sum_{Y_i \in \Phi_{\mathrm{bs}} \setminus \{Y_0\}} \left\|Y_i - U_0\right\|^{-\alpha} g_i\right)\right]$$
$$= \exp\left(-2\pi\lambda_{\mathrm{bs}} \int_r^{\infty} \left(1 - \mathbf{E}_g\left[\exp\left(-sx^{-\alpha} g\right)\right]\right) x\, \mathrm{d}x\right) \quad \text{(C.3)}$$
$$= \exp\left(-2\pi\lambda_{\mathrm{bs}} \left(\mu_g^{-1} s\right)^{2/\alpha} \int_{r(\mu_g^{-1} s)^{-1/\alpha}}^{\infty} \frac{y}{1 + y^{\alpha}} \mathrm{d}y\right),$$

where the main difference is the lower limit r in the second equality, which follows from the fact that each PR is associated with its nearest MBS. The proof is similar to Appendix, so the remaining parts are omitted.

D. Proof of Theorem 8

Since the proof can be seen as parts of Appendix, we give only the definition of this coverage probability:

$$p_c^{\mathrm{pr}'} \triangleq \mathbb{P}\left[\mathrm{SINR}_{\mathrm{pr}'} > T\right] = \mathbb{P}\left[\frac{r^{-\alpha} h}{I_{\mathrm{bs}} + W} > T\right], \quad \text{(D.1)}$$

where I_{bs} is given in (13). The result follows from removing the part of interference of STs in Appendix and proof details are omitted.

E. Proof of Theorem 9

When adopting power control, the desired signal power and interfering power from other STs in IT mode both change, so these two components are the main differences when compared to p_c^{it} in Appendix.

By definition of coverage probability,

$$p_{c,\rho}^{\mathrm{it}} \triangleq \mathbb{P}\left[\mathrm{SINR}_{\mathrm{it}} > T\right] = \mathbb{P}\left[\frac{P_{\rho} d^{-\alpha} q}{I_{\mathrm{sum}} + W} > T\right]$$
$$= \mathbb{P}\left[q > \frac{T\left(I_{\mathrm{sum}} + W\right) d^{\alpha}}{P_{\rho}}\right], \quad \text{(E.1)}$$

where P_{ρ} is the transmit power of the typical ST and d is the constant distance from the typical ST to the typical SR. Different from Appendix, since the transmit power is constant, the derivation will be much simpler as the following:

$$\mathbb{P}\left[q > \frac{T\left(I_{\mathrm{sum}} + W\right) d^{\alpha}}{P_{\rho}}\right]$$
$$= \int_{i>0}^{\infty} \mathbb{P}\left[q > \frac{T\left(I_{\mathrm{sum}} + W\right) d^{\alpha}}{P_{\rho}}\right] f_I(i)\, \mathrm{d}i \quad \text{(E.2)}$$
$$= \exp\left(-sW\right) \mathscr{L}_{I_{\mathrm{sum}}}(s),$$

where $s = \mu_q T d^\alpha / P_\rho$. Similarly $\mathscr{L}_{I_{\text{sum}}}(s) = \mathscr{L}_{I_{\text{it}}^\rho}(s) \cdot \mathscr{L}_{I_{\text{bs}}}(s)$, and the two Laplace transform components can be derived as

$$\begin{aligned}
&\mathscr{L}_{I_{\text{it}}^\rho}(s) \\
&= \mathbf{E}_{\Phi_\rho} \mathbf{E}_{g_i} \left[\exp\left(-s \sum_{X_i \in \Phi_\rho \setminus \{X_0\}} P_\rho \left\| X_i - Z_0 \right\|^{-\alpha} g_i \right) \right] \quad \text{(E.3)} \\
&= \exp\left(-2\pi\lambda_\rho \left(\mu_g^{-1} s \right)^{2/\alpha} P_\rho^{2/\alpha} K(\alpha) \right),
\end{aligned}$$

and $\mathscr{L}_{I_{\text{bs}}}(s)$ is the same as (B.5) except the specific value of s. Substituting intermediate results will finish the proof.

F. Proof of Theorem 10

Since interfering power from other STs to a PR is the sole difference when STs adopt power control, only $\mathscr{L}_{I_{\text{it}}}(s)$ differs from that in Appendix. Moreover, it is the same as (E.3) except the specific value of s, and s is the same as that in Appendix. So we omit the proof details.

Notations

α: Path-loss exponent
β: Backscatter portion in BC mode
η, η_b: Signal to DC efficiency and backscatter efficiency
λ: Intensity of a point process
μ: Parameter of an exponential distribution (fading)
ξ: Available portion of harvested energy E_H
Φ: A Poisson point process
h: Fading of signal from an MBS to its ST or its PR
g: Fading of any interference signal
q: Fading of signal from an ST to its SR
p_c: Coverage probability
p_{ch}: Probability that a channel of a cell is used by an ST
p_{sat}: Circuit power constraint satisfaction probability
p_ρ: Probability that an ST transmits at power P_ρ
P, S, I, W: Transmit, desired signal, interference, and noise power
R_m, R_M: Inner and outer radii of the annular region
$\mathscr{L}_A(s)$: Laplace transform of r.v. A
$\mathbf{C}, c$: Channel set and a channel
M: Minislot number of a time slot
D_B, D_E: Backscatter and energy harvesting minislot number
E_H, E_C: Harvested energy and circuit power consumption
T: SINR Threshold
Y, U, X, Z: An MBS, a PR, an ST, and an SR (or their positions)
ρ: Sensitivity of an SR in IT mode
P_ρ: Transmit power considering power control
$\cdot_{\text{bs}}$ or $\cdot^{\text{bs}}$: Notations about busy MBSs
$\cdot_{\text{bc}}$ or $\cdot^{\text{bc}}$: Notations about STs in BC mode
$\cdot_{\text{it}}$ or $\cdot^{\text{it}}$: Notations about STs in IT mode or working STs
$\cdot_0$: The typical entities ($\cdot$ can be MBS, PR, ST, or SR).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Natural Science Foundation of China (61701230), Natural Science Foundation of Jiangsu Province (BK20170805, BK20160812), China Postdoctoral Science Foundation (2017M611806), Postdoctoral Science Foundation of Jiangsu Province (1701137A), research funding (2016-PYS/K-KY-J061), Foundation of Graduate Innovation Center in NUAA (KFJJ20171604), and the Fundamental Research Funds for the Central Universities.

References

[1] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proceedings of the 2016 ACM Conference on Special Interest Group on Data Communication, SIGCOMM 2016*, pp. 370–383, Brazil, August 2016.

[2] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-Fi backscatter: Internet connectivity for RF-powered devices," in *Proceedings of the 2014 ACM Conference on Special Interest Group on Data Communication, SIGCOMM 2014*, pp. 607–618, Chicago, Illinois, USA, August 2014.

[3] K. V. S. Rao, P. V. Nikitin, and S. F. Lam, "Antenna design for UHF RFID tags: a review and a practical application," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 12, pp. 3870–3876, 2005.

[4] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," in *Proceedings of the ACM Conference on SIGCOMM (SIGCOMM '13)*, pp. 39–50, Hong Kong, China, August 2013.

[5] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: a contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[6] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4788–4799, 2013.

[7] V. Rakovic, D. Denkovski, Z. Hadzi-Velkov, and L. Gavrilovska, "Optimal time sharing in underlay cognitive radio systems with RF energy harvesting," in *Proceedings of the IEEE International Conference on Communications, ICC '15*, pp. 7689–7694, London, UK, June 2015.

[8] H. D. Thai, D. Niyato, P. Wang, D. I. Kim, and Z. Han, "The tradeoff analysis in RF-powered backscatter cognitive radio networks," in *Proceedings of the 59th IEEE Global Communications Conference, GLOBECOM 2016*, Washington, D.C., USA, December 2016.

[9] F. Akhtar, M. H. Rehmani, and M. Reisslein, "White space: definitional perspectives and their role in exploiting spectrum opportunities," *Telecommunications Policy*, vol. 40, no. 4, pp. 319–331, 2016.

[10] M. Monemi, M. Rasti, and E. Hossain, "Characterizing feasible interference region for underlay cognitive radio networks," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 7603–7608, London, UK, June 2015.

[11] M. Monemi, M. Rasti, and E. Hossain, "On Characterization of Feasible Interference Regions in Cognitive Radio Networks," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 511–524, 2016.

[12] Y. Saleem and M. H. Rehmani, "Primary radio user activity models for cognitive radio networks: a survey," *Journal of Network and Computer Applications*, vol. 43, pp. 1–16, 2014.

[13] Y. Chen and H.-S. Oh, "A survey of measurement-based spectrum occupancy modeling for cognitive radios," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 848–859, 2016.

[14] M. Eskola, M. Matinmikko, J. Kalliovaara et al., "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2386–2414, 2016.

[15] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, "Spectrum prediction in cognitive radio networks," *IEEE Wireless Communications Magazine*, vol. 20, no. 2, pp. 90–96, 2013.

[16] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient Backscatter Assisted Wireless Powered Communications," *IEEE Wireless Communications Magazine*, pp. 2–9, 2018.

[17] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Optimal time sharing in RF-powered backscatter cognitive radio networks," in *Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017*, Paris, France, May 2017.

[18] S. H. Kim and D. I. Kim, "Hybrid Backscatter Communication for Wireless-Powered Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6557–6570, 2017.

[19] K. Han and K. Huang, "Wirelessly Powered Backscatter Communication Networks: Modeling, Coverage, and Capacity," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2548–2561, 2017.

[20] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and P. Wang, "Analysis of Wireless-Powered Device-to-Device Communications with Ambient Backscattering," in *Proceedings of the 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–6, Toronto, ON, Canada, September 2017.

[21] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-Powered Device-to-Device Communications with Ambient Backscattering: Performance Modeling and Analysis," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1528–1544, 2018.

[22] M. Haenggi, "A geometric interpretation of fading in wireless networks: theory and applications," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 12, pp. 5500–5510, 2008.

[23] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[24] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6727–6740, 2014.

[25] Y. J. Chun, M. O. Hasna, and A. Ghrayeb, "Modeling heterogeneous cellular networks interference using poisson cluster processes," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 10, pp. 2182–2195, 2015.

[26] K. Zhu and E. Hossain, "Joint mode selection and spectrum partitioning for device-to-device communication: a dynamic stackelberg game," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1406–1420, 2015.

[27] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*, Wiley Series in Probability and Mathematical Statistics: Applied Probability and Statistics, John Wiley & Sons, Ltd., Chichester, New York, NY, USA, 1995.

[28] Y. L. Che, L. Duan, and R. Zhang, "Spatial Throughput Maximization of Wireless Powered Communication Networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 8, pp. 1534–1548, 2015.

[29] H. ElSawy, E. Hossain, and M.-S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147–4161, 2014.

[30] K. S. Ali, H. ElSawy, and M.-S. Alouini, "Modeling Cellular Networks with Full-Duplex D2D Communication: A Stochastic Geometry Approach," *IEEE Transactions on Communications*, vol. 64, no. 10, pp. 4409–4424, 2016.

[31] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418–428, 2014.

[32] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Time-Hopping Multiple-Access for Backscatter Interference Networks," in *Proceedings of the GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–7, Singapore, December 2017.

[33] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: stochastic geometry modeling and analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1867–1880, 2015.